



Guida per l'utente

Amazon Macie



Amazon Macie: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Cos'è Amazon Macie?	1
Caratteristiche di Macie	2
Accedere a Macie	5
Prezzi per Macie	6
Servizi correlati	7
Nozioni di base	8
Prima di iniziare	8
Passaggio 1: abilitare Macie	8
Fase 2: Configurare un repository per i risultati della scoperta di dati sensibili	9
Fase 3: Esplora alcuni esempi di risultati	10
Fase 4: Crea un lavoro per scoprire dati sensibili	11
Fase 5: Esaminare i risultati	12
Concetti e terminologia	14
account	14
account amministratore	14
elenco di indirizzi consentiti	15
rilevamento automatico di dati sensibili	15
AWS Formato ASFF (Security Finding Format)	15
byte o dimensioni classificabili	16
oggetto classificabile	16
identificatore di dati personalizzato	17
regola di filtro	17
risultato	17
ricerca di un evento	18
job	18
identificatore di dati gestito	18
account membro	18
organizzazione	19
definizione delle politiche	19
esempio di reperto	19
ricerca di dati sensibili	20
lavoro di scoperta di dati sensibili	20
risultato della scoperta di dati sensibili	20
session	21

account autonomo	21
scoperta soppressa	21
regola di soppressione	21
byte o dimensioni non classificabili	22
oggetto inclassificabile	22
Monitoraggio della sicurezza e della privacy dei dati	23
In che modo Macie monitora la sicurezza dei dati di Amazon S3	24
Componenti chiave	24
Aggiornamenti dei dati	28
Considerazioni	30
Valutazione del tuo livello di sicurezza in Amazon S3	32
Visualizzazione del pannello di controllo	33
Comprendere i componenti del dashboard	33
Comprensione delle statistiche sulla sicurezza dei dati sulla dashboard	38
Analisi del livello di sicurezza di Amazon S3	42
Revisione dell'inventario dei bucket S3	42
Filtrare l'inventario dei bucket S3	55
Consentire a Macie di accedere a bucket e oggetti S3	68
Rilevamento dei dati sensibili	73
Utilizzo di identificatori di dati gestiti	75
Requisiti delle parole chiave	76
Riferimento rapido per tipo di dati sensibili	78
Riferimento dettagliato per categoria di dati sensibili	100
Creazione di identificatori di dati personalizzati	153
Opzioni di configurazione per identificatori di dati personalizzati	154
Creazione di un identificatore di dati personalizzato	159
Eliminazione di un identificatore di dati personalizzato	166
Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti	169
Opzioni di configurazione per gli elenchi consentiti	170
Creazione di un elenco di autorizzazioni	182
Verifica dello stato di una lista consentita	190
Modifica di un elenco di autorizzazioni	195
Eliminazione di un elenco consentito	198
Esecuzione del rilevamento automatico di dati sensibili	200
Come funziona il rilevamento automatico	202
Configurazione del rilevamento automatico	209

Revisione delle statistiche e dei risultati della scoperta automatica	239
Valutazione della copertura automatizzata del rilevamento	271
Regolazione dei punteggi di sensibilità per i bucket S3	284
Punteggio di sensibilità per i bucket S3	290
Impostazioni di rilevamento automatico predefinite	298
Esecuzione di processi di rilevamento dei dati sensibili	309
Opzioni relative all'ambito per i processi	311
Creazione di un processo	324
Revisione dei risultati del lavoro	336
Gestione dei processi	340
Monitoraggio dei lavori con CloudWatch Logs	352
Previsione e monitoraggio dei costi del lavoro	369
Identificatori di dati gestiti consigliati per i lavori	373
Analisi di oggetti S3 crittografati	376
Opzioni di crittografia per oggetti S3	377
Consentire a Macie di utilizzare un servizio gestito dal cliente AWS KMS key	379
Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili	386
Prima di iniziare: impara i concetti chiave	387
Passaggio 1: verifica le autorizzazioni	389
Fase 2: Configurare un AWS KMS key	390
Passaggio 3: scegli un bucket S3	394
Classi e formati di archiviazione supportati	403
Classi di storage supportate	403
Formati di file e di archiviazione supportati	404
Revisione e analisi dei risultati	407
Tipi di risultati	409
Tipi di risultati politici	410
Tipi di dati sensibili rilevati	413
Punteggio di gravità dei risultati	414
Punteggio di severità per i risultati delle politiche	415
Punteggio di gravità per le rilevazioni di dati sensibili	416
Lavorare con i risultati di esempio	423
Creazione di risultati di esempio	424
Revisione dei risultati di esempio	425
Soppressione dei risultati dei campioni	427
Analisi dei risultati	427

Filtro dei risultati	431
Nozioni fondamentali sui filtri	432
Campi per filtrare i risultati	441
Creazione e applicazione di filtri	470
Definizione delle regole di filtro	480
Analisi dei dati sensibili con risultati	489
Individuazione di dati sensibili	490
Recupero di campioni di dati sensibili	495
Schema per l'ubicazione dei dati sensibili	537
Eliminazione dei risultati	547
Creazione di una regola di soppressione	549
Revisione dei risultati soppressi	553
Modifica di una regola di soppressione	555
Eliminazione di una regola di soppressione	558
Monitoraggio ed elaborazione dei risultati	560
Configurazione delle impostazioni di pubblicazione per i risultati	561
Scelta delle destinazioni di pubblicazione	562
Modifica della frequenza di pubblicazione	563
Elaborazione dei risultati con Amazon EventBridge	565
Utilizzo di EventBridge	566
Creazione di EventBridge regole per i risultati	566
Monitoraggio dei risultati con Notifiche all'utente AWS	571
Utilizzo di Notifiche all'utente AWS	572
Abilitazione e configurazione delle notifiche per i risultati	572
Mappatura dei campi di notifica ai campi di ricerca	574
Modifica delle impostazioni di notifica per i risultati	578
Disattivazione delle notifiche relative ai risultati	578
Valutazione dei risultati con AWS Security Hub	578
Come Macie pubblica i risultati su Security Hub	579
Esempi di scoperte di Macie in Security Hub	584
Integrazione di Macie con Security Hub	590
Interruzione della pubblicazione dei risultati di Macie su Security Hub	590
Schema EventBridge degli eventi di Amazon per i risultati	590
Schema degli eventi per i risultati di Macie	591
Esempio di evento relativo alla definizione di una politica	592
Esempio di evento per il rilevamento di dati sensibili	596

Previsione e monitoraggio dei costi	603
Comprendere i costi di utilizzo stimati	603
Revisione dei costi di utilizzo stimati	607
Analisi dei costi di utilizzo stimati sulla console	607
Interrogazione dei costi di utilizzo stimati con l'API	608
Partecipare alla prova gratuita	613
Gestione di più account	617
Relazioni tra amministratore e account membro	617
Gestione degli account con AWS Organizations	623
Considerazioni e raccomandazioni	625
Integrazione e configurazione di un'organizzazione	629
Revisione degli account dell'organizzazione	639
Gestione degli account dei membri	643
Modifica dell'account amministratore	651
Disabilitazione dell'integrazione con AWS Organizations	655
Gestione degli account tramite invito	656
Considerazioni e raccomandazioni	657
Creazione e gestione di un'organizzazione	662
Revisione degli account dell'organizzazione	674
Modifica dell'account amministratore	679
Gestire l'appartenenza a un'organizzazione	681
Applicazione di tag alle risorse	687
Nozioni fondamentali sull'etichettatura	687
Aggiunta di tag alle risorse	689
Controllo dell'accesso alle risorse mediante i tag	694
Revisione e modifica dei tag delle risorse	694
Revisione dei tag relativi alle risorse	695
Modifica dei tag per le risorse	698
Rimozione dei tag dalle risorse	701
Sicurezza	705
Protezione dei dati	706
Crittografia dei dati a riposo	707
Crittografia in transito	707
Gestione dell'identità e degli accessi	707
Destinatari	708
Autenticazione con identità	708

Gestione dell'accesso con policy	712
Come funziona Macie con IAM	715
Esempi di policy basate su identità	724
AWS politiche gestite	733
Ruoli collegati ai servizi	738
Risoluzione dei problemi	741
Convalida della conformità	742
Resilienza	743
Sicurezza dell'infrastruttura	744
AWS PrivateLink	745
Considerazioni sugli endpoint dell'interfaccia Macie	745
Creazione di un endpoint di interfaccia per Macie	746
Creazione di una policy sugli endpoint per Macie	746
Registrazione delle chiamate API di AWS CloudTrail con	749
Eventi gestionali di Macie in CloudTrail	750
Esempi di eventi Macie in CloudTrail	751
Esempio: elenco dei risultati	751
Esempio: recupero di campioni di dati sensibili per una scoperta	752
Creazione di risorse con AWS CloudFormation	756
Macie e modelli AWS CloudFormation	756
Risorse didattiche aggiuntive	756
Sospendere Macie	758
Disabilitazione di Macie	760
Quote	762
Cronologia dei documenti	766
.....	dcxc

Cos'è Amazon Macie?

Amazon Macie è un servizio di sicurezza dei dati che rileva dati sensibili utilizzando machine learning e la corrispondenza del modello, fornisce visibilità sui rischi legati alla sicurezza dei dati e consente una protezione automatizzata da tali rischi.

Per aiutarti a gestire il livello di sicurezza del patrimonio di dati Amazon Simple Storage Service (Amazon S3) della tua organizzazione, Macie ti fornisce un inventario dei tuoi bucket S3 per uso generico e valuta e monitora automaticamente i bucket per la sicurezza e il controllo degli accessi. Se Macie rileva un possibile problema con la sicurezza o la privacy dei dati dell'utente, ad esempio un bucket che diventa accessibile pubblicamente, genera un risultato per eseguire la verifica e la correzione, in base alle esigenze.

Macie automatizza anche l'individuazione e la segnalazione di dati sensibili per fornirti una migliore comprensione dei dati che la tua organizzazione archivia in Amazon S3. Per rilevare dati sensibili, è possibile utilizzare criteri e tecniche predefiniti forniti da Macie, criteri personalizzati definiti dall'utente o una combinazione dei due. Se Macie rileva dati sensibili in un oggetto S3, Macie genera un risultato per informarti dei dati sensibili che ha trovato.

Oltre ai risultati, Macie fornisce statistiche e informazioni che offrono informazioni sullo stato di sicurezza dei tuoi dati Amazon S3 e su dove potrebbero risiedere i dati sensibili nel tuo patrimonio di dati. Le statistiche e le informazioni possono guidare le vostre decisioni per eseguire indagini più approfondite su specifici bucket e oggetti S3. Puoi esaminare e analizzare risultati, statistiche e altre informazioni utilizzando la console Amazon Macie o l'API Amazon Macie. Puoi anche sfruttare l'integrazione di Macie con Amazon EventBridge e AWS Security Hub monitorare, elaborare e correggere i risultati utilizzando altri servizi, applicazioni e sistemi.

Argomenti

- [Caratteristiche di Macie](#)
- [Accedere a Macie](#)
- [Prezzi per Macie](#)
- [Servizi correlati](#)

Caratteristiche di Macie

Ecco alcuni dei modi principali in cui Amazon Macie può aiutarti a scoprire, monitorare e proteggere i tuoi dati sensibili in Amazon S3.

Automatizza la scoperta di dati sensibili

Con Macie, puoi automatizzare il rilevamento e la segnalazione dei dati sensibili in due modi: configurando Macie per [eseguire il rilevamento automatico dei dati sensibili e creando ed eseguendo processi di rilevamento](#) di dati sensibili. Se Macie rileva dati sensibili in un oggetto S3, crea una ricerca di dati sensibili per te. La scoperta fornisce un rapporto dettagliato dei dati sensibili rilevati da Macie.

Il rilevamento automatico dei dati sensibili offre un'ampia visibilità su dove potrebbero risiedere i dati sensibili nel tuo patrimonio di dati Amazon S3. Con questa opzione, Macie valuta continuamente l'inventario dei bucket S3 e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi dai bucket. Macie recupera e analizza quindi gli oggetti selezionati, ispezionandoli alla ricerca di dati sensibili.

I lavori di rilevamento di dati sensibili forniscono un'analisi più approfondita e mirata. Con questa opzione, definisci l'ampiezza e la profondità dell'analisi: i bucket S3 da analizzare, la profondità di campionamento e i criteri personalizzati che derivano dalle proprietà degli oggetti S3. È inoltre possibile configurare un processo in modo che venga eseguito una sola volta per l'analisi e la valutazione su richiesta o su base ricorrente per analisi, valutazione e monitoraggio periodici.

Entrambe le opzioni possono aiutarti a creare e mantenere una visione completa dei dati archiviati dalla tua organizzazione in Amazon S3 e di eventuali rischi di sicurezza o conformità per tali dati.

Scopri una varietà di tipi di dati sensibili

Per scoprire dati sensibili con Macie, puoi utilizzare criteri e tecniche integrati, come l'apprendimento automatico e il pattern matching, per analizzare gli oggetti nei bucket S3. Questi criteri e tecniche, denominati [identificatori di dati gestiti](#), sono in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili per molti paesi e aree geografiche, inclusi diversi tipi di informazioni di identificazione personale (PII), informazioni finanziarie e dati relativi alle credenziali.

[È inoltre possibile utilizzare identificatori di dati personalizzati.](#) Un identificatore di dati personalizzato è un insieme di criteri definiti per rilevare dati sensibili: un'espressione regolare

(regex) che definisce uno schema di testo da abbinare e, facoltativamente, sequenze di caratteri e una regola di prossimità che perfeziona i risultati. Con questo tipo di identificatore, puoi rilevare dati sensibili che riflettono scenari particolari, proprietà intellettuale o dati proprietari. Puoi integrare gli identificatori di dati gestiti forniti da Macie.

[Per ottimizzare le analisi, puoi anche utilizzare gli elenchi consentiti.](#) Gli elenchi Consenti definiscono testo e modelli di testo specifici che vuoi che Macie ignori negli oggetti S3. Si tratta in genere di eccezioni relative ai dati sensibili per scenari o ambienti particolari, ad esempio i nomi dei rappresentanti pubblici dell'organizzazione, i numeri di telefono pubblici dell'organizzazione o dati di esempio utilizzati dall'organizzazione per i test.

Valuta e monitora i dati per la sicurezza e il controllo degli accessi

Quando abiliti Macie, Macie genera automaticamente e inizia a gestire un inventario dei tuoi bucket S3 per uso generico. Macie inizia anche a valutare e monitorare i bucket per la sicurezza e il controllo degli accessi. [Se Macie rileva un potenziale problema con la sicurezza o la privacy di un bucket, crea una policy per te.](#)

Oltre ai risultati, una [dashboard](#) offre un'istantanea delle statistiche aggregate per i dati di Amazon S3. Ciò include statistiche per parametri chiave come il numero di bucket accessibili pubblicamente o condivisi con altri. Account AWS Puoi approfondire ogni statistica per esaminare i dati di supporto.

Macie fornisce anche informazioni e statistiche dettagliate per i singoli bucket S3 presenti nell'inventario. I dati includono le suddivisioni delle impostazioni di accesso pubblico e crittografia di un bucket e le dimensioni e il numero di oggetti che Macie può analizzare per rilevare i dati sensibili nel bucket. Puoi [sfogliare l'inventario](#) o ordinare e filtrare l'inventario in base a determinati campi.

Rivedi e analizza i risultati

In Macie, un risultato è un rapporto dettagliato sui dati sensibili rilevati da Macie in un oggetto S3 o su un potenziale problema con la sicurezza o la privacy di un bucket S3 per uso generico. Ogni risultato fornisce un indice di gravità, informazioni sulla risorsa interessata e dettagli aggiuntivi, ad esempio quando e come Macie ha rilevato i dati o il problema.

Per [esaminare, analizzare e gestire i risultati](#), puoi utilizzare le pagine Findings sulla console Amazon Macie. Queste pagine elencano i risultati e forniscono i dettagli dei singoli risultati. Forniscono inoltre diverse opzioni per raggruppare, filtrare, ordinare e sopprimere i risultati. Puoi anche utilizzare l'API Amazon Macie per recuperare ed esaminare i risultati. Se utilizzi l'API, puoi

passare i dati a un'altra applicazione, servizio o sistema per analisi più approfondite, archiviazione a lungo termine o reportistica.

Monitora ed elabora i risultati con altri servizi e sistemi

Per supportare l'integrazione con altri servizi e sistemi, Macie [pubblica i risultati su Amazon sotto EventBridge](#) forma di eventi. EventBridge è un servizio di bus eventi senza server in grado di indirizzare i dati dei risultati verso destinazioni come AWS Lambda funzioni e argomenti di Amazon Simple Notification Service (Amazon SNS). Con EventBridge, puoi monitorare ed elaborare i risultati quasi in tempo reale come parte dei flussi di lavoro di sicurezza e conformità esistenti.

Puoi configurare Macie per [pubblicare i risultati anche su](#) AWS Security Hub. Security Hub è un servizio che fornisce una visione completa del livello di sicurezza in tutto l'AWS ambiente e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Con Security Hub, puoi valutare ed elaborare più facilmente i risultati come parte di un'analisi più ampia del livello di sicurezza della tua organizzazione. AWS è inoltre possibile aggregare i risultati di più Regioni AWS risultati e quindi valutare ed elaborare i dati aggregati relativi ai risultati provenienti da una singola regione.

Gestisci centralmente più account Macie

Se il tuo AWS ambiente ha più account, puoi [gestire centralmente Macie](#) for Account nel tuo ambiente. Puoi farlo in due modi: integrando Macie con Macie AWS Organizations o inviando e accettando gli inviti all'iscrizione in Macie.

In una configurazione con più account, un amministratore Macie designato può eseguire determinate attività e accedere a determinate impostazioni, dati e risorse di Macie per gli account che sono membri della stessa organizzazione. Le attività includono la revisione delle informazioni sui bucket S3 di proprietà degli account dei membri, la revisione dei risultati delle politiche per tali bucket e l'ispezione dei bucket alla ricerca di dati sensibili. Se gli account sono associati tramite AWS Organizations, l'amministratore di Macie può abilitare Macie anche per gli account dei membri dell'organizzazione.

Sviluppa e gestisci le risorse in modo programmatico

[Oltre alla console Amazon Macie, puoi interagire con Macie utilizzando l'API Amazon Macie.](#)

L'API Amazon Macie ti offre un accesso completo e programmatico alle impostazioni, ai dati e alle risorse di Macie.

Per interagire con Macie a livello di codice, puoi inviare richieste HTTPS direttamente a Macie o utilizzare una versione corrente di uno strumento a riga di comando o di un AWS SDK. AWS

AWS fornisce strumenti SDKs che consistono in librerie e codice di esempio per vari linguaggi e piattaforme, come Java PowerShell, Go, Python, C++ e .NET.

Accedere a Macie

Amazon Macie è disponibile nella maggior parte dei casi. Regioni AWS Per un elenco delle regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS Per informazioni sulla gestione Regioni AWS del tuo account Account AWS, consulta [Abilita o disabilita Regioni AWS nel tuo account nella Guida](#) di riferimento. Gestione dell'account AWS

In ogni regione, puoi lavorare con Macie in uno dei seguenti modi.

AWS Management Console

AWS Management Console È un'interfaccia basata su browser che puoi utilizzare per creare e gestire risorse. AWS Come parte di tale console, la console Amazon Macie fornisce l'accesso all'account, ai dati e alle risorse Macie. Puoi eseguire qualsiasi attività su Macie utilizzando la console Macie: rivedi le statistiche e altre informazioni sui tuoi bucket S3, crea ed esegui processi di rilevamento di dati sensibili, rivedi e analizza i risultati e altro ancora.

AWS strumenti da riga di comando

Con gli strumenti da riga di AWS comando, puoi impartire comandi dalla riga di comando del tuo sistema per eseguire attività e AWS attività di Macie. L'uso della riga di comando può essere più rapido e comodo rispetto all'utilizzo della console. Gli strumenti a riga di comando sono inoltre utili per creare script che eseguono le attività di .

AWS fornisce due set di strumenti da riga di comando: the AWS Command Line Interface (AWS CLI) e the AWS Strumenti per PowerShell. Per informazioni sull'installazione e l'utilizzo di AWS CLI, consulta la [Guida AWS Command Line Interface per l'utente](#). Per informazioni sull'installazione e l'utilizzo degli strumenti per PowerShell, consultate la [Guida per AWS Strumenti per PowerShell l'utente](#).

AWS SDKs

AWS fornisce SDKs che consistono in librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, ad esempio Java, Go, Python, C++ e .NET. SDKs Forniscono un accesso comodo e programmatico a Macie e ad altri. Servizi AWS Gestiscono anche attività come la firma

crittografica delle richieste, la gestione degli errori e il tentativo automatico delle richieste. Per informazioni sull'installazione e l'utilizzo di AWS SDKs, consulta [Tools to Build on. AWS](#)

API REST di Amazon Macie

L'API REST di Amazon Macie ti offre un accesso completo e programmatico all'account, ai dati e alle risorse Macie. Con questa API, puoi inviare richieste HTTPS direttamente a Macie. Tuttavia, a differenza degli strumenti a riga di AWS comando e SDKs, l'uso di questa API richiede che l'applicazione gestisca dettagli di basso livello, come la generazione di un hash per firmare una richiesta. Per informazioni su questa API, consulta [Amazon Macie API Reference](#).

Prezzi per Macie

Come per altri AWS prodotti, non sono previsti contratti o impegni minimi per l'utilizzo di Amazon Macie.

I prezzi di Macie si basano su diverse dimensioni: valutazione e monitoraggio dei bucket S3 per la sicurezza e il controllo degli accessi, monitoraggio degli oggetti S3 per l'individuazione automatica di dati sensibili e analisi degli oggetti S3 per rilevare e segnalare i dati sensibili contenuti negli oggetti. Per ulteriori informazioni, consulta i [prezzi di Amazon Macie](#).

Per aiutarti a comprendere e prevedere i costi di utilizzo di Macie, Macie fornisce una stima dei costi di utilizzo del tuo account. Puoi [rivedere queste stime](#) sulla console Amazon Macie e accedervi con l'API Amazon Macie. A seconda di come utilizzi il servizio, potresti incorrere in costi aggiuntivi per l'utilizzo di Other Servizi AWS in combinazione con determinate funzionalità di Macie, come il recupero dei dati del bucket da Amazon S3 e l'utilizzo di oggetti gestiti dal cliente per decrittografare gli oggetti per l'analisi. AWS KMS keys

Quando abiliti Macie per la prima volta, vieni automaticamente registrato alla prova gratuita di 30 giorni di Macie. Account AWS Sono inclusi gli account individuali abilitati come parte di un'organizzazione in. AWS Organizations Durante la prova gratuita, non è previsto alcun costo per l'utilizzo di Macie nella versione applicabile Regione AWS per valutare e monitorare i bucket S3 per motivi di sicurezza e controllo degli accessi. A seconda delle impostazioni dell'account, la prova gratuita può includere anche l'individuazione automatica di dati sensibili per i dati di Amazon S3. La versione di prova gratuita non include l'esecuzione di processi di rilevamento di dati sensibili per rilevare e segnalare dati sensibili negli oggetti S3.

Per aiutarti a comprendere e prevedere il costo dell'utilizzo di Macie al termine del periodo di prova gratuito, Macie fornisce una stima dei costi di utilizzo in base all'utilizzo di Macie durante il periodo di

prova. I dati di utilizzo indicano anche il tempo che rimane prima della fine della prova gratuita. Puoi esaminare questi dati sulla console Amazon Macie e accedervi con l'API Amazon Macie. Per ulteriori informazioni, consulta [Partecipare alla prova gratuita](#).

Servizi correlati

Per proteggere ulteriormente dati, carichi di lavoro e applicazioni, prendi in AWS considerazione l'utilizzo di quanto segue Servizi AWS in combinazione con Amazon Macie.

AWS Security Hub

AWS Security Hub ti offre una visione completa dello stato di sicurezza delle tue AWS risorse e ti aiuta a controllare il tuo AWS ambiente rispetto agli standard e alle best practice del settore della sicurezza. Lo fa in parte consumando, aggregando, organizzando e dando priorità ai risultati di sicurezza provenienti da più prodotti Servizi AWS (incluso Macie) e supportati AWS Partner Network (APN). Security Hub ti aiuta ad analizzare le tendenze della sicurezza e a identificare i problemi di sicurezza con la massima priorità in tutto l' AWS ambiente.

Per ulteriori informazioni su Security Hub, consulta la [Guida AWS Security Hub per l'utente](#). Per ulteriori informazioni sull'utilizzo congiunto di Macie e Security Hub, consulta [Valutazione dei risultati di Macie con AWS Security Hub](#).

Amazon GuardDuty

Amazon GuardDuty è un servizio di monitoraggio della sicurezza che analizza ed elabora determinati tipi di AWS log, come i registri degli eventi di AWS CloudTrail dati per Amazon S3 e i registri degli eventi di gestione. CloudTrail Utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, e l'apprendimento automatico per identificare attività impreviste, potenzialmente non autorizzate e dannose all'interno dell'ambiente. AWS

Per ulteriori informazioni GuardDuty, consulta la [Amazon GuardDuty User Guide](#).

Per ulteriori informazioni sui servizi AWS di sicurezza aggiuntivi, consulta [Sicurezza, identità e conformità su AWS](#).

Guida introduttiva a Macie

Questo tutorial fornisce un'introduzione ad Amazon Macie. Imparerai come abilitare Macie per il tuo Account AWS. Imparerai anche a valutare il tuo livello di sicurezza di Amazon Simple Storage Service (Amazon S3) e a configurare le impostazioni e le risorse chiave per scoprire e segnalare dati sensibili nei tuoi bucket S3.

Attività

- [Prima di iniziare](#)
- [Passaggio 1: abilitare Macie](#)
- [Fase 2: Configurare un repository per i risultati della scoperta di dati sensibili](#)
- [Fase 3: Esplora alcuni esempi di risultati](#)
- [Fase 4: Crea un lavoro per scoprire dati sensibili](#)
- [Fase 5: Esaminare i risultati](#)

Prima di iniziare

Quando ti registri ad Amazon Web Services (AWS), il tuo account viene automaticamente registrato per tutti Servizi AWS, incluso Amazon Macie. Tuttavia, per abilitare e utilizzare Macie, devi prima configurare le autorizzazioni che ti consentano di accedere alla console Amazon Macie e alle operazioni API. Tu o il tuo AWS amministratore potete farlo utilizzando AWS Identity and Access Management (IAM) per allegare la policy AWS gestita denominata AmazonMacieFullAccess alla vostra identità IAM. Per ulteriori informazioni, consulta [AWS politiche gestite per Macie](#).

Passaggio 1: abilitare Macie

Dopo aver configurato le autorizzazioni richieste, puoi abilitare Amazon Macie per il tuo Account AWS. Segui questi passaggi per abilitare Macie per il tuo account.

Per abilitare Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri abilitare e usare Macie.

3. Nella pagina Amazon Macie, scegli Inizia.
4. (Facoltativo) Quando attivi Macie, Macie crea automaticamente un ruolo collegato al servizio che gli consente di chiamare altre persone Servizi AWS e monitorare AWS le risorse per tuo conto. Per rivedere la politica delle autorizzazioni per questo ruolo, scegli Visualizza le autorizzazioni dei ruoli sulla console. Per ulteriori informazioni su questo ruolo, consulta [Utilizzo di ruoli collegati ai servizi per Macie](#)
5. Scegliere Abilita Macie.

In pochi minuti, Macie genera e inizia automaticamente a gestire un inventario dei bucket generici S3 nella regione corrente. Macie inizia anche a valutare e monitorare i bucket per la sicurezza e il controllo degli accessi. Per ulteriori informazioni, consulta [Monitoraggio della sicurezza e della privacy dei dati](#).

A seconda delle impostazioni dell'account, Macie inizia anche a eseguire il rilevamento automatico dei dati sensibili per i bucket S3. Macie inizia a identificare, selezionare e analizzare continuamente gli oggetti rappresentativi nei bucket, ispezionando gli oggetti alla ricerca di dati sensibili. Man mano che le analisi procedono, Macie fornisce statistiche e altri risultati che è possibile esaminare, in genere entro 48 ore. Puoi personalizzare le analisi. Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#).

Per esaminare le statistiche aggregate per i dati di Amazon S3, scegli Riepilogo nel riquadro di navigazione sulla console. Per visualizzare i dettagli sui singoli bucket S3 presenti nel tuo inventario, scegli i bucket S3 nel pannello di navigazione. Per visualizzare quindi i dettagli di un bucket, scegli il bucket. Il pannello dei dettagli mostra statistiche e altre informazioni che forniscono informazioni sulla sicurezza, la privacy e la sensibilità dei dati del bucket. Per ulteriori informazioni su questi dettagli, consulta [Revisione dell'inventario dei bucket S3](#).

Fase 2: Configurare un repository per i risultati della scoperta di dati sensibili

Con Amazon Macie, puoi scoprire dati sensibili nei bucket S3 in due modi: configurando Macie per eseguire il rilevamento automatico dei dati sensibili ed eseguendo processi di rilevamento di dati sensibili. Un processo di rilevamento di dati sensibili è un processo creato per analizzare gli oggetti nei bucket S3 per determinare se gli oggetti contengono dati sensibili.

Macie crea un record per ogni oggetto S3 che analizza quando esegui processi di rilevamento di dati sensibili o esegue il rilevamento automatico di dati sensibili. Questi record, denominati risultati

di rilevamento di dati sensibili, registrano dettagli sull'analisi dei singoli oggetti. Macie crea anche risultati di rilevamento di dati sensibili per oggetti che non può analizzare a causa di errori o problemi. I risultati dell'individuazione di dati sensibili forniscono record di analisi che possono essere utili per controlli o indagini sulla privacy e sulla protezione dei dati.

Macie archivia i risultati della scoperta dei dati sensibili per soli 90 giorni. Per accedere ai risultati e consentirne l'archiviazione e la conservazione a lungo termine, configura Macie in modo che memorizzi i risultati in un bucket S3. Dovresti farlo entro 30 giorni dall'attivazione di Macie. Dopo averlo fatto, il bucket può fungere da archivio definitivo a lungo termine per tutti i risultati della scoperta di dati sensibili.

Per informazioni su come configurare questo repository, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#)

Fase 3: Esplora alcuni esempi di risultati

In Amazon Macie, esistono due categorie di risultati, risultati relativi alle politiche e risultati relativi a dati sensibili. Macie crea una policy rilevando quando le politiche o le impostazioni per un bucket generico S3 vengono modificate in modo da ridurre la sicurezza o la privacy del bucket e degli oggetti in esso contenuti. Macie crea una ricerca di dati sensibili quando rileva dati sensibili in un oggetto S3. All'interno di ogni categoria, esistono diversi tipi di risultati.

Per esplorare e conoscere le diverse categorie e tipi di risultati forniti da Macie, opzionalmente crea ed esamina i risultati di esempio. I risultati di esempio utilizzano dati di esempio e valori segnaposto per dimostrare i tipi di informazioni che Macie potrebbe includere in ogni tipo di risultato.

Segui questi passaggi per creare ed esaminare risultati di esempio.

Per creare ed esaminare i risultati di esempio

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione scegli Impostazioni.
3. In Risultati di esempio, scegli Genera risultati di esempio. Macie genera un risultato di esempio per ogni tipo di risultato supportato da Macie.
4. Nel riquadro di navigazione, seleziona Esiti. La pagina Risultati mostra i risultati relativi al tuo account nella versione corrente. Regione AWS Ciò include i risultati di esempio che hai creato nel passaggio precedente.

5. Nella pagina Risultati, individuate i risultati il cui tipo inizia con [ESEMPIO].
6. Per esaminare i dettagli di un particolare risultato campionario, scegliete il risultato. Il pannello dei dettagli mostra i dettagli del risultato.

Per ulteriori informazioni su ciascun tipo di risultato, vedere [Tipi di risultati](#). Per ulteriori informazioni sulla creazione e la revisione dei risultati di esempio, vedere [Lavorare con i risultati di esempio](#).

Fase 4: Crea un lavoro per scoprire dati sensibili

Per scoprire e segnalare dati sensibili nei bucket S3, puoi eseguire processi di rilevamento di dati sensibili. Un processo di rilevamento di dati sensibili è un processo creato per analizzare gli oggetti nei bucket S3 per determinare se gli oggetti contengono dati sensibili. A differenza del rilevamento automatico di dati sensibili, sei tu a definire l'ampiezza e la profondità dell'analisi. È inoltre possibile specificare la frequenza con cui eseguire un processo, una volta o periodicamente in base a una pianificazione.

Segui questi passaggi per creare un processo che venga eseguito una sola volta, subito dopo averlo creato, e utilizzi le impostazioni predefinite. Per informazioni su come creare un processo che viene eseguito periodicamente o utilizza impostazioni personalizzate, consulta [Creazione di un processo di rilevamento dei dati sensibili](#).

Per creare un processo di rilevamento di dati sensibili

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi).
3. Scegli Crea processo.
4. Per la fase Scegli i bucket S3, scegli Seleziona bucket specifici. Quindi, nella tabella, seleziona la casella di controllo per ogni bucket S3 che desideri venga analizzato dal processo.

La tabella fornisce un inventario dei bucket generici S3 attualmente in uso. Regione AWS Per trovare più facilmente bucket specifici, inserisci i criteri di filtro nella casella del filtro sopra la tabella. Puoi anche ordinare la tabella scegliendo un'intestazione di colonna.

5. Quando hai finito di selezionare i bucket, scegli Avanti.
6. Per il passaggio Rivedi i bucket S3, esamina e verifica le selezioni dei bucket, quindi scegli Avanti.
7. Per il passaggio Perfeziona l'ambito, scegli Elaborazione singola, quindi scegli Avanti.

8. Per il passaggio Seleziona identificatori di dati gestiti, scegli Consigliato. Facoltativamente, esamina la tabella degli identificatori di dati gestiti consigliati per i lavori, quindi scegli Avanti.

Un identificatore di dati gestito è un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili, ad esempio numeri di carte di credito, chiavi di accesso AWS segrete o numeri di passaporto per un particolare paese o area geografica. Per ulteriori informazioni, consulta [Utilizzo di identificatori di dati gestiti](#).

9. Per il passaggio Seleziona identificatori di dati personalizzati, scegli Avanti.

Un identificatore di dati personalizzato è un insieme di criteri che definisci per rilevare dati sensibili: un'espressione regolare (regex) che definisce uno schema di testo da abbinare e, facoltativamente, sequenze di caratteri e una regola di prossimità che perfezionano i risultati. Per ulteriori informazioni, consulta [Creazione di identificatori di dati personalizzati](#).

10. Per il passaggio Seleziona elenchi consentiti, scegli Avanti.

In Macie, un elenco consentito specifica il testo o uno schema di testo che vuoi che Macie ignori quando ispeziona gli oggetti S3 alla ricerca di dati sensibili. Si tratta in genere di eccezioni relative ai dati sensibili per scenari o ambienti particolari. Per ulteriori informazioni, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).

11. Per il passaggio Inserisci impostazioni generali, inserisci un nome e, facoltativamente, una descrizione del lavoro. Quindi scegli Successivo.
12. Per la fase di revisione e creazione, rivedi le impostazioni di configurazione del lavoro e verifica che siano corrette.

Puoi anche rivedere il costo totale stimato (in dollari USA) dell'esecuzione del processo. La stima può aiutarvi a determinare se modificare le impostazioni del lavoro prima di salvarlo. Per ulteriori informazioni, consulta [Previsione del costo di un lavoro di scoperta di dati sensibili](#).

13. Al termine della revisione e della verifica delle impostazioni del lavoro, scegli Invia.

Macie inizia immediatamente a eseguire il lavoro. Per informazioni su come monitorare il lavoro, consulta [Verifica dello stato dei processi di rilevamento di dati sensibili](#).

Fase 5: Esaminare i risultati

Amazon Macie monitora automaticamente i bucket S3 per scopi generici per la sicurezza e il controllo degli accessi e crea risultati politici per segnalare potenziali problemi con la sicurezza o la privacy dei bucket. Se esegui un processo di rilevamento di dati sensibili o configuri Macie per eseguire il

rilevamento automatico di dati sensibili, Macie crea rilevamenti di dati sensibili per segnalare i dati sensibili rilevati negli oggetti S3.

Segui questi passaggi per esaminare i risultati.

Per esaminare i risultati

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti. La pagina Risultati mostra i risultati relativi al tuo account nella versione corrente Regione AWS.
3. Per filtrare i risultati in base a criteri specifici, inserisci i criteri nella casella del filtro sopra la tabella.
4. Per esaminare i dettagli di un particolare risultato, scegli il risultato. Il pannello dei dettagli mostra i dettagli del risultato.

Per ulteriori informazioni sui risultati, incluso come raggrupparli e filtrarli, consulta [Revisione e analisi dei risultati](#).

Concetti e terminologia in Macie

In Amazon Macie, ci basiamo su AWS concetti e terminologia comuni e utilizziamo questi termini aggiuntivi.

account

Uno standard Account AWS che contiene AWS le tue risorse e le identità che possono accedere a tali risorse.

Per usare Macie, accedi AWS con le tue Account AWS credenziali, seleziona quello Regione AWS in cui vuoi usare Macie, quindi abiliti Macie per te in quella regione. Account AWS Per ulteriori informazioni, consulta [Guida introduttiva a Macie](#).

Esistono tre tipi di account in Macie:

- Account amministratore: questo tipo di account gestisce gli account Macie per un'organizzazione. Un'organizzazione è un insieme di account Macie associati tra loro e gestiti centralmente come gruppo di account correlati in uno specifico gruppo. Regione AWS
- Account membro: questo tipo di account è associato e gestito dall'account amministratore Macie di un'organizzazione.
- Account autonomo: questo tipo di account non è né un account amministratore né un account membro. Non fa parte di un'organizzazione.

Puoi aggiungere account Macie a un'organizzazione in due modi: integrando Macie AWS Organizations o inviando e accettando gli inviti di iscrizione a Macie. Per ulteriori informazioni, consulta [Gestione di più account](#).

account amministratore

In Macie, un account che gestisce gli account Macie per un'organizzazione. Un'organizzazione è un insieme di account Macie associati tra loro e gestiti centralmente come gruppo di account correlati in uno specifico gruppo. Regione AWS

Gli utenti di un account amministratore Macie hanno accesso ai dati di inventario di Amazon Simple Storage Service (Amazon S3), ai [risultati delle policy](#) e a determinate impostazioni e risorse di Macie per tutti gli account della loro organizzazione. Possono anche eseguire operazioni [automatiche di](#)

[rilevamento di dati sensibili](#) ed eseguire [operazioni di rilevamento di dati sensibili](#) per rilevare dati sensibili nei bucket S3 di proprietà degli account. A seconda di come un account viene designato come account amministratore, possono anche essere in grado di eseguire attività aggiuntive per altri account della propria organizzazione.

Per ulteriori informazioni, consulta [Gestione di più account](#).

elenco di indirizzi consentiti

In Macie, un elenco consentito specifica il testo o uno schema di testo che si desidera che Macie ignori quando ispeziona gli oggetti S3 alla ricerca di dati sensibili.

È possibile creare due tipi di elenchi di caratteri consentiti in Macie: un file di testo semplice che elenca parole specifiche e altri tipi di sequenze di caratteri da ignorare o un'espressione regolare (regex) che definisce uno schema di testo da ignorare. Se un oggetto contiene testo che corrisponde a una voce o a uno schema in un elenco consentito, Macie non riporta il testo nei risultati relativi a [dati sensibili, statistiche e altri tipi di risultati](#). Questo è il caso anche se il testo corrisponde ai criteri di un identificatore di [dati gestito o di un identificatore](#) di [dati personalizzato](#).

Per ulteriori informazioni, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).

rilevamento automatico di dati sensibili

Una serie di attività di analisi automatizzate che Macie esegue continuamente per identificare e selezionare oggetti rappresentativi dai bucket S3 e ispezionare gli oggetti selezionati alla ricerca di dati sensibili.

[Man mano che le analisi procedono, Macie registra i dati sensibili che trova \(rilevamenti di dati sensibili\) e le analisi che esegue \(risultati della scoperta di dati sensibili\)](#). Macie aggiorna anche le statistiche e altre informazioni che fornisce sui dati di Amazon S3.

Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#).

AWS Formato ASFF (Security Finding Format)

Un formato JSON standardizzato per il contenuto dei [risultati](#) pubblicati o generati da AWS Security Hub. L'ASFF include dettagli sull'origine di un problema di sicurezza, sulle risorse interessate e sullo stato di un risultato.

Per informazioni su ASFF, vedere [AWS Security Finding Format \(ASFF\)](#) nella Guida per l'AWS Security Hub utente. Per informazioni sulla pubblicazione dei risultati di Macie su Security Hub, vedere [Valutazione dei risultati con AWS Security Hub](#).

byte o dimensioni classificabili

Nelle statistiche del bucket S3 fornite da Macie, la dimensione totale di archiviazione di tutti gli oggetti [classificabili](#) in un bucket S3.

Se il controllo delle versioni è abilitato per un bucket, questo valore si basa sulla dimensione di archiviazione della versione più recente di ogni oggetto classificabile nel bucket. Se un oggetto è un file compresso, questo valore non riflette la dimensione effettiva del contenuto del file dopo la decompressione.

Per ulteriori informazioni, consulta [Revisione dell'inventario dei bucket S3](#) e [Valutazione del tuo livello di sicurezza in Amazon S3](#).

oggetto classificabile

Un oggetto S3 che Macie può analizzare per rilevare dati sensibili.

Nel calcolare le statistiche del bucket S3, Macie determina che un oggetto è classificabile in base alla classe di archiviazione e all'estensione del nome di file dell'oggetto. Un oggetto è classificabile se utilizza una classe di storage Amazon S3 supportata e ha un'estensione del nome di file per un file o un formato di storage supportato.

Per ulteriori informazioni, consulta [Revisione dell'inventario dei bucket S3](#) e [Classi e formati di archiviazione supportati](#).

Per l'individuazione di dati sensibili, Macie determina che un oggetto è classificabile in base alla classe di archiviazione, all'estensione del nome di file e al contenuto dell'oggetto. Un oggetto è classificabile se: utilizza una classe di storage Amazon S3 supportata, ha un'estensione del nome di file per un file o un formato di storage supportato e Macie ha verificato che sia in grado di estrarre e analizzare i dati dall'oggetto.

Per ulteriori informazioni, consulta [Rilevamento dei dati sensibili](#) e [Classi e formati di archiviazione supportati](#).

identificatore di dati personalizzato

Un insieme di criteri definiti per rilevare dati sensibili.

I criteri sono costituiti da un'espressione regolare (regex) che definisce uno schema di testo da abbinare e, facoltativamente, sequenze di caratteri e una regola di prossimità che perfeziona i risultati. Le sequenze di caratteri possono essere:

- Parole chiave, che sono parole o frasi che devono trovarsi in prossimità di un testo che corrisponde all'espressione regolare, oppure
- Parole da ignorare, che sono parole o frasi da escludere dai risultati.

Oltre ai criteri di rilevamento, è possibile definire impostazioni di gravità personalizzate per i [dati sensibili rilevati](#) da un identificatore di dati personalizzato.

Per ulteriori informazioni, consulta [Creazione di identificatori di dati personalizzati](#).

regola di filtro

Un set di criteri di filtro basati sugli attributi che crei e salvi per analizzare i [risultati sulla console](#) Amazon Macie. Le regole di filtro possono aiutarti a eseguire un'analisi coerente dei risultati con caratteristiche specifiche, come tutti i risultati ad alta gravità che riportano un tipo specifico di dati sensibili.

Per ulteriori informazioni, consulta [Definizione delle regole di filtro](#).

risultato

Un rapporto dettagliato sui dati sensibili rilevati da Macie in un oggetto S3 o su un potenziale problema di sicurezza o privacy di un bucket S3 per uso generico. Ogni risultato fornisce dettagli come un indice di gravità, informazioni sulla risorsa interessata e su quando Macie ha rilevato i dati o il problema.

Macie genera due categorie di risultati: i [risultati relativi ai dati sensibili](#), per i dati sensibili rilevati da Macie negli oggetti S3, e i [risultati delle policy](#), per i potenziali problemi rilevati da Macie con le impostazioni di sicurezza e controllo degli accessi per i bucket S3. All'interno di ogni categoria, esistono tipi specifici di risultati.

Per ulteriori informazioni, consulta [Tipi di risultati](#).

ricerca di un evento

Un EventBridge evento Amazon che contiene i dettagli di una [ricerca di dati sensibili](#) o di una [policy](#).

Macie pubblica automaticamente i dati sensibili e i risultati delle politiche su Amazon EventBridge come eventi. Un evento è un oggetto JSON conforme allo schema degli EventBridge eventi. AWS È possibile utilizzare questi eventi per monitorare, elaborare e agire in base ai risultati utilizzando altre applicazioni, servizi e sistemi.

Per ulteriori informazioni, consulta [Elaborazione dei risultati con Amazon EventBridge](#) e [Schema EventBridge degli eventi di Amazon per i risultati](#).

job

Guarda il [processo di individuazione di dati sensibili](#).

identificatore di dati gestito

Un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili. Esempi di dati sensibili includono numeri di carte di credito, chiavi di accesso AWS segrete o numeri di passaporto per un determinato paese o regione. Questi identificatori sono in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili per molti paesi e regioni.

Per ulteriori informazioni, consulta [Utilizzo di identificatori di dati gestiti](#).

account membro

Un account Macie gestito dall'[account amministratore](#) Macie designato per un'organizzazione. Un'organizzazione è un insieme di account Macie associati tra loro e gestiti centralmente come gruppo di account correlati in uno specifico gruppo. Regione AWS

Un account può diventare un account membro in due modi: integrando Macie con l'organizzazione dell'account AWS Organizations o accettando un invito a iscriversi a Macie.

Se disponi di un account membro, il tuo amministratore Macie ha accesso ai dati di inventario di Amazon S3, [ai risultati delle policy](#) e ad alcune impostazioni e risorse di Macie per il tuo account.

L'amministratore può anche eseguire il rilevamento [automatico di dati sensibili ed eseguire processi di rilevamento di dati sensibili](#) per rilevare i dati sensibili nei bucket S3. Potrebbero anche essere in grado di eseguire attività aggiuntive per il tuo account, a seconda di come l'account è diventato un account membro.

Per ulteriori informazioni, consulta [Gestione di più account](#).

organizzazione

Un insieme di account Macie associati tra loro e gestiti centralmente come gruppo di account correlati in uno specifico Regione AWS.

Ogni organizzazione è composta da un [account amministratore Macie designato e da uno o più account membro](#) associati. L'account amministratore può accedere a determinate impostazioni, dati e risorse di Macie per gli account dei membri. Puoi creare un'organizzazione in due modi: integrando Macie AWS Organizations o inviando e accettando gli inviti di iscrizione in Macie.

Per ulteriori informazioni, consulta [Gestione di più account](#).

definizione delle politiche

Un rapporto dettagliato di una potenziale violazione delle policy o di un problema relativo alle impostazioni di sicurezza e controllo degli accessi per un bucket S3 per uso generico. I dettagli includono un indice di gravità, informazioni sulla risorsa interessata e su quando Macie ha riscontrato il problema.

Macie genera i risultati delle policy quando i criteri o le impostazioni di un bucket generico S3 vengono modificati in modo da ridurre la sicurezza o la privacy del bucket e degli oggetti in esso contenuti. Macie genera questi risultati nell'ambito delle sue continue attività di monitoraggio dei dati di Amazon S3. Macie può generare diversi tipi di risultati politici.

Per ulteriori informazioni, consulta [Tipi di risultati](#) e [Monitoraggio della sicurezza e della privacy dei dati](#).

esempio di reperto

Una [scoperta](#) che utilizza dati di esempio e valori segnaposto per dimostrare i tipi di informazioni che un risultato potrebbe contenere.

Per ulteriori informazioni, consulta [Lavorare con i risultati di esempio](#).

ricerca di dati sensibili

Un rapporto dettagliato sui dati sensibili che Macie ha trovato in un oggetto S3. I dettagli includono una valutazione di gravità, informazioni sulla risorsa interessata, il tipo e il numero di occorrenze dei dati sensibili trovati da Macie e quando Macie ha trovato i dati sensibili.

[Macie genera risultati sui dati sensibili se rileva dati sensibili negli oggetti S3 che analizza quando si eseguono processi di rilevamento di dati sensibili o esegue il rilevamento automatico di dati sensibili.](#)

Macie può generare diversi tipi di rilevazioni di dati sensibili.

Per ulteriori informazioni, consulta [Tipi di risultati](#) e [Rilevamento dei dati sensibili](#).

lavoro di scoperta di dati sensibili

Chiamato anche job, una serie di attività automatizzate di elaborazione e analisi eseguite da Macie per rilevare e segnalare dati sensibili negli oggetti S3. Quando crei un lavoro, specifichi la frequenza con cui desideri che il lavoro venga eseguito e definisci l'ambito e la natura dell'analisi del lavoro.

Quando un lavoro viene eseguito, Macie registra i dati sensibili che trova ([rilevamenti di dati sensibili](#)) e le analisi che esegue ([risultati della scoperta di dati sensibili](#)). Macie pubblica anche i dati di registrazione su Amazon Logs. CloudWatch

Per ulteriori informazioni, consulta [Esecuzione di processi di rilevamento dei dati sensibili](#).

risultato della scoperta di dati sensibili

Un record che registra i dettagli sull'analisi eseguita da Macie su un oggetto S3 per determinare se l'oggetto contiene dati sensibili. Macie genera e scrive questi record in file JSON Lines (.jsonl), che crittografa e archivia in un bucket S3 specificato dall'utente. I record aderiscono a uno schema standardizzato.

Quando si esegue un [processo di rilevamento di dati sensibili](#) o Macie esegue un [rilevamento automatico di dati sensibili](#), Macie crea un risultato di rilevamento di dati sensibili per ogni oggetto incluso nell'ambito dell'analisi. Questo include:

- Oggetti in cui Macie trova dati sensibili e quindi producono anche risultati su dati [sensibili](#).

- Oggetti in cui Macie non trova dati sensibili e quindi non producono risultati su dati sensibili.
- Oggetti che Macie non può analizzare a causa di errori o problemi come le impostazioni delle autorizzazioni o l'uso di un file o di un formato di archiviazione non supportato.

Per ulteriori informazioni, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

session

Una risorsa che rappresenta il servizio Macie per uno specifico in uno specifico Account AWS . Regione AWS E Account AWS può avere solo una sessione Macie in ogni regione.

Quando abiliti Macie per la prima volta, il servizio genera una sessione Macie per il tuo account nella regione corrente. Assegna inoltre un identificatore univoco a quella sessione. La sessione consente a Macie di diventare operativo per il tuo account nella Regione.

account autonomo

[Un account Macie che non è né un account amministratore né un account membro di un'organizzazione](#). L'account non fa parte di un'organizzazione.

scoperta soppressa

Un [risultato](#) che è stato archiviato automaticamente da una regola di [soppressione](#). Vale a dire, Macie ha cambiato automaticamente lo stato del risultato in archiviato perché il risultato corrispondeva ai criteri di una regola di soppressione quando Macie ha generato il risultato.

Per ulteriori informazioni, consulta [Eliminazione dei risultati](#).

regola di soppressione

[Un set di criteri di filtro basati sugli attributi che puoi creare e salvare automaticamente per archiviare \(sopprimere\) i risultati](#). Le regole di soppressione sono utili in situazioni in cui hai esaminato una classe di risultati e non desideri riceverne nuovamente una notifica.

Se sopprimi i risultati con una regola di soppressione, Macie continua a generare risultati che soddisfano i criteri della regola. Tuttavia, Macie modifica automaticamente lo stato dei risultati in

Archiviati. Ciò significa che i risultati non vengono visualizzati per impostazione predefinita sulla console Amazon Macie e Macie non li pubblica su altri. Servizi AWS

Per ulteriori informazioni, consulta [Eliminazione dei risultati](#).

byte o dimensioni non classificabili

[Nelle statistiche del bucket S3 fornite da Macie, la dimensione totale di archiviazione di tutti gli oggetti inclassificabili in un bucket S3.](#)

Se il controllo delle versioni è abilitato per un bucket, questo valore si basa sulla dimensione di archiviazione della versione più recente di ogni oggetto inclassificabile nel bucket. Se un oggetto è un file compresso, questo valore non riflette la dimensione effettiva del contenuto del file dopo la decompressione.

Per ulteriori informazioni, consulta [Revisione dell'inventario dei bucket S3](#) e [Valutazione del tuo livello di sicurezza in Amazon S3](#).

oggetto inclassificabile

Un oggetto S3 che Macie non può analizzare per rilevare dati sensibili.

Nel calcolare le statistiche del bucket S3, Macie determina che un oggetto è inclassificabile in base alla classe di archiviazione e all'estensione del nome di file dell'oggetto. Un oggetto non è classificabile se non utilizza una classe di storage Amazon S3 supportata o non ha un'estensione del nome di file per un formato di file o di storage supportato.

Per ulteriori informazioni, consulta [Revisione dell'inventario dei bucket S3](#) e [Classi e formati di archiviazione supportati](#).

Per l'individuazione di dati sensibili, Macie determina che un oggetto è inclassificabile in base alla classe di archiviazione, all'estensione del nome di file e al contenuto dell'oggetto. Un oggetto è inclassificabile se: non utilizza una classe di storage Amazon S3 supportata, non ha un'estensione del nome di file per un formato di file o storage supportato o Macie non è stato in grado di estrarre e analizzare i dati dall'oggetto. Ad esempio, l'oggetto è un file in formato errato.

Per ulteriori informazioni, consulta [Rilevamento dei dati sensibili](#) e [Classi e formati di archiviazione supportati](#).

Monitoraggio della sicurezza e della privacy dei dati con Macie

Quando abiliti Amazon Macie per il tuo Account AWS, Macie genera automaticamente e inizia a mantenere un inventario dei tuoi bucket generici Amazon Simple Storage Service (Amazon S3) S3 nella versione corrente. Regione AWS Macie inizia anche a valutare e monitorare i bucket per la sicurezza e il controllo degli accessi. Se Macie rileva un evento che riduce la sicurezza o la privacy di un bucket, Macie crea una [policy](#) da esaminare e correggere se necessario.

Per valutare e monitorare anche la presenza di dati sensibili nei bucket S3, puoi creare ed eseguire processi di rilevamento di dati sensibili. I job di rilevamento dei dati sensibili possono eseguire analisi incrementali degli oggetti bucket su base giornaliera, settimanale o mensile. Se Macie rileva dati sensibili in un oggetto S3, Macie crea una [ricerca di dati sensibili per avvisarti dei dati sensibili](#) che ha trovato. A seconda delle impostazioni del tuo account, puoi anche configurare Macie per eseguire il rilevamento automatico dei dati sensibili. L'individuazione automatica dei dati sensibili utilizza tecniche di campionamento per identificare, selezionare e analizzare continuamente gli oggetti rappresentativi presenti nei bucket. Per ulteriori informazioni su entrambe le opzioni, vedere.

[Rilevamento dei dati sensibili](#)

Macie offre inoltre una visibilità costante sulla sicurezza e sulla privacy dei dati di Amazon S3. Per valutare il livello di sicurezza dei tuoi dati e determinare dove intervenire, puoi utilizzare la dashboard di riepilogo sulla console. La dashboard fornisce un'istantanea delle statistiche aggregate per i dati di Amazon S3. Le statistiche includono dati relativi a parametri di sicurezza chiave, come il numero di bucket generici accessibili pubblicamente o condivisi con altri. Account AWS La dashboard mostra anche gruppi di dati aggregati relativi ai risultati del tuo account, ad esempio i nomi di 1-5 bucket con il maggior numero di risultati relativi ai sette giorni precedenti. Puoi approfondire ogni statistica per esaminarne i dati di supporto. Per interrogare le statistiche a livello di codice, utilizza il [GetBucketStatistics](#) funzionamento dell'API Amazon Macie.

Per un'analisi e una valutazione più approfondite, Macie fornisce informazioni e statistiche dettagliate per i singoli bucket S3 presenti nell'inventario. Ciò include le suddivisioni delle impostazioni di accesso pubblico e crittografia di ciascun bucket e la dimensione e il numero di oggetti che Macie può analizzare per rilevare i dati sensibili nel bucket. L'inventario indica anche se sono stati configurati processi di rilevamento di dati sensibili o di rilevamento automatico di dati sensibili per analizzare gli oggetti in un bucket. In caso affermativo, indica quando è stata effettuata l'analisi più recente. Puoi sfogliare, ordinare e filtrare l'inventario utilizzando la console Amazon Macie o il [DescribeBuckets](#) funzionamento dell'API Amazon Macie.

Se sei l'amministratore Macie di un'organizzazione, puoi accedere a dati statistici e di altro tipo sui bucket S3 di proprietà dei tuoi account membro. Puoi anche accedere ai risultati delle policy generati da Macie per i bucket e ispezionare i bucket per verificare la presenza di dati sensibili. Ciò significa che puoi utilizzare Macie per valutare e monitorare il livello di sicurezza generale del patrimonio di dati Amazon S3 della tua organizzazione. Per ulteriori informazioni, consulta [Gestione di più account](#).

Argomenti

- [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#)
- [Valutazione del tuo livello di sicurezza in Amazon S3 con Macie](#)
- [Analisi del livello di sicurezza di Amazon S3 con Macie](#)
- [Consentire a Macie di accedere a bucket e oggetti S3](#)

In che modo Macie monitora la sicurezza dei dati di Amazon S3

Quando abiliti Amazon Macie per il tuo account Account AWS, Macie crea un [ruolo collegato al servizio AWS Identity and Access Management](#) (IAM) per il tuo account nella versione corrente.

Regione AWS La politica di autorizzazione per questo ruolo consente a Macie di chiamare altri utenti Servizi AWS e monitorare le risorse per tuo conto. AWS Utilizzando questo ruolo, Macie genera e gestisce un inventario dei tuoi bucket generici Amazon Simple Storage Service (Amazon S3) nella regione. Macie monitora e valuta anche i bucket per la sicurezza e il controllo degli accessi.

Se sei l'amministratore Macie di un'organizzazione, l'inventario include dati statistici e di altro tipo sui bucket S3 per il tuo account e gli account dei membri dell'organizzazione. Con questi dati, puoi utilizzare Macie per monitorare e valutare il livello di sicurezza della tua organizzazione in tutto il tuo patrimonio di dati Amazon S3. Per ulteriori informazioni, consulta [Gestione di più account](#).

Argomenti

- [Componenti chiave](#)
- [Aggiornamenti dei dati](#)
- [Considerazioni](#)

Componenti chiave

Amazon Macie utilizza una combinazione di caratteristiche e tecniche per fornire e gestire i dati di inventario per i bucket generici S3 e per monitorare e valutare i bucket per motivi di sicurezza e controllo degli accessi.

Raccolta di metadati e calcolo delle statistiche

Per generare e gestire metadati e statistiche per l'inventario dei bucket, Macie recupera i metadati di bucket e oggetti direttamente da Amazon S3. Per ogni bucket, i metadati includono:

- Informazioni generali sul bucket, come il nome del bucket, Amazon Resource Name (ARN), la data di creazione, le impostazioni di crittografia, i tag e l'ID dell'account del proprietario del Account AWS bucket.
- Impostazioni delle autorizzazioni a livello di account che si applicano al bucket, come le impostazioni di blocco dell'accesso pubblico per l'account.
- Impostazioni delle autorizzazioni a livello di bucket per il bucket, ad esempio le impostazioni di blocco dell'accesso pubblico per il bucket e le impostazioni che derivano da una policy del bucket o da una lista di controllo degli accessi (ACL).
- Impostazioni di accesso e replica condivise per il bucket, incluso se i dati del bucket vengono replicati o condivisi con persone che non fanno parte dell'organizzazione. Account AWS
- Numero di oggetti e impostazioni per gli oggetti nel bucket, ad esempio il numero di oggetti nel bucket e la suddivisione del conteggio degli oggetti per tipo di crittografia, tipo di file e classe di archiviazione.

Macie ti fornisce queste informazioni direttamente. Macie utilizza le informazioni anche per calcolare statistiche e fornire valutazioni sulla sicurezza e la privacy dell'inventario complessivo dei bucket e dei singoli bucket presenti nell'inventario. Ad esempio, puoi trovare la dimensione totale di archiviazione e il numero di bucket nel tuo inventario, la dimensione totale di archiviazione e il numero di oggetti in quei bucket, nonché la dimensione totale di archiviazione e il numero di oggetti che Macie può analizzare per rilevare i dati sensibili nei bucket.

Per impostazione predefinita, i metadati e le statistiche includono i dati relativi a tutte le parti dell'oggetto esistenti a causa di caricamenti multiparte incompleti. Se aggiorni manualmente i metadati degli oggetti per un bucket specifico, Macie ricalcola le statistiche relative al bucket e all'inventario complessivo del bucket ed esclude i dati relativi alle parti dell'oggetto dai valori ricalcolati. La prossima volta che Macie recupera i metadati di bucket e oggetti da Amazon S3 come parte del ciclo di aggiornamento giornaliero, Macie aggiorna i dati dell'inventario e include nuovamente i dati per le parti dell'oggetto. Per informazioni su quando Macie recupera i metadati del bucket e dell'oggetto, consulta [Aggiornamenti dei dati](#)

È importante notare che Macie non è in grado di analizzare parti di oggetti per rilevare dati sensibili. Amazon S3 deve prima completare l'assemblaggio delle parti in uno o più oggetti affinché Macie possa analizzarle. Per informazioni sui caricamenti in più parti e sulle parti di

oggetti, incluso come eliminare le parti automaticamente con le regole del ciclo di vita, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte nella Guida per l'utente di Amazon Simple Storage Service](#). Per identificare i bucket che contengono parti di oggetti, puoi fare riferimento a metriche di caricamento multiparte incomplete in Amazon S3 Storage Lens. Per ulteriori informazioni, consulta la sezione [Valutazione dell'attività e dell'utilizzo dello storage](#) nella Guida per l'utente di Amazon Simple Storage Service.

Monitoraggio della sicurezza e della privacy dei bucket

Per garantire l'accuratezza dei dati a livello di bucket nel tuo inventario, Macie monitora e analizza determinati [AWS CloudTrail](#) eventi che possono verificarsi per i dati di Amazon S3. Se si verifica un evento rilevante, Macie aggiorna i dati di inventario appropriati.

Ad esempio, se abiliti le impostazioni di blocco dell'accesso pubblico per un bucket, Macie aggiorna tutti i dati relativi alle impostazioni di accesso pubblico del bucket. Allo stesso modo, se aggiungi o aggiorni la policy del bucket per un bucket, Macie analizza la policy e aggiorna i dati appropriati nel tuo inventario.

Se Macie stabilisce che un evento riduce la sicurezza o la privacy di un bucket, Macie crea anche una [policy](#) da esaminare e correggere se necessario.

Macie monitora e analizza i dati per i seguenti eventi: CloudTrail

- Eventi a livello di account e DeletePublicAccessBlock PutPublicAccessBlock
- Eventi a livello di bucket: CreateBucket, DeleteAccountPublicAccessBlock, DeleteBucket, DeleteBucketEncryption, DeleteBucketPolicy, DeleteBucketPublicAccessBlock,, DeleteBucketReplication, DeleteBucketTagging, PutAccountPublicAccessBlock, PutBucketAcl,, PutBucketEncryption PutBucketPolicy, e PutBucketPublicAccessBlock PutBucketReplication PutBucketTagging PutBucketVersioning

Non puoi abilitare il monitoraggio di CloudTrail eventi aggiuntivi o disabilitare il monitoraggio per nessuno degli eventi precedenti. Per informazioni dettagliate sulle operazioni corrispondenti per gli eventi precedenti, consulta l'[Amazon Simple Storage Service API Reference](#).

Tip

Per monitorare gli eventi a livello di oggetto, ti consigliamo di utilizzare la funzionalità di protezione Amazon S3 di Amazon GuardDuty. Questa funzionalità monitora gli eventi relativi ai dati di Amazon S3 a livello di oggetto e li analizza per individuare attività

dannose e sospette. Per ulteriori informazioni, consulta [GuardDuty S3 Protection](#) nella Amazon GuardDuty User Guide.

Valutazione della sicurezza e del controllo degli accessi dei bucket

Per valutare la sicurezza a livello di bucket e il controllo degli accessi, Macie utilizza un ragionamento automatizzato e basato sulla logica per analizzare le politiche basate sulle risorse che si applicano a un bucket. Macie analizza anche le impostazioni delle autorizzazioni a livello di account e bucket che si applicano a un bucket. Questa analisi tiene conto delle politiche del bucket, a livello di ACLs bucket e delle impostazioni di accesso pubblico di blocco per l'account e il bucket.

[Per le politiche basate sulle risorse, Macie utilizza Zelkova.](#) Zelkova è un motore di ragionamento automatizzato che traduce le politiche AWS Identity and Access Management (IAM) in istruzioni logiche ed esegue una suite di risolutori logici generici e specializzati (teorie dei moduli di soddisfacibilità) per risolvere il problema decisionale. [Per saperne di più sulla natura dei solutori utilizzati da Zelkova, consulta Satisfiability Modulo Theories.](#)

Macie applica ripetutamente Zelkova a una politica basata sulle risorse, utilizzando interrogazioni sempre più specifiche per caratterizzare le classi di comportamenti consentite dalla politica. L'analisi è progettata per identificare i potenziali rischi di sicurezza per i dati di Amazon S3 e ridurre al minimo i falsi negativi. Non include politiche di AWS Organizations autorizzazione che definiscono le autorizzazioni massime disponibili per le risorse dell'organizzazione, come le politiche di controllo dei servizi (SCPs) o le politiche di controllo delle risorse (). RCPs Inoltre, non include le politiche chiave per gli associati AWS KMS keys. Ad esempio, se una policy bucket utilizza la chiave di condizione [s3:x-amz-server-side-encryption-aws-kms-key-id](#) per limitare l'accesso in scrittura al bucket, Macie non analizza la policy chiave per la chiave specificata. Ciò significa che Macie potrebbe segnalare che il bucket è accessibile al pubblico, a seconda di altri componenti della policy del bucket e delle impostazioni delle autorizzazioni di Amazon S3 che si applicano al bucket.

Inoltre, quando Macie valuta la sicurezza e la privacy di un bucket, non esamina i log di accesso né analizza utenti, ruoli e altre configurazioni pertinenti per gli account. Invece, Macie analizza e riporta i dati per le impostazioni chiave che indicano potenziali rischi per la sicurezza. Ad esempio, se un risultato di una policy indica che un bucket è accessibile pubblicamente, ciò non significa necessariamente che un'entità esterna abbia avuto accesso al bucket. Allo stesso modo, se un risultato di una policy indica che un bucket è condiviso con una persona Account AWS esterna

all'organizzazione, Macie non tenta di determinare se questo accesso sia previsto e sicuro. Questi risultati indicano invece che un'entità esterna può potenzialmente accedere ai dati del bucket, il che potrebbe rappresentare un rischio involontario per la sicurezza.

Se Macie segnala che un'entità esterna può potenzialmente accedere a un bucket S3, ti consigliamo di rivedere la politica e le impostazioni del bucket per determinare se questo accesso è intenzionale e sicuro. Se applicabile, esamina anche le politiche e le impostazioni per le risorse associate, ad esempio AWS KMS keys, e le politiche di AWS Organizations autorizzazione per la tua organizzazione.

Important

Per eseguire le attività precedenti per un bucket, il bucket deve essere un bucket S3 generico. Macie non monitora né analizza i bucket di directory S3.

Inoltre, a Macie deve essere consentito l'accesso al bucket. Se le impostazioni delle autorizzazioni di un bucket impediscono a Macie di recuperare i metadati per il bucket o gli oggetti del bucket, Macie può fornire solo un sottoinsieme di informazioni sul bucket, come il nome e la data di creazione del bucket. Macie non può eseguire alcuna attività aggiuntiva per il bucket. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Macie può eseguire le attività precedenti per un massimo di 10.000 bucket per account. Se memorizzi più di 10.000 bucket in Amazon S3, Macie esegue queste attività solo per i 10.000 bucket che sono stati creati o modificati più di recente. Per tutti gli altri bucket, Macie non conserva dati di inventario completi, non valuta o monitora la sicurezza e la privacy dei dati dei bucket né genera risultati politici. Macie fornisce invece solo un sottoinsieme di informazioni sui bucket.

Aggiornamenti dei dati

Quando abiliti Amazon Macie per il tuo Account AWS, Macie recupera i metadati per i tuoi bucket e oggetti generici S3 direttamente da Amazon S3. Successivamente, Macie recupera automaticamente i metadati di bucket e oggetti direttamente da Amazon S3 su base giornaliera come parte di un ciclo di aggiornamento giornaliero.

Macie recupera anche i metadati del bucket direttamente da Amazon S3 quando si verifica una delle seguenti situazioni:

- Macie rileva un evento rilevante. AWS CloudTrail
- Puoi aggiornare i dati dell'inventario scegliendo refresh



sulla console Amazon Macie. A seconda delle dimensioni del tuo patrimonio di dati, puoi aggiornare i dati ogni cinque minuti.

- Invia una [DescribeBuckets](#) richiesta all'API Amazon Macie in modo programmatico e Macie ha terminato l'elaborazione di tutte le richieste precedenti. DescribeBuckets

Macie può anche recuperare i metadati degli oggetti più recenti per un bucket specifico se scegli di aggiornare manualmente tali dati. Questo può essere utile se hai creato di recente un bucket o hai apportato modifiche significative agli oggetti di un bucket nelle ultime 24 ore. Per aggiornare manualmente i metadati degli oggetti per un bucket, scegli refresh



nella sezione Statistiche degli oggetti del [pannello dei dettagli del bucket nella pagina dei bucket S3](#) della console. Questa funzionalità è disponibile per i bucket che memorizzano 30.000 o meno oggetti.

Per determinare quando Macie ha recuperato l'ultima volta i metadati del bucket o dell'oggetto per il tuo account, puoi fare riferimento al campo Ultimo aggiornamento sulla console. Questo campo viene visualizzato nella dashboard di riepilogo, nella pagina dei bucket S3 e nel pannello dei dettagli dei bucket [della pagina dei bucket S3](#). Se utilizzi l'API Amazon Macie per interrogare i dati di inventario, il `lastUpdated` campo fornisce queste informazioni. Se sei l'amministratore Macie di un'organizzazione, il campo indica la prima data e ora in cui Macie ha recuperato i dati per un account della tua organizzazione.

Ogni volta che Macie recupera i metadati del bucket o dell'oggetto, Macie aggiorna automaticamente i dati appropriati nel tuo inventario. Se Macie rileva differenze che influiscono sulla sicurezza o sulla privacy di un bucket, Macie inizia immediatamente a valutare e analizzare le modifiche. Una volta completata l'analisi, Macie aggiorna i dati appropriati nel tuo inventario. Se alcune differenze riducono la sicurezza o la privacy di un bucket, Macie crea anche i [risultati delle policy](#) appropriati da esaminare e correggere se necessario. Macie lo fa per un massimo di 10.000 bucket per il tuo account. Se hai più di 10.000 bucket, Macie lo fa per i 10.000 bucket che sono stati creati o modificati più di recente. Se sei l'amministratore Macie di un'organizzazione, questa quota si applica a ogni account dell'organizzazione, non all'intera organizzazione.

In rare occasioni, in determinate condizioni, la latenza e altri problemi potrebbero impedire a Macie di recuperare i metadati di bucket e oggetti. Potrebbero anche ritardare le notifiche che Macie riceve in merito alle modifiche all'inventario dei bucket o alle impostazioni e alle politiche delle autorizzazioni

per i singoli bucket. Ad esempio, i problemi di consegna relativi CloudTrail agli eventi potrebbero causare ritardi. In tal caso, Macie analizza i dati nuovi e aggiornati la prossima volta che esegue l'aggiornamento giornaliero, ovvero entro 24 ore.

Considerazioni

Quando utilizzi Amazon Macie per monitorare e valutare il livello di sicurezza dei tuoi dati Amazon S3, tieni presente quanto segue:

- I dati di inventario si applicano solo ai bucket S3 per uso generico attualmente disponibili. Regione AWS Per accedere ai dati per altre regioni, abilita e usa Macie in ogni regione aggiuntiva.
- Se sei l'amministratore Macie di un'organizzazione, puoi accedere ai dati di inventario per un account membro solo se Macie è abilitato per quell'account nella regione corrente.
- Macie può fornire dati di inventario completi per non più di 10.000 bucket per account. Inoltre, Macie può valutare e monitorare la sicurezza e la privacy di non più di 10.000 bucket per account. Se il tuo account supera questa quota, Macie valuta, monitora e fornisce informazioni dettagliate sui 10.000 bucket che sono stati creati o modificati più di recente. Per tutti gli altri bucket, Macie fornisce solo un sottoinsieme di informazioni sui bucket.

Se il tuo account si avvicina a questa quota, ti avviseremo creando un AWS Health evento per il tuo account. Inviando anche un'e-mail all'indirizzo associato al tuo account. Ti avviseremo nuovamente se il tuo account supera la quota. Se sei un amministratore di Macie, questa quota si applica a ogni account della tua organizzazione, non all'intera organizzazione.

- Se le impostazioni delle autorizzazioni di un bucket impediscono a Macie di recuperare informazioni sul bucket o sugli oggetti del bucket, Macie non può valutare e monitorare la sicurezza e la privacy dei dati del bucket o fornire informazioni dettagliate sul bucket. Per aiutarti a identificare un bucket in questo caso, Macie fa quanto segue:

- Nell'inventario dei bucket sulla console, Macie visualizza un'icona di avviso



per il bucket.

- Per i dettagli del bucket, Macie fornisce i dati solo per un sottoinsieme di campi: l'ID account del proprietario del bucket, il Account AWS nome del bucket, Amazon Resource Name (ARN), la data di creazione e la regione; e la data e l'ora in cui Macie ha recentemente recuperato i metadati del bucket e dell'oggetto per il bucket come parte del ciclo di aggiornamento giornaliero. Se esegui una query sui dati di inventario in modo programmatico con l'API Amazon Macie, Macie fornisce anche un codice di errore e un messaggio per il bucket.

- Nella dashboard di riepilogo sulla console, il bucket ha un valore Unknown per le statistiche di accesso pubblico, crittografia e condivisione. Inoltre, Macie esclude il bucket quando calcola i dati per le statistiche di Storage and Objects.
- Se si interrogano statistiche aggregate a livello di codice utilizzando l'[GetBucketStatistics](#) operazione, il bucket ha un valore pari a 4 unknown per molte statistiche e Macie lo esclude quando calcola il conteggio degli oggetti e i valori delle dimensioni di archiviazione.

Per esaminare il problema, consulta la policy e le impostazioni delle autorizzazioni del bucket in Amazon S3. Ad esempio, il bucket potrebbe avere una politica restrittiva. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

- I dati relativi all'accesso e alle autorizzazioni sono limitati alle impostazioni a livello di account e bucket. Non riflette le impostazioni a livello di oggetto che determinano l'accesso a oggetti specifici in un bucket. Ad esempio, se l'accesso pubblico è abilitato per un oggetto specifico in un bucket, Macie non segnala che il bucket o gli oggetti del bucket sono accessibili pubblicamente.

Per monitorare le operazioni a livello di oggetto e identificare potenziali rischi per la sicurezza, ti consigliamo di utilizzare la funzionalità di protezione Amazon S3 di Amazon GuardDuty. Questa funzionalità monitora gli eventi relativi ai dati di Amazon S3 a livello di oggetto e li analizza per individuare attività dannose e sospette. Per ulteriori informazioni, consulta [GuardDuty S3 Protection](#) nella Amazon GuardDuty User Guide.

- Se aggiorni manualmente i metadati degli oggetti per un bucket specifico:
 - Macie riporta temporaneamente Unknown per le statistiche di crittografia che si applicano agli oggetti. La prossima volta che Macie esegue l'aggiornamento quotidiano dei dati (entro 24 ore), Macie rivaluta i metadati di crittografia degli oggetti e riporta nuovamente i dati quantitativi per le statistiche.
 - Macie esclude temporaneamente i dati per tutte le parti dell'oggetto contenute nel bucket a causa di caricamenti incompleti in più parti. La prossima volta che Macie esegue l'aggiornamento giornaliero dei dati (entro 24 ore), Macie ricalcola i conteggi e i valori delle dimensioni di archiviazione per gli oggetti del bucket e include i dati per le parti in quei calcoli.
- In alcuni casi, Macie potrebbe non essere in grado di determinare se un bucket è accessibile pubblicamente o condiviso o richiede la crittografia lato server di nuovi oggetti. Ad esempio, un problema di quota o temporaneo potrebbe impedire a Macie di recuperare e analizzare i dati richiesti. Oppure Macie potrebbe non essere in grado di determinare con precisione se una o più dichiarazioni politiche concedono l'accesso a un'entità esterna. In questi casi, Macie riporta

Unknown per le statistiche e i campi pertinenti nell'inventario dei desideri. Per esaminare questi casi, consulta la policy e le impostazioni delle autorizzazioni del bucket in Amazon S3.

Tieni inoltre presente che Macie genera i risultati delle policy solo se la sicurezza o la privacy di un bucket vengono ridotte dopo aver abilitato Macie per il tuo account. Ad esempio, se disabiliti le impostazioni di blocco dell'accesso pubblico per un bucket dopo aver abilitato Macie, Macie genera una ricerca Policy: IAMUser /S3 per il bucket. BlockPublicAccessDisabled Tuttavia, se le impostazioni di blocco dell'accesso pubblico sono state disabilitate per un bucket quando hai abilitato Macie e continuano a esserlo, Macie non genera una ricerca Policy: /S3 per il bucket. IAMUser BlockPublicAccessDisabled

Valutazione del tuo livello di sicurezza in Amazon S3 con Macie

Per valutare lo stato di sicurezza generale dei dati di Amazon Simple Storage Service (Amazon S3) e determinare dove intervenire, puoi utilizzare la dashboard di riepilogo sulla console Amazon Macie.

La dashboard di riepilogo fornisce un'istantanea delle statistiche aggregate per i dati di Amazon S3 nella versione corrente. Regione AWS Le statistiche includono dati relativi a parametri di sicurezza chiave, come il numero di bucket generici accessibili pubblicamente o condivisi con altri. Account AWS La dashboard mostra anche gruppi di dati aggregati relativi ai risultati dell'account, ad esempio i tipi di risultati che hanno avuto il maggior numero di ricorrenze nei sette giorni precedenti. Se sei l'amministratore Macie di un'organizzazione, la dashboard fornisce statistiche e dati aggregati per tutti gli account dell'organizzazione. Puoi facoltativamente filtrare i dati per account.

Per eseguire un'analisi più approfondita, puoi approfondire ed esaminare i dati di supporto per i singoli elementi della dashboard. Puoi anche [rivedere e analizzare l'inventario dei bucket S3](#) utilizzando la console Amazon Macie oppure interrogare e analizzare i dati di inventario in modo programmatico utilizzando il funzionamento [DescribeBuckets](#) dell'API Amazon Macie.

Argomenti

- [Visualizzazione del pannello di riepilogo](#)
- [Comprensione dei componenti della dashboard di riepilogo](#)
- [Comprensione delle statistiche sulla sicurezza dei dati nella dashboard di riepilogo](#)

Visualizzazione del pannello di riepilogo

Sulla console Amazon Macie, la dashboard di riepilogo fornisce un'istantanea delle statistiche aggregate e dei dati dei risultati per i dati di Amazon S3 nella versione corrente. Regione AWS Se preferisci interrogare le statistiche a livello di codice, puoi utilizzare il [GetBucketStatistics](#) funzionamento dell'API Amazon Macie.

Per visualizzare la dashboard di riepilogo

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, scegli Riepilogo. Macie visualizza la dashboard di riepilogo.
3. Per determinare quando Macie ha recuperato l'ultima volta i metadati del bucket o dell'oggetto da Amazon S3 per il tuo account, consulta il campo Ultimo aggiornamento nella parte superiore della dashboard. Per ulteriori informazioni, consulta [Aggiornamenti dei dati](#).
4. Per approfondire ed esaminare i dati di supporto per un elemento sulla dashboard, scegli l'elemento.

Se sei l'amministratore Macie di un'organizzazione, la dashboard mostra statistiche e dati aggregati per il tuo account e gli account dei membri dell'organizzazione. Per filtrare la dashboard e visualizzare i dati solo per un determinato account, inserisci l'ID dell'account nella casella Account sopra la dashboard.

Comprensione dei componenti della dashboard di riepilogo

Nella dashboard di riepilogo, le statistiche e i dati sono organizzati in diverse sezioni. Nella parte superiore della dashboard, troverai statistiche aggregate che indicano la quantità di dati archiviata in Amazon S3 e la quantità di dati che Amazon Macie può analizzare per rilevare dati sensibili. Puoi anche fare riferimento al campo Ultimo aggiornamento per determinare quando Macie ha recuperato l'ultima volta i metadati del bucket o dell'oggetto da Amazon S3 per il tuo account. Le sezioni aggiuntive forniscono statistiche e dati sui risultati recenti che possono aiutarti a valutare la sicurezza, la privacy e la sensibilità dei tuoi dati Amazon S3 nella versione attuale. Regione AWS

Le statistiche e i dati sono organizzati nelle seguenti sezioni:

[Storage e rilevamento di dati sensibili](#) | [Problemi di rilevamento e copertura automatizzati](#) | [Sicurezza dei dati](#) | [Principali bucket S3](#) | [Principali tipi di ricerca](#) | [Risultati delle policy](#)

Mentre esamini ogni sezione, opzionalmente scegli un elemento per approfondire ed esaminare i dati di supporto. Tieni inoltre presente che la dashboard non include i dati per i bucket di directory S3, ma solo i bucket per uso generico. Macie non monitora né analizza i bucket di directory.

Archiviazione e individuazione di dati sensibili

Nella parte superiore della dashboard, le statistiche indicano la quantità di dati archiviata in Amazon S3 e la quantità di dati che Macie può analizzare per rilevare dati sensibili. L'immagine seguente mostra un esempio di queste statistiche per un'organizzazione con sette account.

Total accounts	Storage (classifiable/total)	Objects (classifiable/total)
7	307.7 GB / 313.4 GB	626.3 k / 633.0 k

Le statistiche individuali in questa sezione sono:

- **Account totali:** questo campo viene visualizzato se sei l'amministratore Macie di un'organizzazione o hai un account Macie autonomo. Indica il numero totale di Account AWS bucket personali presenti nel tuo inventario di bucket. Se sei un amministratore Macie, questo è il numero totale di account Macie che gestisci per la tua organizzazione. Se hai un account Macie indipendente, questo valore è 1.

Bucket S3 totali: questo campo viene visualizzato se disponi di un account membro in un'organizzazione. Indica il numero totale di bucket generici presenti nel tuo inventario, inclusi i bucket che non contengono oggetti.

- **Archiviazione:** queste statistiche forniscono informazioni sulla dimensione di archiviazione degli oggetti nel tuo inventario bucket:
 - **Classificabile:** la dimensione totale di archiviazione di tutti gli oggetti che Macie può analizzare nei bucket.
 - **Totale:** la dimensione totale di archiviazione di tutti gli oggetti nei bucket, inclusi gli oggetti che Macie non può analizzare.

Se uno qualsiasi degli oggetti è un file compresso, questi valori non riflettono la dimensione effettiva di quei file dopo la decompressione. Se il controllo delle versioni è abilitato per uno qualsiasi dei bucket, questi valori si basano sulla dimensione di archiviazione della versione più recente di ogni oggetto in quei bucket.

- **Oggetti:** queste statistiche forniscono informazioni sul numero di oggetti presenti nell'inventario dei bucket:
 - **Classificabile:** il numero totale di oggetti che Macie può analizzare nei bucket.

- **Totale:** il numero totale di oggetti nei bucket, inclusi gli oggetti che Macie non può analizzare.

Nelle statistiche precedenti, i dati e gli oggetti sono classificabili se utilizzano una classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un file o un formato di storage supportato. È possibile rilevare dati sensibili negli oggetti utilizzando Macie. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).

Tieni presente che le statistiche di Storage and Objects non includono dati sugli oggetti nei bucket a cui Macie non può accedere. Ad esempio, oggetti nei bucket che hanno politiche restrittive sui bucket. Per identificare i bucket in cui ciò si verifica, puoi [esaminare il tuo inventario dei bucket utilizzando la tabella dei bucket S3](#). Se l'icona di avviso

() appare accanto al nome di un bucket, a Macie non è consentito accedere al bucket.

Problemi di rilevamento e copertura automatizzati

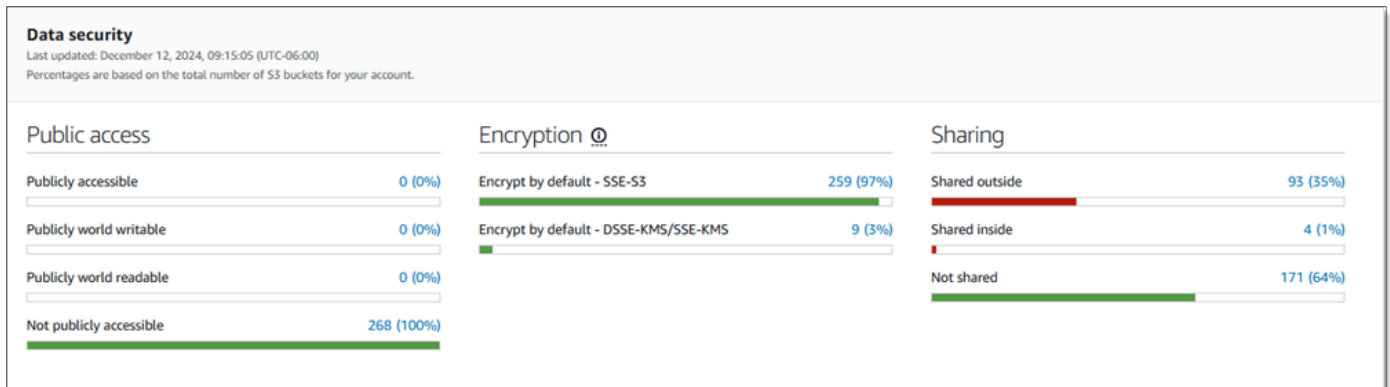
Se il rilevamento automatico dei dati sensibili è abilitato, queste sezioni vengono visualizzate nella dashboard. Acquisiscono lo stato e i risultati delle attività automatizzate di rilevamento di dati sensibili che Macie ha svolto finora per i tuoi dati Amazon S3. L'immagine seguente mostra un esempio delle statistiche fornite da queste sezioni.



Per informazioni dettagliate su queste statistiche, vedere [Revisione delle statistiche sulla sensibilità dei dati nella dashboard di riepilogo](#).

Sicurezza dei dati

Questa sezione fornisce statistiche che indicano potenziali rischi per la sicurezza e la privacy dei dati di Amazon S3. L'immagine seguente mostra un esempio delle statistiche contenute in questa sezione.



Per informazioni dettagliate su queste statistiche, vedere [Comprensione delle statistiche sulla sicurezza dei dati nella dashboard di riepilogo](#).

I migliori bucket S3

Questa sezione elenca i bucket S3 che hanno generato il maggior numero di risultati di qualsiasi tipo nei sette giorni precedenti, per un massimo di cinque bucket. Indica anche il numero di risultati che Macie ha creato per ogni bucket. L'immagine seguente mostra un esempio dei dati forniti da questa sezione.

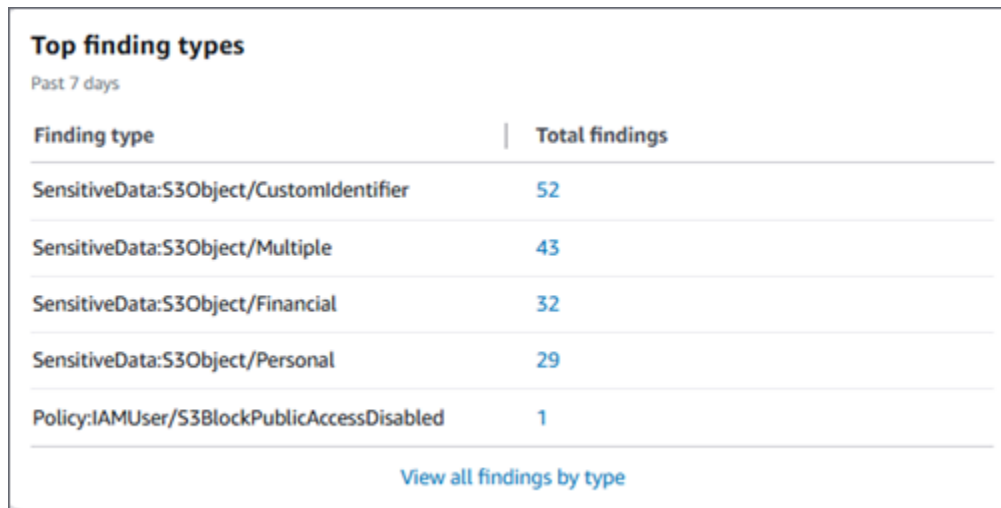
Top S3 buckets	
Past 7 days	
S3 Bucket	Total findings
amzn-s3-demo-bucket1	302
amzn-s3-demo-bucket2	33
amzn-s3-demo-bucket3	11
amzn-s3-demo-bucket4	7
amzn-s3-demo-bucket5	2
View all findings by bucket	

Per visualizzare e, facoltativamente, approfondire tutti i risultati di un bucket per i sette giorni precedenti, scegli il valore nel campo Risultati totali. Per visualizzare tutti i risultati correnti per tutti i tuoi bucket, raggruppati per bucket, scegli Visualizza tutti i risultati per bucket.

Questa sezione è vuota se Macie non ha creato alcun risultato nei sette giorni precedenti. [Oppure tutti i risultati creati nei sette giorni precedenti sono stati soppressi da una regola di soppressione.](#)

Principali tipi di ricerca

Questa sezione elenca i [tipi di risultati](#) che hanno avuto il maggior numero di ricorrenze nei sette giorni precedenti, per un massimo di cinque tipi di risultati. Indica anche il numero di risultati creati da Macie per ogni tipo. L'immagine seguente mostra un esempio dei dati forniti da questa sezione.



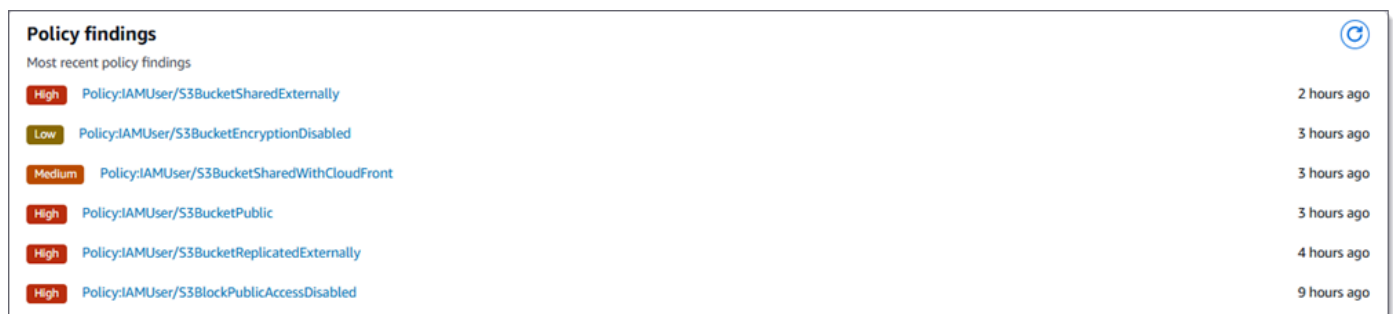
Finding type	Total findings
SensitiveData:S3Object/CustomIdentifier	52
SensitiveData:S3Object/Multiple	43
SensitiveData:S3Object/Financial	32
SensitiveData:S3Object/Personal	29
Policy:IAMUser/S3BlockPublicAccessDisabled	1

Per visualizzare e, facoltativamente, approfondire tutti i risultati di un particolare tipo relativi ai sette giorni precedenti, scegli il valore nel campo Risultati totali. Per visualizzare tutti i risultati correnti, raggruppati per tipo di risultato, scegli Visualizza tutti i risultati per tipo.

Questa sezione è vuota se Macie non ha creato alcun risultato nei sette giorni precedenti. [Oppure tutti i risultati creati nei sette giorni precedenti sono stati soppressi da una regola di soppressione.](#)

Risultati delle politiche

Questa sezione elenca i [risultati politici](#) che Macie ha creato o aggiornato più di recente, per un massimo di dieci risultati. L'immagine seguente mostra un esempio dei dati forniti da questa sezione.



High	Policy:IAMUser/S3BucketSharedExternally	2 hours ago
Low	Policy:IAMUser/S3BucketEncryptionDisabled	3 hours ago
Medium	Policy:IAMUser/S3BucketSharedWithCloudFront	3 hours ago
High	Policy:IAMUser/S3BucketPublic	3 hours ago
High	Policy:IAMUser/S3BucketReplicatedExternally	4 hours ago
High	Policy:IAMUser/S3BlockPublicAccessDisabled	9 hours ago

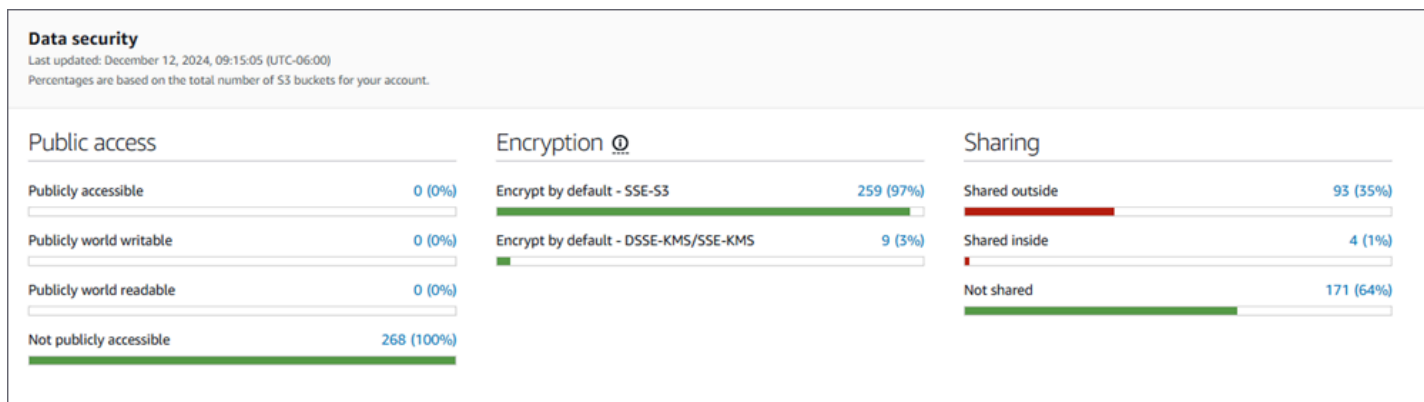
Per visualizzare i dettagli di una particolare scoperta, scegliete la scoperta.

Questa sezione è vuota se Macie non ha creato o aggiornato alcun risultato relativo alle politiche nei sette giorni precedenti. [Oppure tutti i risultati delle policy creati o aggiornati nei sette giorni precedenti sono stati eliminati da una regola di soppressione.](#)

Comprensione delle statistiche sulla sicurezza dei dati nella dashboard di riepilogo

La sezione Sicurezza dei dati della dashboard di riepilogo fornisce statistiche che possono aiutarti a identificare e analizzare i potenziali rischi per la sicurezza e la privacy per i tuoi dati Amazon S3 nel momento corrente. Regione AWS Ad esempio, puoi utilizzare questi dati per identificare bucket generici accessibili pubblicamente o condivisi con altri. Account AWS

Se l'individuazione automatica dei dati sensibili è disattivata, [le statistiche relative allo storage e all'individuazione di dati sensibili](#) nella parte superiore di questa sezione indicano la quantità di dati archiviata in Amazon S3 e la quantità di dati che Amazon Macie può analizzare per rilevare dati sensibili. Le statistiche aggiuntive sono organizzate in tre aree, come mostrato nell'immagine seguente.



Quando esaminate ogni area, opzionalmente scegliete un elemento per approfondire e rivedere i dati di supporto. Tieni inoltre presente che le statistiche non includono i dati per i bucket di directory S3, ma solo i bucket per uso generico. Macie non monitora né analizza i bucket di directory.

Le statistiche individuali in ogni area sono le seguenti.

Accesso pubblico

Queste statistiche indicano quanti bucket S3 sono o non sono accessibili al pubblico:

- **Accessibile pubblicamente:** il numero e la percentuale di bucket che consentono al pubblico in generale di avere accesso in lettura o scrittura al bucket.

- Pubblicamente scrivibile in tutto il mondo: il numero e la percentuale di bucket che consentono al pubblico di avere accesso in scrittura al bucket.
- Leggibile pubblicamente da tutto il mondo: il numero e la percentuale di bucket che consentono al pubblico di avere accesso in lettura al bucket.
- Non accessibile pubblicamente: il numero e la percentuale di bucket che non consentono al pubblico di accedere in lettura o scrittura al bucket.

Per calcolare ogni percentuale, Macie divide il numero di bucket applicabili per il numero totale di bucket presenti nell'inventario dei bucket.

Per determinare i valori in quest'area, Macie analizza una combinazione di impostazioni a livello di account e bucket per ogni bucket: le impostazioni di blocco dell'accesso pubblico per l'account, le impostazioni di blocco dell'accesso pubblico per il bucket, la politica del bucket per il bucket e l'elenco di controllo degli accessi (ACL) per il bucket. Per informazioni su queste impostazioni, consulta [Controllo degli accessi](#) e [Blocco dell'accesso pubblico allo storage Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

In alcuni casi, l'area di accesso pubblico mostra anche i valori per Unknown. Se compaiono questi valori, Macie non è stata in grado di valutare le impostazioni di accesso pubblico per il numero e la percentuale di bucket specificati. Ad esempio, un problema temporaneo o le impostazioni delle autorizzazioni dei bucket hanno impedito a Macie di recuperare i dati richiesti. Oppure Macie non è stato in grado di determinare con certezza se una o più dichiarazioni politiche consentano a un'entità esterna di accedere ai bucket. Questo può valere anche per i bucket che superano la quota per il monitoraggio del controllo preventivo. Macie valuta e monitora la sicurezza e la privacy di non più di 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente.

Encryption (Crittografia)

Queste statistiche indicano quanti bucket S3 sono configurati per applicare determinati tipi di crittografia lato server agli oggetti che vengono aggiunti ai bucket:

- Crittografia per impostazione predefinita — SSE-S3: il numero e la percentuale di bucket le cui impostazioni di crittografia predefinite sono configurate per crittografare nuovi oggetti con una chiave gestita di Amazon S3. Per questi bucket, i nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia SSE-S3.
- Crittografia per impostazione predefinita — DSSE-KMS/SSE-KMS — Il numero e la percentuale di bucket le cui impostazioni di crittografia predefinite sono configurate per crittografare nuovi oggetti con una chiave o una chiave gestita dal cliente. AWS KMS key Chiave gestita da

AWS Per questi bucket, i nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia DSSE-KMS o SSE-KMS.

Per calcolare ogni percentuale, Macie divide il numero di bucket applicabili per il numero totale di bucket presenti nell'inventario dei bucket.

Per determinare i valori in quest'area, Macie analizza le impostazioni di crittografia predefinite per ogni bucket. A partire dal 5 gennaio 2023, Amazon S3 applica automaticamente la crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per gli oggetti che vengono aggiunti ai bucket. Facoltativamente, puoi configurare le impostazioni di crittografia predefinite di un bucket per utilizzare invece la crittografia lato server con una chiave (SSE-KMS) o la crittografia lato server a doppio livello con una AWS KMS chiave (DSSE-KMS). AWS KMS Per informazioni sulle impostazioni e le opzioni di crittografia predefinite, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket S3 nella](#) Amazon Simple Storage Service User Guide.

In alcuni casi, l'area Crittografia mostra anche i valori per Unknown. Se compaiono questi valori, Macie non è stata in grado di valutare le impostazioni di crittografia predefinite per il numero e la percentuale di bucket specificati. Ad esempio, un problema temporaneo o le impostazioni delle autorizzazioni dei bucket hanno impedito a Macie di recuperare i dati richiesti. Oppure i bucket superano la quota per il monitoraggio del controllo preventivo. Macie valuta e monitora la sicurezza e la privacy di non più di 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente.

Condivisione

Queste statistiche indicano quanti bucket S3 sono o non sono condivisi con altre identità di accesso di CloudFront origine di Account AWS Amazon (OAIs) o controlli di accesso di CloudFront origine (): OACs

- Condivisi all'esterno: il numero e la percentuale di bucket condivisi con uno o più dei seguenti elementi o una combinazione dei seguenti elementi: un CloudFront OAI, un CloudFront OAC o un account che non fa parte della stessa organizzazione.
- Condivisi all'interno: il numero e la percentuale di bucket condivisi con uno o più account della stessa organizzazione. Questi bucket non sono condivisi con CloudFront OAIs o. OACs
- Non condivisi: il numero e la percentuale di bucket che non sono condivisi con altri account CloudFront OAIs, o. CloudFront OACs

Per calcolare ogni percentuale, Macie divide il numero di bucket applicabili per il numero totale di bucket presenti nell'inventario dei bucket.

Per determinare se i bucket sono condivisi con altri Account AWS, Macie analizza la policy dei bucket e l'ACL per ogni bucket. Inoltre, un'organizzazione è definita come un insieme di account Macie gestiti centralmente come gruppo di account correlati tramite o su invito di Macie. AWS Organizations Per informazioni sulle opzioni di Amazon S3 per la condivisione dei bucket, consulta il [controllo degli accessi](#) nella Guida per l'utente di Amazon Simple Storage Service.

Note

In alcuni casi, Macie potrebbe segnalare erroneamente che un bucket è condiviso con un utente Account AWS che non fa parte della stessa organizzazione.

Ciò può verificarsi se Macie non è in grado di valutare appieno la relazione tra l'Principalelemento della policy di un bucket e determinate chiavi di [contesto della condizione AWS globale o le chiavi](#) di [condizione di Amazon S3](#) nell'elemento

Condition della policy. Questo può essere il caso delle seguenti chiavi di condizione:aws:PrincipalAccount,aws:PrincipalArn,aws:PrincipalOrgID,aws:PrincipalSourceVpc,aws:SourceVpc,aws:SourceVpc:aws:userid, s3:DataAccessPointAccount e. s3:DataAccessPointArn

Per determinare se questo è il caso dei singoli bucket, scegli la statistica esterna condivisa nella dashboard. Nella tabella che appare, annota il nome di ogni bucket. Quindi usa Amazon S3 per rivedere la politica di ogni bucket e determinare se le impostazioni di accesso condiviso sono intenzionali e sicure.

Per determinare se i bucket sono condivisi con CloudFront OAls o OACs, Macie analizza la policy relativa ai bucket per ogni bucket. Un CloudFront OAI o OAC consente agli utenti di accedere agli oggetti di un bucket tramite una o più distribuzioni specifiche. CloudFront Per informazioni su CloudFront OAls e OACs, consulta la sezione [Restrizione dell'accesso a un'origine Amazon S3](#) nella CloudFront Amazon Developer Guide.

In alcuni casi, l'area Condivisione mostra anche i valori per Unknown. Se compaiono questi valori, Macie non è stata in grado di determinare se il numero e la percentuale di bucket specificati sono condivisi con altri account CloudFront OAls, oppure. CloudFront OACs Ad esempio, un problema temporaneo o le impostazioni delle autorizzazioni dei bucket hanno impedito a Macie di recuperare i dati richiesti. Oppure Macie non è stato in grado di valutare appieno le politiche dei bucket o. ACLs Questo può valere anche per i bucket che superano la quota per il monitoraggio del controllo preventivo. Macie valuta e monitora la sicurezza e la privacy di non più di 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente.

Analisi del livello di sicurezza di Amazon S3 con Macie

Per aiutarti a eseguire analisi approfondite e valutare il livello di sicurezza dei tuoi dati Amazon Simple Storage Service (Amazon S3), Amazon Macie genera e mantiene un inventario dei tuoi bucket S3 per uso generico in ognuno dei quali utilizzi Macie. Regione AWS Per scoprire come Macie gestisce questo inventario per te, consulta. [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#) Se sei l'amministratore Macie di un'organizzazione, l'inventario include i dati per i bucket S3 di proprietà dei tuoi account membro.

Utilizzando questo inventario, puoi esaminare il tuo patrimonio di dati Amazon S3 ed esaminare dettagli e statistiche per le impostazioni e i parametri di sicurezza chiave che si applicano ai singoli bucket S3. Ad esempio, puoi accedere alle suddivisioni delle impostazioni di accesso pubblico e crittografia di ogni bucket e alle dimensioni e al numero di oggetti che Macie può analizzare per rilevare i dati sensibili in ogni bucket. Puoi anche determinare se hai configurato processi di rilevamento di dati sensibili o di rilevamento automatico di dati sensibili per analizzare gli oggetti in un bucket. In caso affermativo, i dati dell'inventario indicano quando è stata effettuata l'ultima analisi. Se il rilevamento automatico dei dati sensibili è abilitato, puoi anche utilizzare l'inventario per esaminare i risultati delle attività di rilevamento automatico di dati sensibili che Macie ha svolto finora per i tuoi dati Amazon S3. Per ulteriori informazioni, consulta [Rilevamento dei dati sensibili](#).

Puoi sfogliare e filtrare i dati di inventario utilizzando la pagina dei bucket S3 sulla console Amazon Macie. Puoi anche accedere ai dati dell'inventario in modo programmatico utilizzando il [DescribeBuckets](#) funzionamento dell'API Amazon Macie.

Argomenti

- [Analisi dell'inventario dei bucket S3 in Macie](#)
- [Filtrare l'inventario dei bucket S3 in Macie](#)

Analisi dell'inventario dei bucket S3 in Macie

Sulla console Amazon Macie, la pagina dei bucket S3 fornisce informazioni dettagliate sulla sicurezza e la privacy dei dati correnti di Amazon Simple Storage Service (Amazon S3). Regione AWS Con questa pagina, puoi rivedere e analizzare un inventario dei tuoi bucket S3 generici nella regione e consultare informazioni e statistiche dettagliate per i singoli bucket. Per informazioni su come Macie genera e gestisce questo inventario, consulta. [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#) Se sei l'amministratore Macie di un'organizzazione, il tuo inventario include dettagli e statistiche per i bucket S3 di proprietà dei tuoi account membro.

La pagina dei bucket S3 indica anche quando Macie ha recentemente recuperato i metadati del bucket o dell'oggetto da Amazon S3 per il tuo account. Puoi trovare queste informazioni nel campo Ultimo aggiornamento nella parte superiore della pagina. Se sei l'amministratore Macie di un'organizzazione, questo campo indica la prima data e ora in cui Macie ha recuperato i dati per un account della tua organizzazione. Per ulteriori informazioni, consulta [Aggiornamenti dei dati](#).

Tieni presente che i dati e le statistiche di inventario non includono i dati sui bucket di directory S3, ma solo i bucket per uso generico. Macie non monitora né analizza i bucket di directory. Inoltre, Macie conserva dati di inventario completi per non più di 10.000 bucket generici per account. Se il tuo account supera questa quota, Macie fornisce dati di inventario completi per i 10.000 bucket che sono stati creati o modificati più di recente. Per tutti gli altri bucket, Macie fornisce solo un sottoinsieme di informazioni su ciascun bucket. Se sei l'amministratore Macie di un'organizzazione, questa quota si applica a ogni account dell'organizzazione, non all'intera organizzazione.

Tieni inoltre presente che la maggior parte dei dati di inventario è limitata ai bucket a cui Macie può accedere per il tuo account. Se le impostazioni delle autorizzazioni di un bucket impediscono a Macie di recuperare informazioni sul bucket o sugli oggetti del bucket, Macie può fornire solo un sottoinsieme di informazioni sul bucket. Se questo è il caso di un bucket particolare, Macie visualizza un'icona di avviso (⚠) e un messaggio per il bucket presente nell'inventario dei bucket.



Per i dettagli del bucket, Macie fornisce i dati solo per un sottoinsieme di campi: l'ID dell'account del proprietario del bucket, il Account AWS nome del bucket, Amazon Resource Name (ARN), la data di creazione e la regione; e l'ultima data in cui Macie ha recuperato i metadati del bucket e dell'oggetto per il bucket come parte del ciclo di aggiornamento giornaliero. Per esaminare il problema, consulta la policy e le impostazioni delle autorizzazioni del bucket in Amazon S3. Ad esempio, il bucket potrebbe avere una politica restrittiva. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Se preferisci accedere e interrogare i dati dell'inventario in modo programmatico, puoi utilizzare il [DescribeBuckets](#) funzionamento dell'API Amazon Macie.

Argomenti

- [Revisione dell'inventario dei bucket S3](#)
- [Analisi dei dettagli dei bucket S3](#)

Revisione dell'inventario dei bucket S3

La pagina dei bucket S3 sulla console Amazon Macie fornisce informazioni sui bucket S3 per uso generico attualmente in uso. Regione AWS In questa pagina, una tabella mostra le informazioni di riepilogo per ogni bucket dell'inventario. Per personalizzare la visualizzazione, puoi ordinare e filtrare la tabella. Se scegli un bucket nella tabella, il pannello dei dettagli mostra informazioni aggiuntive sul bucket. Ciò include dettagli e statistiche per impostazioni e metriche che forniscono informazioni sulla sicurezza e la privacy dei dati del bucket. Facoltativamente, puoi esportare i dati dalla tabella in un file con valori separati da virgole (CSV).

Se il rilevamento automatico dei dati sensibili è abilitato, hai anche la possibilità di rivedere l'inventario utilizzando una mappa termica interattiva. La mappa fornisce una rappresentazione visiva della sensibilità dei dati in tutto il tuo patrimonio di dati Amazon S3. Cattura i risultati delle attività automatizzate di scoperta di dati sensibili che Macie ha svolto finora. Per maggiori informazioni su questa mappa, vedi. [Visualizzazione della sensibilità dei dati con la mappa dei bucket S3](#)

Per esaminare l'inventario dei bucket S3

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra l'inventario dei bucket. Se la pagina mostra una mappa interattiva del tuo inventario, scegli table



) nella parte superiore della pagina. Macie mostra quindi il numero di secchi nel tuo inventario e una tabella dei periodi.

Se il rilevamento automatico dei dati sensibili è abilitato, la visualizzazione predefinita non mostra i dati per i bucket attualmente esclusi dal rilevamento automatico. Per visualizzare questi dati, scegli X nel campo È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Nella parte superiore della pagina, scegli facoltativamente refresh



) per recuperare i metadati del bucket più recenti da Amazon S3.

Se l'icona delle informazioni



) appare accanto ai nomi dei bucket, ti consigliamo di farlo. [Questa icona indica che un bucket è stato creato nelle ultime 24 ore, probabilmente dopo l'ultima volta che Macie ha recuperato](#)

[i metadati del bucket e dell'oggetto da Amazon S3 come parte del ciclo di aggiornamento giornaliero.](#)

4. Nella tabella dei bucket S3, esamina un sottoinsieme di informazioni su ogni bucket del tuo inventario:
- Sensibilità: il punteggio di sensibilità attuale del bucket, se il rilevamento automatico dei dati sensibili è abilitato. Per informazioni sulla gamma di punteggi di sensibilità definiti da Macie, consulta [Punteggio di sensibilità per i bucket S3](#)
 - Bucket: il nome del bucket.
 - Account: l'ID dell'account Account AWS che possiede il bucket.
 - Oggetti classificabili: il numero totale di oggetti che Macie può analizzare per rilevare i dati sensibili nel bucket.
 - Dimensioni classificabili: la dimensione totale di archiviazione di tutti gli oggetti che Macie può analizzare per rilevare i dati sensibili nel bucket.

Tieni presente che questo valore non riflette le dimensioni effettive degli oggetti compressi dopo la decompressione. Inoltre, se il controllo delle versioni è abilitato per il bucket, questo valore si basa sulla dimensione di archiviazione della versione più recente di ogni oggetto nel bucket.

- Monitoraggio per processo: indipendentemente dal fatto che tu abbia configurato processi di rilevamento di dati sensibili per analizzare periodicamente gli oggetti nel bucket su base giornaliera, settimanale o mensile.

Se il valore di questo campo è Sì, il bucket viene incluso in modo esplicito in un processo periodico oppure il bucket corrisponde ai criteri per un processo periodico nelle ultime 24 ore. Inoltre, lo stato di almeno uno di questi lavori non è Annullato. Macie aggiorna questi dati su base giornaliera.

- Ultimo processo eseguito: se hai configurato un processo di rilevamento di dati sensibili periodico o una tantum per analizzare gli oggetti nel bucket, questo campo indica la data e l'ora più recenti in cui uno di questi processi ha iniziato a essere eseguito. Altrimenti, in questo campo viene visualizzato un trattino (—).

Nei dati precedenti, gli oggetti sono classificabili se utilizzano una classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un formato di file o di storage supportato. È possibile rilevare dati sensibili negli oggetti utilizzando Macie. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).

5. Per analizzare l'inventario utilizzando la tabella, esegui una delle seguenti operazioni:
 - Per ordinare la tabella in base a un campo specifico, scegli l'intestazione di colonna del campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna.
 - Per filtrare la tabella e visualizzare solo i bucket che hanno un valore specifico per un campo, posiziona il cursore nella casella del filtro, quindi aggiungi una condizione di filtro per il campo. Per rifinire ulteriormente i risultati, aggiungi condizioni di filtro per campi aggiuntivi. Per ulteriori informazioni, consulta [Filtrare l'inventario dei bucket S3](#).
6. Per esaminare i dettagli e le statistiche per un determinato bucket, scegli il nome del bucket nella tabella, quindi consulta il pannello dei dettagli.

 Tip

Puoi eseguire il pivot e approfondire molti campi nel pannello dei dettagli del bucket. Per mostrare i bucket che hanno lo stesso valore per un campo, scegli nel campo.



Per mostrare i bucket che hanno altri valori per un campo, scegli



nel campo.

7. Per esportare i dati dalla tabella in un file CSV, seleziona la casella di controllo per ogni riga che desideri esportare oppure seleziona la casella di controllo nell'intestazione della colonna di selezione per selezionare tutte le righe. Quindi scegli Esporta in CSV nella parte superiore della pagina. Puoi esportare fino a 50.000 righe dalla tabella.

Analisi dei dettagli dei bucket S3

Per esaminare i dettagli e le statistiche per un bucket S3 generico, puoi utilizzare il pannello dei dettagli nella pagina dei bucket S3 della console Amazon Macie. Il pannello mostra dettagli e statistiche che forniscono informazioni sulla sicurezza e la privacy dei dati di un bucket.

Ad esempio, puoi esaminare le suddivisioni delle impostazioni di accesso pubblico di un bucket S3 e determinare se un bucket è configurato per replicare oggetti o è condiviso con altri. Account AWS Puoi anche determinare se hai configurato processi di rilevamento di dati sensibili per ispezionare il bucket alla ricerca di dati sensibili. In caso affermativo, è possibile accedere ai dettagli sul job eseguito più di recente e, facoltativamente, visualizzare tutti i risultati prodotti dal lavoro.

Se l'individuazione automatica dei dati sensibili è abilitata, puoi anche utilizzare il pannello dei dettagli per esaminare le statistiche sull'individuazione dei dati sensibili e altre informazioni sui singoli bucket S3. Il pannello acquisisce i risultati delle attività automatizzate di rilevamento di dati sensibili che Macie ha svolto finora per un sacco di tempo. Per ulteriori informazioni su questi dettagli, consulta.

[Revisione dei dettagli sulla sensibilità dei dati per i bucket S3](#)

Per esaminare i dettagli di un bucket S3

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra l'inventario dei bucket.

Se il rilevamento automatico dei dati sensibili è abilitato, la visualizzazione predefinita non mostra i dati per i bucket attualmente esclusi dal rilevamento automatico. Per visualizzare questi dati, scegli X nel campo È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Nella parte superiore della pagina, scegli facoltativamente refresh



per recuperare i metadati del bucket più recenti da Amazon S3.

4. Scegli il bucket di cui desideri esaminare i dettagli. Il pannello dei dettagli mostra statistiche e altre informazioni sul bucket.

Nel pannello dei dettagli, le statistiche e le informazioni sono organizzate nelle seguenti sezioni principali:

[Panoramica](#) | [Statistiche sugli oggetti](#) | [Crittografia lato server](#) | [Rilevamento di dati sensibili](#) | [Accesso pubblico](#) | [Replica](#) | [Tag](#)

Mentre esami le informazioni contenute in ogni sezione, puoi facoltativamente eseguire operazioni di pivot e approfondire determinati campi. Per mostrare i bucket che hanno lo stesso valore per un campo, scegli nel campo.



Per mostrare i bucket che hanno altri valori per un campo, scegli



nel campo.

Panoramica

Questa sezione fornisce informazioni generali sul bucket, come il nome del bucket, la data di creazione del bucket e l'ID dell'account del bucket Account AWS che possiede il bucket. In particolare, il campo Ultimo aggiornamento indica l'ultima data in cui Macie ha recuperato i metadati da Amazon S3 per il bucket o gli oggetti del bucket.

Il campo Accesso condiviso indica se il bucket è condiviso con un altro bucket Account AWS, un Amazon CloudFront Origin Access Identity (OAI) o un CloudFront Origin Access Control (OAC):

- **Esterno:** il bucket è condiviso con uno o più dei seguenti elementi o una combinazione dei seguenti elementi: un CloudFront OAI, un CloudFront OAC o un account esterno all'organizzazione (che non fa parte della).
 - **Interno:** il bucket è condiviso con uno o più account interni (che fanno parte della) tua organizzazione. Non è condiviso con un CloudFront OAI o un OAC.
 - **Non condiviso:** il bucket non è condiviso con un altro account, un CloudFront OAI o un OAC.
- CloudFront
- **Sconosciuto:** Macie non è stata in grado di valutare le impostazioni di accesso condiviso per il bucket. Ad esempio, una quota o un problema temporaneo ha impedito a Macie di recuperare e valutare i dati richiesti.

Per determinare se un bucket è condiviso con un altro Account AWS, Macie analizza la policy del bucket e la lista di controllo degli accessi (ACL) per il bucket. L'analisi è limitata alle impostazioni a livello di bucket. Non riflette alcuna impostazione a livello di oggetto per la condivisione di oggetti specifici nel bucket. Inoltre, un'organizzazione è definita come un insieme di account Macie gestiti centralmente come gruppo di account correlati tramite AWS Organizations o su invito di Macie. Per ulteriori informazioni sulle opzioni di Amazon S3 per la condivisione dei bucket, consulta il [controllo degli accessi](#) nella Guida per l'utente di Amazon Simple Storage Service.

Note

In alcuni casi, Macie potrebbe indicare erroneamente che un bucket è condiviso con un utente esterno (Account AWS che non fa parte della) tua organizzazione. Ciò può verificarsi se Macie non è in grado di valutare appieno la relazione tra l'Principale elemento della policy del bucket e determinate chiavi di [contesto della condizione AWS globale o le chiavi di condizione di Amazon S3](#) nell'elemento Condition della policy. Questo può essere il caso delle seguenti chiavi di

condizione:aws:PrincipalAccount,aws:PrincipalArn,aws:PrincipalOrgID,aws:PrincipalSourceVpc,aws:SourceVpc,aws:SourceVpcAccount,aws:userid,s3:DataAccessPointAccount e s3:DataAccessPointArn

Ti consigliamo di rivedere la politica del bucket per determinare se questo accesso è previsto e sicuro.

Per determinare se un bucket è condiviso con un CloudFront OAI o un OAC, Macie analizza la policy relativa al bucket. Un CloudFront OAI o OAC consente agli utenti di accedere agli oggetti di un bucket tramite una o più distribuzioni specificate. CloudFront Per ulteriori informazioni CloudFront OAI OACs, consulta la sezione [Restrizione dell'accesso a un'origine Amazon S3](#) nella CloudFront Amazon Developer Guide.

La sezione Panoramica include anche il campo Latest automated discovery run. Questo campo indica quando Macie ha analizzato l'ultima volta gli oggetti nel bucket durante l'individuazione automatica dei dati sensibili. Se questa analisi non è stata effettuata, in questo campo viene visualizzato un trattino (—).

Statistiche sugli oggetti

Questa sezione fornisce informazioni sugli oggetti nel bucket, a partire dal numero totale di oggetti nel bucket (conteggio totale), dalla dimensione di archiviazione totale di tutti gli oggetti (dimensione totale di archiviazione) e dalla dimensione totale di archiviazione di tutti gli oggetti che sono file compressi (.gz, .gzip o .zip) (dimensione totale compressa). Le statistiche aggiuntive in questa sezione possono aiutarti a valutare la quantità di dati che Macie può analizzare per rilevare i dati sensibili nel bucket.

Se hai creato il bucket di recente o hai apportato modifiche significative agli oggetti del bucket nelle ultime 24 ore, opzionalmente scegli refresh



per recuperare i metadati più recenti per gli oggetti del bucket. Macie visualizza l'icona delle informazioni



per aiutarti a determinare se questo potrebbe essere il caso. L'opzione di aggiornamento è disponibile se un bucket contiene 30.000 o meno oggetti.

Mentre esaminate le statistiche di questa sezione, tenete presente quanto segue:

- Se il controllo delle versioni è abilitato per il bucket, i valori delle dimensioni si basano sulla dimensione di archiviazione della versione più recente di ogni oggetto nel bucket.

- Se il bucket memorizza oggetti compressi, i valori delle dimensioni non riflettono la dimensione effettiva di tali oggetti dopo la loro decompressione.
- Se aggiorni i metadati degli oggetti per un bucket, Macie segnala temporaneamente Unknown per le statistiche di crittografia che si applicano agli oggetti. Macie rivaluterà e aggiornerà i dati per queste statistiche quando eseguirà il successivo [aggiornamento giornaliero](#) dei metadati del bucket e dell'oggetto, ovvero entro 24 ore.
- Per impostazione predefinita, il numero di oggetti e i valori delle dimensioni includono i dati per tutte le parti dell'oggetto contenute nel bucket a seguito di caricamenti incompleti in più parti. Se aggiorni i metadati degli oggetti per un bucket, Macie esclude i dati relativi alle parti dell'oggetto dai valori ricalcolati. Quando Macie esegue il successivo aggiornamento giornaliero dei metadati del bucket e dell'oggetto (entro 24 ore), Macie ricalcola e aggiorna i valori di queste statistiche e include nuovamente i dati per le parti dell'oggetto nei valori.

Tieni presente che Macie non può analizzare le parti dell'oggetto per rilevare dati sensibili. Amazon S3 deve prima completare l'assemblaggio delle parti in uno o più oggetti affinché Macie possa analizzarle. Per informazioni sui caricamenti in più parti e sulle parti di oggetti, incluso come eliminare le parti automaticamente con le regole del ciclo di vita, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte nella Guida per l'utente di Amazon Simple Storage Service](#). Per identificare i bucket che contengono parti di oggetti, puoi fare riferimento a metriche di caricamento multiparte incomplete in Amazon S3 Storage Lens. Per ulteriori informazioni, consulta la sezione [Valutazione dell'attività e dell'utilizzo dello storage](#) nella Guida per l'utente di Amazon Simple Storage Service.

Le statistiche sugli oggetti sono organizzate come segue.

Oggetti classificabili

Questa sezione indica il numero totale di oggetti che Macie può analizzare per rilevare dati sensibili e la dimensione totale di archiviazione di tali oggetti. Questi oggetti utilizzano una classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un file o un formato di storage supportato. Puoi rilevare dati sensibili negli oggetti usando Macie. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).

Oggetti inclassificabili

Questa sezione indica il numero totale di oggetti che Macie non può analizzare per rilevare dati sensibili e la dimensione totale di archiviazione di tali oggetti. Questi oggetti non utilizzano una

classe di storage Amazon S3 supportata o non hanno un'estensione del nome di file per un file o un formato di storage supportato.

Oggetti non classificabili: classe di archiviazione

Questa sezione fornisce un'analisi dettagliata del numero e delle dimensioni di archiviazione degli oggetti che Macie non può analizzare perché gli oggetti non utilizzano una classe di storage Amazon S3 supportata.

Oggetti non classificabili: tipo di file

Questa sezione fornisce un'analisi dettagliata del numero e della dimensione di archiviazione degli oggetti che Macie non può analizzare perché gli oggetti non hanno un'estensione del nome di file per un formato di file o di archiviazione supportato.

Oggetti per tipo di crittografia

Questa sezione fornisce un'analisi dettagliata del numero di oggetti che utilizzano ogni tipo di crittografia supportato da Amazon S3:

- Fornito dal cliente: il numero di oggetti crittografati con una chiave fornita dal cliente. Questi oggetti utilizzano la crittografia SSE-C.
- AWS KMS gestiti: il numero di oggetti crittografati con una chiave gestita dal cliente Chiave gestita da AWS o con una AWS KMS key chiave gestita dal cliente. Questi oggetti utilizzano la crittografia DSSE-KMS o SSE-KMS.
- Amazon S3 gestito: il numero di oggetti crittografati con una chiave gestita di Amazon S3. Questi oggetti utilizzano la crittografia SSE-S3.
- Nessuna crittografia: il numero di oggetti che non sono crittografati o che utilizzano la crittografia lato client. (Se un oggetto è crittografato utilizzando la crittografia lato client, Macie non può accedere e segnalare i dati di crittografia relativi all'oggetto.)
- Sconosciuto: il numero di oggetti per i quali Macie non dispone dei metadati di crittografia correnti. Ciò si verifica in genere se di recente hai scelto di aggiornare manualmente i metadati per gli oggetti del bucket. Macie aggiornerà le statistiche di crittografia quando eseguirà il successivo aggiornamento giornaliero dei metadati del bucket e dell'oggetto, ovvero entro 24 ore.

Per informazioni su ogni tipo di crittografia supportato, consulta la sezione [Protezione dei dati con crittografia](#) nella Guida per l'utente di Amazon Simple Storage Service.

Crittografia lato server

Questa sezione fornisce informazioni sulle impostazioni di crittografia lato server per il bucket.

Il campo Encryption required by bucket policy indica se la policy del bucket richiede la crittografia degli oggetti sul lato server quando gli oggetti vengono aggiunti al bucket:

- No: il bucket non dispone di una policy del bucket o la politica del bucket non richiede la crittografia lato server di nuovi oggetti. Se esiste una policy bucket, non richiede che le [PutObject](#) richieda includano un'intestazione di crittografia lato server valida.
- Sì, la policy del bucket richiede la crittografia lato server di nuovi oggetti. [PutObject](#) richiede per il bucket devono includere un'intestazione di crittografia lato server valida. In caso contrario, Amazon S3 rifiuta la richiesta.
- Sconosciuto: Macie non è stata in grado di valutare la politica del bucket per determinare se richieda la crittografia lato server di nuovi oggetti. Ad esempio, una quota o un problema impedivano a Macie di recuperare e valutare la policy.

Per questa valutazione, le intestazioni di crittografia lato server valide sono: `x-amz-server-side-encryption` con un valore `o` e con un valore `aws:kms` `x-amz-server-side-encryption-customer-algorithm` `AES256`. Per informazioni sull'utilizzo delle policy bucket per richiedere la crittografia lato server di nuovi oggetti, consulta [Protection data with server-side encryption nella](#) Amazon Simple Storage Service User Guide.

Il campo di crittografia predefinito indica l'algoritmo di crittografia lato server che il bucket è configurato per applicare di default agli oggetti che vengono aggiunti al bucket:

- AES256— Le impostazioni di crittografia predefinite del bucket sono configurate per crittografare nuovi oggetti con una chiave gestita Amazon S3. I nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia SSE-S3.
- `aws:kms` — Le impostazioni di crittografia predefinite del bucket sono configurate per crittografare nuovi oggetti con una chiave o una AWS KMS key chiave gestita dal cliente. Chiave gestita da AWS I nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia SSE-KMS. Il AWS KMS keycampo mostra l'Amazon Resource Name (ARN) o l'identificatore univoco (ID chiave) per la chiave utilizzata.
- `aws:kms:dsse` — Le impostazioni di crittografia predefinite del bucket sono configurate per crittografare nuovi oggetti con una chiave, una o una chiave gestita dal cliente. AWS KMS key

Chiave gestita da AWS I nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia DSSE-KMS. Il AWS KMS keycampo mostra l'ARN o l'ID della chiave utilizzata.

- Nessuno: le impostazioni di crittografia predefinite del bucket non specificano il comportamento di crittografia lato server per i nuovi oggetti.

A partire dal 5 gennaio 2023, Amazon S3 applica automaticamente la crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per gli oggetti che vengono aggiunti ai bucket. Facoltativamente, puoi configurare le impostazioni di crittografia predefinite di un bucket per utilizzare invece la crittografia lato server con una chiave (SSE-KMS) o la crittografia lato server a doppio livello con una AWS KMS chiave (DSSE-KMS). AWS KMS Per informazioni sulle impostazioni e le opzioni di crittografia predefinite, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket S3 nella](#) Amazon Simple Storage Service User Guide.

Rilevamento di dati sensibili

Questa sezione indica se sono stati configurati processi di rilevamento di dati sensibili per analizzare periodicamente gli oggetti nel bucket su base giornaliera, settimanale o mensile. Se il valore del campo Monitoraggio attivo per processo è Sì, il bucket viene incluso in modo esplicito in un processo periodico oppure il bucket corrisponde ai criteri per un processo periodico nelle ultime 24 ore. Inoltre, lo stato di almeno uno di questi lavori non è Annullato. Macie aggiorna questi dati su base giornaliera.

Se hai configurato qualsiasi tipo di processo di rilevamento di dati sensibili (un processo periodico o un processo occasionale) per analizzare gli oggetti nel bucket, il campo Ultimo processo fornisce l'identificatore univoco del lavoro che ha iniziato a essere eseguito più di recente. Il campo Ultimo processo eseguito indica quando è iniziata l'esecuzione del processo.

Tip

Per visualizzare tutti i dati sensibili rilevati dal lavoro, scegli il link nel campo Ultimo lavoro. Nel pannello dei dettagli del lavoro che appare, scegli Mostra risultati nella parte superiore del pannello, quindi scegli Mostra risultati.

Accesso pubblico

Questa sezione indica se il bucket è accessibile al pubblico. Fornisce inoltre un'analisi dettagliata delle varie impostazioni a livello di account e bucket che determinano se questo è il caso. Il campo Autorizzazione effettiva indica il risultato cumulativo di queste impostazioni:

- Non pubblico: il bucket non è accessibile al pubblico.
- Pubblico: il bucket è accessibile al pubblico.
- Sconosciuto: Macie non è stata in grado di valutare tutte le impostazioni di accesso pubblico per il bucket. Ad esempio, un problema di quota o temporaneo ha impedito a Macie di recuperare e valutare i dati richiesti.

Per questa valutazione, Macie analizza una combinazione di impostazioni a livello di account e bucket per ogni bucket: le impostazioni di blocco dell'accesso pubblico per l'account, le impostazioni di blocco dell'accesso pubblico per il bucket, la politica del bucket per il bucket e l'elenco di controllo degli accessi (ACL) per il bucket. Tieni presente che la valutazione non include impostazioni a livello di oggetto che consentono l'accesso pubblico a oggetti specifici in un bucket.

Per ulteriori informazioni sulle impostazioni di Amazon S3 per la gestione dell'accesso pubblico ai bucket e ai dati dei bucket, consulta [Controllo degli accessi e blocco dell'accesso pubblico allo storage Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

Replica

In questa sezione, il campo Replicato indica se il bucket è configurato per replicare oggetti su altri bucket. Se il valore di questo campo è Sì, una o più regole di replica sono configurate e abilitate per il bucket. Questa sezione elenca quindi anche l'ID dell'account per ogni utente Account AWS che possiede un bucket di destinazione.

Il campo Replicato esternamente indica se il bucket è configurato per replicare oggetti in bucket, in quanto sono esterni all'organizzazione (Account AWS non fanno parte dell'organizzazione). Un'organizzazione è un insieme di account Macie gestiti centralmente come gruppo di account correlati tramite o su invito di Macie. AWS Organizations Se il valore di questo campo è Sì, viene configurata e abilitata una regola di replica per il bucket e la regola è configurata per replicare gli oggetti in un bucket di proprietà di un esterno. Account AWS

Note

In determinate condizioni, Macie potrebbe indicare erroneamente che un bucket è configurato per replicare oggetti in un bucket di proprietà di un esterno. Account AWS [Ciò può verificarsi se il bucket di destinazione è stato creato in un altro Regione AWS ambiente nelle 24 ore precedenti, dopo che Macie ha recuperato i metadati del bucket e dell'oggetto da Amazon S3 come parte del ciclo di aggiornamento giornaliero.](#) Per esaminare il problema utilizzando Macie, scegli refresh



per recuperare i metadati del bucket più recenti da Amazon S3. Quindi esamina l'elenco degli account in questa sezione. IDs Per un'indagine più approfondita, usa Amazon S3 per rivedere le regole di replica per il bucket.

Per ulteriori informazioni sulle opzioni e le impostazioni di Amazon S3 per la replica di oggetti bucket, consulta [Replicating objects nella Amazon Simple Storage Service User Guide](#).

Tag

Se i tag sono associati al bucket, questa sezione viene visualizzata nel pannello e li elenca. I tag sono etichette che è possibile definire e assegnare a determinati tipi di AWS risorse, inclusi i bucket S3. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale.

Per ulteriori informazioni sull'etichettatura dei bucket, consulta [Using cost allocation S3 bucket tag nella Guida per l'utente di Amazon Simple Storage Service](#).

Filtrare l'inventario dei bucket S3 in Macie

Per identificare e concentrarti sui bucket con caratteristiche specifiche, puoi filtrare l'inventario dei bucket S3 sulla console Amazon Macie e nelle query inviate a livello di codice utilizzando l'API Amazon Macie. Quando crei un filtro, utilizzi attributi specifici del bucket per definire criteri per includere o escludere i bucket da una vista o dai risultati delle query. Un attributo bucket è un campo che memorizza metadati specifici per un bucket.

In Macie, un filtro è costituito da una o più condizioni. Ogni condizione, nota anche come criterio, è composta da tre parti:

- Un campo basato su attributi, ad esempio Bucket name, Tag key o Defined in job.
- Un operatore, ad esempio uguale o non uguale.
- Uno o più valori. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti.

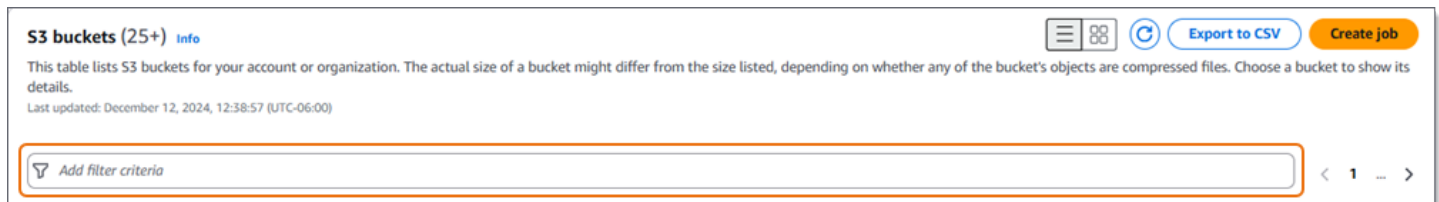
Il modo in cui definisci e applichi le condizioni di filtro dipende dal fatto che utilizzi la console Amazon Macie o l'API Amazon Macie.

Argomenti

- [Filtrare l'inventario sulla console Amazon Macie](#)
- [Filtrare l'inventario in modo programmatico con l'API Amazon Macie](#)

Filtrare l'inventario sulla console Amazon Macie

Se utilizzi la console Amazon Macie per filtrare l'inventario dei bucket S3, Macie offre opzioni per aiutarti a scegliere campi, operatori e valori per condizioni individuali. Puoi accedere a queste opzioni utilizzando la casella del filtro nella pagina dei bucket S3, come mostrato nell'immagine seguente.

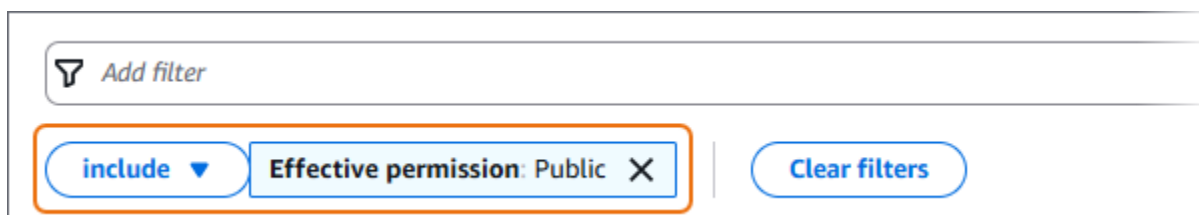


Quando posizioni il cursore nella casella del filtro, Macie visualizza un elenco di campi che puoi utilizzare nelle condizioni di filtro. I campi sono organizzati per categorie logiche. Ad esempio, la categoria Campi comuni include campi che memorizzano informazioni generali su un bucket S3. Le categorie di accesso pubblico includono campi che memorizzano dati sui vari tipi di impostazioni di accesso pubblico che possono essere applicate a un bucket. I campi sono ordinati alfabeticamente all'interno di ogni categoria.

Per aggiungere una condizione, inizia scegliendo un campo dall'elenco. Per trovare un campo, sfoglia l'elenco completo o inserisci parte del nome del campo per restringere l'elenco dei campi.

A seconda del campo scelto, Macie mostra diverse opzioni. Le opzioni riflettono il tipo e la natura del campo scelto. Ad esempio, se scegli il campo Accesso condiviso, Macie visualizza un elenco di valori tra cui scegliere. Se scegli il campo Bucket name, Macie visualizza una casella di testo in cui puoi inserire il nome di un bucket S3. Qualunque campo tu scelga, Macie ti guida attraverso i passaggi per aggiungere una condizione che includa le impostazioni richieste per il campo.

Dopo aver aggiunto una condizione, Macie applica i criteri relativi alla condizione e la visualizza in un token di filtro sotto la casella del filtro, come mostrato nell'immagine seguente.



In questo esempio, la condizione è configurata per includere tutti i bucket accessibili pubblicamente e per escludere tutti gli altri bucket. Restituisce i bucket in cui il valore del campo Autorizzazione effettiva è uguale a Pubblico.

Man mano che aggiungi altre condizioni, Macie applica i relativi criteri e li visualizza sotto la casella del filtro. Se aggiungi più condizioni, Macie utilizza la logica AND per unire le condizioni e valutare i criteri di filtro. Ciò significa che un bucket S3 soddisfa i criteri del filtro solo se soddisfa tutte le condizioni del filtro. Puoi fare riferimento all'area sotto la casella del filtro in qualsiasi momento per determinare quali criteri hai applicato.

Per filtrare l'inventario utilizzando la console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra l'inventario dei bucket.

Se il rilevamento automatico dei dati sensibili è abilitato, la visualizzazione predefinita non mostra i dati per i bucket attualmente esclusi dal rilevamento automatico. Se sei l'amministratore Macie di un'organizzazione, inoltre, non vengono visualizzati i dati degli account per i quali il rilevamento automatico è attualmente disabilitato. Per visualizzare questi dati, scegli X nel campo È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Nella parte superiore della pagina, scegli facoltativamente refresh



per recuperare i metadati del bucket più recenti da Amazon S3.

4. Posiziona il cursore nella casella del filtro, quindi scegli il campo da utilizzare per la condizione.
5. Scegli o inserisci il tipo di valore appropriato per il campo, tenendo presenti i seguenti suggerimenti.

Date, orari e intervalli di tempo

Per le date e gli orari, utilizzate le caselle Da e A per definire un intervallo di tempo inclusivo:

- Per definire un intervallo di tempo fisso, utilizzate le caselle Da e A per specificare rispettivamente la prima data e ora e l'ultima data e ora dell'intervallo.
- Per definire un intervallo di tempo relativo che inizi in una determinata data e ora e termini nell'ora corrente, immettete la data e l'ora di inizio nelle caselle Da ed eliminate il testo nelle caselle To.

- Per definire un intervallo di tempo relativo che termini con una determinata data e ora, inserite la data e l'ora di fine nelle caselle A ed eliminate il testo nelle caselle Da.

Tieni presente che i valori temporali utilizzano la notazione a 24 ore. Se si utilizza il selettore di date per scegliere le date, è possibile rifinire i valori inserendo il testo direttamente nelle caselle Da e A.

Numeri e intervalli numerici

Per i valori numerici, utilizzate le caselle Da e A per inserire numeri interi che definiscono un intervallo numerico inclusivo:

- Per definire un intervallo numerico fisso, utilizzate le caselle Da e A per specificare rispettivamente i numeri più bassi e più alti dell'intervallo.
- Per definire un intervallo numerico fisso limitato a un valore specifico, inserite il valore nelle caselle Da e A. Ad esempio, per includere solo i bucket S3 che memorizzano esattamente 15 oggetti, inseriscilo **15** nelle caselle Da e To.
- Per definire un intervallo numerico relativo che inizi da un determinato numero, inserite il numero nella casella Da e non immettete alcun testo nella casella To.
- Per definire un intervallo numerico relativo che termina con un determinato numero, inserite il numero nella casella A e non immettete alcun testo nella casella Da.

Valori di testo (stringa)

Per questo tipo di valore, inserisci un valore completo e valido per il campo. I valori distinguono tra maiuscole e minuscole

Tieni presente che non puoi utilizzare un valore parziale o caratteri jolly in questo tipo di valore. L'unica eccezione è il campo Bucket name. Per quel campo, puoi specificare un prefisso anziché un nome completo del bucket. Ad esempio, per trovare tutti i bucket S3 i cui nomi iniziano con my-S3, inserisci **my-S3** come valore del filtro il campo Bucket name. Se inserisci qualsiasi altro valore, ad esempio **My-s3** o, Macie non restituirà i **my*** bucket.

6. Quando hai finito di aggiungere un valore per il campo, scegli Applica. Macie applica i criteri di filtro e visualizza la condizione in un token di filtro sotto la casella del filtro.
7. Ripeti i passaggi da 4 a 6 per ogni condizione aggiuntiva che desideri aggiungere.
8. Per rimuovere una condizione, scegli la X nel token del filtro relativo alla condizione.
9. Per modificare una condizione, rimuovila scegliendo la X nel token del filtro relativo alla condizione. Quindi ripeti i passaggi da 4 a 6 per aggiungere una condizione con le impostazioni corrette.

Filtrare l'inventario in modo programmatico con l'API Amazon Macie

Per filtrare l'inventario dei bucket S3 in modo programmatico, specifica i criteri di filtro nelle query inviate utilizzando il funzionamento [DescribeBuckets](#) dell'API Amazon Macie. Questa operazione restituisce una serie di oggetti. Ogni oggetto contiene dati statistici e altre informazioni su un bucket che corrisponde ai criteri di filtro.

Per specificare i criteri di filtro in una query, includi una mappa delle condizioni di filtro nella richiesta. Per ogni condizione, specificate un campo, un operatore e uno o più valori per il campo. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti. Per informazioni sui campi, gli operatori e i tipi di valori che puoi utilizzare in una condizione, consulta [Amazon S3 Data Sources](#) nel Amazon Macie API Reference.

[Gli esempi seguenti mostrano come specificare i criteri di filtro nelle query inviate utilizzando \(\).AWS Command Line InterfaceAWS CLI](#) Puoi farlo anche utilizzando la versione corrente di un altro strumento a riga di AWS comando o di un AWS SDK oppure inviando richieste HTTPS direttamente a Macie. Per informazioni sugli AWS strumenti e SDKs, consulta [Tools to Build on](#). AWS

Esempi

- [Esempio: trova i bucket in base al nome del bucket](#)
- [Esempio: trova bucket accessibili pubblicamente](#)
- [Esempio: trova i bucket che memorizzano oggetti non crittografati](#)
- [Esempio: trova bucket che replicano i dati su account esterni](#)
- [Esempio: trova i bucket che non sono monitorati da un processo di rilevamento di dati sensibili](#)
- [Esempio: trova i bucket che non sono monitorati dal rilevamento automatico di dati sensibili](#)
- [Esempio: trova i bucket in base a più criteri](#)

Negli esempi viene utilizzato il comando [describe-buckets](#). Se il comando viene eseguito correttamente, Macie restituisce un array. `buckets` L'array contiene un oggetto per ogni bucket che si trova nella versione corrente Regione AWS e corrisponde ai criteri di filtro. Per un esempio di questo output, espandi la sezione seguente.

Esempio di **buckets** array

In questo esempio, l'`buckets` array fornisce dettagli su due bucket che corrispondono ai criteri di filtro specificati in una query.

```
{
  "buckets": [
    {
      "accountId": "123456789012",
      "allowsUnencryptedObjectUploads": "FALSE",
      "automatedDiscoveryMonitoringStatus": "MONITORED",
      "bucketArn": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
      "bucketName": "amzn-s3-demo-bucket1",
      "classifiableObjectCount": 13,
      "classifiableSizeInBytes": 1592088,
      "jobDetails": {
        "isDefinedInJob": "TRUE",
        "isMonitoredByJob": "TRUE",
        "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
        "lastJobRunTime": "2024-05-26T14:55:30.270000+00:00"
      },
      "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
      "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
      "objectCount": 13,
      "objectCountByEncryptionType": {
        "customerManaged": 0,
        "kmsManaged": 2,
        "s3Managed": 7,
        "unencrypted": 4,
        "unknown": 0
      },
      "publicAccess": {
        "effectivePermission": "NOT_PUBLIC",
        "permissionConfiguration": {
          "accountLevelPermissions": {
            "blockPublicAccess": {
              "blockPublicAcls": true,
              "blockPublicPolicy": true,
              "ignorePublicAcls": true,
              "restrictPublicBuckets": true
            }
          },
          "bucketLevelPermissions": {
            "accessControlList": {
              "allowsPublicReadAccess": false,
              "allowsPublicWriteAccess": false
            }
          }
        }
      }
    }
  ]
}
```

```

        "blockPublicAccess": {
            "blockPublicAcls": true,
            "blockPublicPolicy": true,
            "ignorePublicAcls": true,
            "restrictPublicBuckets": true
        },
        "bucketPolicy": {
            "allowsPublicReadAccess": false,
            "allowsPublicWriteAccess": false
        }
    }
},
"region": "us-east-1",
"replicationDetails": {
    "replicated": false,
    "replicatedExternally": false,
    "replicationAccounts": []
},
"sensitivityScore": 78,
"serverSideEncryption": {
    "kmsMasterKeyId": null,
    "type": "NONE"
},
"sharedAccess": "NOT_SHARED",
"sizeInBytes": 4549746,
"sizeInBytesCompressed": 0,
"tags": [
    {
        "key": "Division",
        "value": "HR"
    },
    {
        "key": "Team",
        "value": "Recruiting"
    }
],
"unclassifiableObjectCount": {
    "fileType": 0,
    "storageClass": 0,
    "total": 0
},
"unclassifiableObjectSizeInBytes": {
    "fileType": 0,

```

```

        "storageClass": 0,
        "total": 0
    },
    "versioning": true
},
{
    "accountId": "123456789012",
    "allowsUnencryptedObjectUploads": "TRUE",
    "automatedDiscoveryMonitoringStatus": "MONITORED",
    "bucketArn": "arn:aws:s3:::amzn-s3-demo-bucket2",
    "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
    "bucketName": "amzn-s3-demo-bucket2",
    "classifiableObjectCount": 8,
    "classifiableSizeInBytes": 133810,
    "jobDetails": {
        "isDefinedInJob": "TRUE",
        "isMonitoredByJob": "FALSE",
        "lastJobId": "188d4f6044d621771ef7d65f2example",
        "lastJobRunTime": "2024-04-09T19:37:11.511000+00:00"
    },
    "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
    "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
    "objectCount": 8,
    "objectCountByEncryptionType": {
        "customerManaged": 0,
        "kmsManaged": 0,
        "s3Managed": 8,
        "unencrypted": 0,
        "unknown": 0
    },
    "publicAccess": {
        "effectivePermission": "NOT_PUBLIC",
        "permissionConfiguration": {
            "accountLevelPermissions": {
                "blockPublicAccess": {
                    "blockPublicAcls": true,
                    "blockPublicPolicy": true,
                    "ignorePublicAcls": true,
                    "restrictPublicBuckets": true
                }
            },
            "bucketLevelPermissions": {
                "accessControlList": {
                    "allowsPublicReadAccess": false,

```

```

        "allowsPublicWriteAccess": false
    },
    "blockPublicAccess": {
        "blockPublicAcls": true,
        "blockPublicPolicy": true,
        "ignorePublicAcls": true,
        "restrictPublicBuckets": true
    },
    "bucketPolicy": {
        "allowsPublicReadAccess": false,
        "allowsPublicWriteAccess": false
    }
}
},
"region": "us-east-1",
"replicationDetails": {
    "replicated": false,
    "replicatedExternally": false,
    "replicationAccounts": []
},
"sensitivityScore": 95,
"serverSideEncryption": {
    "kmsMasterKeyId": null,
    "type": "AES256"
},
"sharedAccess": "EXTERNAL",
"sizeInBytes": 175978,
"sizeInBytesCompressed": 0,
"tags": [
    {
        "key": "Division",
        "value": "HR"
    },
    {
        "key": "Team",
        "value": "Recruiting"
    }
],
"unclassifiableObjectCount": {
    "fileType": 3,
    "storageClass": 0,
    "total": 3
},

```

```

        "unclassifiableObjectSizeInBytes": {
            "fileType": 2999826,
            "storageClass": 0,
            "total": 2999826
        },
        "versioning": true
    }
]
}

```

Se nessun bucket soddisfa i criteri di filtro, Macie restituisce un array vuoto. `buckets`

```

{
  "buckets": []
}

```

Esempio: trova i bucket in base al nome del bucket

Questo esempio interroga i metadati per i bucket che si trovano nella versione corrente Regione AWS e i cui nomi iniziano con `my-S3`.

Per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"bucketName":{"prefix":"my-S3"}}
```

Dove:

- *bucketName* specifica il nome JSON del campo Bucket name.
- *prefix* specifica l'operatore di prefisso.
- *my-S3* è il valore per il campo Bucket name.

Esempio: trova bucket accessibili pubblicamente

Questo esempio esegue una query sui metadati relativi ai bucket presenti nella versione corrente Regione AWS e che, in base a una combinazione di impostazioni di autorizzazione, sono accessibili pubblicamente.

Per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":["PUBLIC"]}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"publicAccess.effectivePermission\":"eq\":["PUBLIC\"]}}
```

Dove:

- *publicAccess.effectivePermission* specifica il nome JSON del campo Autorizzazione effettiva.
- *eq* specifica l'operatore equals.
- *PUBLIC* è un valore enumerato per il campo Autorizzazione effettiva.

Esempio: trova i bucket che memorizzano oggetti non crittografati

Questo esempio interroga i metadati per i bucket che si trovano nella cartella corrente Regione AWS e memorizzano oggetti non crittografati.

Per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":{"gte":1}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"objectCountByEncryptionType.unencrypted\":"gte\":1}}
```

Dove:

- *objectCountByEncryptionType.unencrypted* specifica il nome JSON del campo Nessuna crittografia.
- *gte* specifica l'operatore maggiore o uguale a.
- *1* è il valore più basso in un intervallo numerico relativo inclusivo per il campo Nessuna crittografia.

Esempio: trova bucket che replicano i dati su account esterni

Questo esempio interroga i metadati per i bucket che si trovano nella versione corrente Regione AWS e sono configurati per replicare oggetti in bucket per un bucket Account AWS che non fa parte dell'organizzazione.

Per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally": {"eq":["true"]}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --  
criteria={"replicationDetails.replicatedExternally\":{\"eq\":{\"true\"}}}
```

Dove:

- *replicationDetails.replicatedExternally* specifica il nome JSON del campo Replicato esternamente.
- *eq* specifica l'operatore equals.
- *true* specifica un valore booleano per il campo Replicato esternamente.

Esempio: trova i bucket che non sono monitorati da un processo di rilevamento di dati sensibili

Questo esempio interroga i metadati per i bucket che si trovano nell'attuale versione Regione AWS e non sono associati a nessun processo periodico di rilevamento di dati sensibili.

Per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"jobDetails.isMonitoredByJob\":{\"eq\":{\"FALSE\"}}}
```

Dove:

- *jobDetails.isMonitoredByJob* specifica il nome JSON del campo Monitorato attivamente dal processo.
- *eq* specifica l'operatore equals.
- *FALSE* è un valore enumerato per il campo Monitoraggio attivo per processo.

Esempio: trova i bucket che non sono monitorati dal rilevamento automatico di dati sensibili

Questo esempio interroga i metadati per i bucket che si trovano nella versione corrente Regione AWS e sono esclusi dal rilevamento automatico dei dati sensibili.

Per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"automatedDiscoveryMonitoringStatus":{"eq":["NOT_MONITORED"]}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria="{\"automatedDiscoveryMonitoringStatus\":{\"eq\":[\"NOT_MONITORED\"]}}"
```

Dove:

- *automatedDiscoveryMonitoringStatus* specifica il nome JSON del campo È monitorato da un rilevamento automatico.
- *eq* specifica l'operatore equals.
- *NOT_MONITORED* è un valore enumerato per il campo È monitorato da un rilevamento automatico.

Esempio: trova i bucket in base a più criteri

Questo esempio interroga i metadati per individuare i bucket presenti nella versione corrente Regione AWS e che soddisfano i seguenti criteri: sono accessibili pubblicamente in base a una combinazione di impostazioni di autorizzazione, memorizzano oggetti non crittografati e non sono associati ad alcun processo periodico di rilevamento di dati sensibili.

Per Linux, macOS o Unix, utilizzando il carattere di continuazione di riga con barra rovesciata (\) per migliorare la leggibilità:

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Per Microsoft Windows, utilizzando il carattere di continuazione di riga con cursore (^) per migliorare la leggibilità:

```
C:\> aws macie2 describe-buckets ^
--criteria={"publicAccess.effectivePermission\":{"eq\":
[\ "PUBLIC\"]},\ "objectCountByEncryptionType.unencrypted\":{"gte\":1},
\ "jobDetails.isMonitoredByJob\":{"eq\":[\ "FALSE\"]}}
```

Dove:

- *publicAccess.effectivePermission* specifica il nome JSON del campo Autorizzazione effettiva e:
 - *eq* specifica l'operatore equals.
 - *PUBLIC* è un valore enumerato per il campo Autorizzazione effettiva.
- *objectCountByEncryptionType.unencrypted* specifica il nome JSON del campo Nessuna crittografia e:
 - *gte* specifica l'operatore maggiore o uguale a.
 - *1* è il valore più basso in un intervallo numerico relativo inclusivo per il campo Nessuna crittografia.
- *jobDetails.isMonitoredByJob* specifica il nome JSON del campo Actively monitored by job e:
 - *eq* specifica l'operatore equals.
 - *FALSE* è un valore enumerato per il campo Monitoraggio attivo per processo.

Consentire a Macie di accedere a bucket e oggetti S3

Quando abiliti Amazon Macie for your Account AWS, Macie crea un [ruolo collegato al servizio](#) che concede a Macie le autorizzazioni necessarie per chiamare Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e altro per tuo conto. Servizi AWS Un ruolo collegato al servizio semplifica il processo di configurazione di un ruolo Servizio AWS perché non è necessario aggiungere manualmente le autorizzazioni affinché il servizio completi le azioni per

tuo conto. Per ulteriori informazioni su questo tipo di ruolo, consulta i [ruoli IAM](#) nella Guida per l'utente. AWS Identity and Access Management

La politica di autorizzazione per il ruolo collegato al servizio Macie (`AWSServiceRoleForAmazonMacie`) consente a Macie di eseguire azioni che includono il recupero di informazioni sui bucket e sugli oggetti S3 e il recupero di oggetti dai bucket. Se sei l'amministratore Macie di un'organizzazione, la policy consente inoltre a Macie di eseguire queste azioni per tuo conto per gli account dei membri dell'organizzazione.

Macie utilizza queste autorizzazioni per eseguire attività come:

- Genera e gestisci un inventario dei tuoi bucket S3 per uso generico.
- Fornisci dati statistici e di altro tipo sui bucket e sugli oggetti contenuti nei bucket.
- Monitora e valuta i bucket per la sicurezza e il controllo degli accessi.
- Analizza gli oggetti nei bucket per rilevare dati sensibili.

Nella maggior parte dei casi, Macie dispone delle autorizzazioni necessarie per eseguire queste attività. Tuttavia, se un bucket S3 ha una politica restrittiva sui bucket, la politica potrebbe impedire a Macie di eseguire alcune o tutte queste attività.

Una bucket policy è una policy basata sulle risorse AWS Identity and Access Management (IAM) che specifica quali azioni un principale (utente, account, servizio o altra entità) può eseguire su un bucket S3 e le condizioni in base alle quali un principale può eseguire tali azioni. Le azioni e le condizioni possono essere applicate a operazioni a livello di bucket, come il recupero di informazioni su un bucket, e a operazioni a livello di oggetto, come il recupero di oggetti da un bucket.

Le politiche del bucket in genere concedono o limitano l'accesso utilizzando dichiarazioni e condizioni esplicite o. `Allow Deny` Ad esempio, una policy del bucket potrebbe contenere un'istruzione `Allow` o che nega l'accesso al bucket a meno che non vengano utilizzati indirizzi IP di origine specifici, endpoint Amazon Virtual Private Cloud (Amazon VPC) o VPCs per accedere al bucket. Per informazioni sull'utilizzo delle policy dei bucket per concedere o limitare l'accesso ai bucket, consulta [le politiche Bucket per Amazon S3 e Come Amazon S3 autorizza una richiesta nella Guida per l'utente di Amazon Simple Storage Service](#).

Se una policy bucket utilizza un'istruzione `Allow` esplicita, la policy non impedisce a Macie di recuperare informazioni sul bucket e sugli oggetti del bucket o di recuperare oggetti dal bucket. Questo perché le `Allow` istruzioni contenute nella politica delle autorizzazioni per il ruolo collegato al servizio Macie concedono queste autorizzazioni.

Tuttavia, se una policy sui bucket utilizza un'istruzione esplicita con una o più condizioni, a Macie potrebbe non essere consentito recuperare informazioni sul bucket o sugli oggetti del bucket o recuperare gli oggetti del bucket. Ad esempio, se una policy bucket nega esplicitamente l'accesso da tutte le fonti tranne un indirizzo IP specifico, a Macie non sarà consentito analizzare gli oggetti del bucket quando si esegue un processo di rilevamento di dati sensibili. Questo perché le policy restrittive relative ai bucket hanno la precedenza sulle Allow dichiarazioni contenute nella politica di autorizzazione per il ruolo Macie collegato al servizio.

Per consentire a Macie di accedere a un bucket S3 con una politica restrittiva sui bucket, puoi aggiungere una condizione per il ruolo collegato al servizio Macie () alla policy del bucket. `AWSServiceRoleForAmazonMacie` La condizione può escludere che il ruolo collegato al servizio Macie corrisponda alla restrizione della policy. Deny Può farlo utilizzando la [chiave di contesto della condizione `aws:PrincipalArn` globale](#) e l'Amazon Resource Name (ARN) del ruolo collegato al servizio Macie.

La procedura seguente guida l'utente attraverso questo processo e fornisce un esempio.

Per aggiungere il ruolo collegato al servizio Macie a una policy bucket

1. Accedi a AWS Management Console e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il bucket S3 a cui desideri consentire l'accesso a Macie.
4. Nella sezione Autorizzazioni, alla voce Policy del bucket, scegliere Modifica.
5. Nell'editor delle policy di Bucket, identifica ogni Deny istruzione che limita l'accesso e impedisce a Macie di accedere al bucket o agli oggetti del bucket.
6. In ogni Deny istruzione, aggiungi una condizione che utilizzi la chiave di contesto della condizione `aws:PrincipalArn` globale e specifichi l'ARN del ruolo collegato al servizio Macie per il tuo. Account AWS

Il valore per la chiave di condizione dovrebbe essere `arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie, 123456789012` dov'è l'ID dell'account per il tuo. Account AWS

La posizione in cui lo aggiungi a una policy bucket dipende dalla struttura, dagli elementi e dalle condizioni attualmente contenuti nella policy. Per informazioni sulle strutture e gli elementi supportati, consulta [Policies and permissions in Amazon S3 nella Amazon Simple Storage Service User Guide](#).

Di seguito è riportato un esempio di policy sui bucket che utilizza un'istruzione esplicita per limitare l'accesso a un bucket S3 denominato. `amzn-s3-demo-bucket` Con la politica attuale, è possibile accedere al bucket solo dall'endpoint VPC il cui ID è. `vpce-1a2b3c4d` L'accesso da tutti gli altri endpoint VPC è negato, incluso l'accesso da Macie e da Macie. AWS Management Console

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115example",
  "Statement": [
    {
      "Sid": "Access only from specific VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

[Per modificare questa politica e consentire a Macie di accedere al bucket S3 e agli oggetti del bucket, possiamo aggiungere una condizione che utilizza l'operatore condition e la chiave `globalStringNotLike condition context. aws:PrincipalArn`](#) Questa condizione aggiuntiva esclude che il ruolo collegato al servizio Macie corrisponda alla restrizione. Deny

```
{
  "Version": "2012-10-17",
  "Id": " Policy1415115example ",
  "Statement": [
    {
      "Sid": "Access only from specific VPCE and Macie",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
```

```

        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:SourceVpce": "vpce-1a2b3c4d"
        },
        "StringNotLike": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
    }
}
]
}

```

Nell'esempio precedente, l'operatore `StringNotLike` condition utilizza la chiave `aws:PrincipalArn` condition context per specificare l'ARN del ruolo collegato al servizio Macie, dove:

- `123456789012` è l'ID dell'account Account AWS che è autorizzato a utilizzare Macie per recuperare informazioni sul bucket e sugli oggetti del bucket e recuperare oggetti dal bucket.
- `macie.amazonaws.com` è l'identificatore del principale servizio Macie.
- `AWSServiceRoleForAmazonMacie` è il nome del ruolo collegato al servizio Macie.

Abbiamo utilizzato l'`StringNotLike` operatore perché la politica utilizza già un operatore. `StringNotEquals` Una politica può utilizzare l'`StringNotEquals` operatore una sola volta.

Per ulteriori esempi di policy e informazioni dettagliate sulla gestione dell'accesso alle risorse di Amazon S3, consulta [Access control](#) nella Amazon Simple Storage Service User Guide.

Alla scoperta di dati sensibili con Macie

Con Amazon Macie, puoi automatizzare il rilevamento, la registrazione e il reporting di dati sensibili nel tuo patrimonio di dati Amazon Simple Storage Service (Amazon S3). Puoi farlo in due modi: configurando Macie per eseguire il rilevamento automatico dei dati sensibili e creando ed eseguendo processi di rilevamento di dati sensibili.

Il rilevamento automatico dei dati sensibili offre un'ampia visibilità su dove potrebbero risiedere i dati sensibili nel tuo patrimonio di dati Amazon S3. Con questa opzione, Macie valuta l'inventario dei bucket S3 su base giornaliera e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi dai bucket. Macie recupera e analizza quindi gli oggetti selezionati, ispezionandoli alla ricerca di dati sensibili. Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#).

I lavori di rilevamento di dati sensibili forniscono un'analisi più approfondita e mirata. Con questa opzione, definisci l'ampiezza e la profondità dell'analisi: bucket S3 specifici che selezioni o bucket che soddisfano criteri specifici. Puoi anche affinare l'ambito dell'analisi scegliendo opzioni come criteri personalizzati che derivano dalle proprietà degli oggetti S3. Inoltre, è possibile configurare un job in modo che venga eseguito una sola volta per l'analisi e la valutazione su richiesta o su base ricorrente per l'analisi, la valutazione e il monitoraggio periodici. Per ulteriori informazioni, consulta [Esecuzione di processi di rilevamento dei dati sensibili](#).

Con entrambe le opzioni, i processi automatizzati di rilevamento di dati sensibili o di rilevamento di dati sensibili, puoi configurare Macie per analizzare gli oggetti S3 utilizzando gli identificatori di dati gestiti che fornisce, identificatori di dati personalizzati definiti dall'utente o una combinazione dei due. Puoi anche ottimizzare l'analisi con gli elenchi consentiti. Quando si configurano le impostazioni per l'individuazione automatica di dati sensibili o un processo di rilevamento di dati sensibili, si specifica quale utilizzare:

- **Identificatori di dati gestiti:** si tratta di criteri e tecniche integrati progettati per rilevare tipi specifici di dati sensibili. Ad esempio, possono rilevare numeri di carte di credito, chiavi di accesso AWS segrete e numeri di passaporto per determinati paesi e regioni. Sono in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili per molti paesi e regioni. Ciò include diversi tipi di informazioni di identificazione personale (PII), informazioni finanziarie e dati sulle credenziali. Per ulteriori informazioni, consulta [Utilizzo di identificatori di dati gestiti](#).
- **Identificatori di dati personalizzati:** si tratta di criteri personalizzati definiti dall'utente per rilevare dati sensibili. Ogni identificatore di dati personalizzato specifica un'espressione regolare (regex) che

definisce uno schema di testo da abbinare e, facoltativamente, sequenze di caratteri e una regola di prossimità che perfezionano i risultati. È possibile utilizzarli per rilevare dati sensibili che riflettono scenari particolari, proprietà intellettuale o dati proprietari, ad esempio dipendenti IDs, numeri di conto clienti o classificazioni interne dei dati. Per ulteriori informazioni, consulta [Creazione di identificatori di dati personalizzati](#).

- Elenchi consentiti: specificano il testo e i modelli di testo che vuoi che Macie ignori. È possibile utilizzarli per specificare eccezioni relative ai dati sensibili per scenari o ambienti particolari, ad esempio nomi o numeri di telefono pubblici dell'organizzazione o dati di esempio utilizzati dall'organizzazione per i test. Se Macie trova del testo che corrisponde a una voce o a uno schema in un elenco consentito, Macie non segnala tale occorrenza di testo. Questo è il caso anche se il testo corrisponde ai criteri di un identificatore di dati gestito o personalizzato. Per ulteriori informazioni, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).

Quando Macie analizza un oggetto S3, Macie recupera la versione più recente dell'oggetto da Amazon S3, quindi ispeziona il contenuto dell'oggetto alla ricerca di dati sensibili. Macie può analizzare un oggetto se è vero quanto segue:

- L'oggetto utilizza un file o un formato di archiviazione supportato ed è archiviato in un bucket S3 generico utilizzando una classe di archiviazione supportata. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).
- Se l'oggetto è crittografato, viene crittografato con una chiave a cui Macie può accedere e che può usare. Per ulteriori informazioni, consulta [Analisi di oggetti S3 crittografati](#).
- Se l'oggetto è archiviato in un bucket con una politica restrittiva, la policy consente a Macie di accedere agli oggetti nel bucket. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Per aiutarti a soddisfare e mantenere la conformità ai requisiti di sicurezza e privacy dei dati, Macie registra i dati sensibili che trova e le analisi che esegue: rilevamenti di dati sensibili e risultati di scoperta di dati sensibili. Un rilevamento di dati sensibili è un rapporto dettagliato sui dati sensibili che Macie ha trovato in un oggetto S3. Un risultato di rilevamento dei dati sensibili è un report che registra i dettagli relativi all'analisi di un oggetto. Ogni tipo di record aderisce a uno schema standardizzato, che può aiutarti a interrogarli, monitorarli ed elaborarli utilizzando altre applicazioni, servizi e sistemi, se necessario.

 Tip

Sebbene Macie sia ottimizzato per Amazon S3, puoi utilizzarlo per scoprire dati sensibili nelle risorse che attualmente memorizzi altrove. Puoi farlo spostando i dati su Amazon S3 in modo temporaneo o permanente. Ad esempio, esporta le istantanee di Amazon Relational Database Service o Amazon Aurora su Amazon S3 in formato Apache Parquet. Oppure esporta una tabella Amazon DynamoDB in Amazon S3. È quindi possibile creare un processo per analizzare i dati in Amazon S3.

Argomenti

- [Utilizzo di identificatori di dati gestiti](#)
- [Creazione di identificatori di dati personalizzati](#)
- [Definizione delle eccezioni relative ai dati sensibili con elenchi consentiti](#)
- [Esecuzione del rilevamento automatico di dati sensibili](#)
- [Esecuzione di processi di rilevamento dei dati sensibili](#)
- [Analisi di oggetti Amazon S3 crittografati](#)
- [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#)
- [Classi e formati di storage supportati](#)

Utilizzo di identificatori di dati gestiti

Amazon Macie utilizza una combinazione di criteri e tecniche, tra cui l'apprendimento automatico e il pattern matching, per rilevare dati sensibili negli oggetti Amazon Simple Storage Service (Amazon S3). Questi criteri e tecniche, denominati collettivamente identificatori di dati gestiti, sono in grado di rilevare un ampio e crescente elenco di tipi di dati sensibili per molti paesi e regioni, inclusi diversi tipi di dati relativi alle credenziali, informazioni finanziarie, informazioni sanitarie personali (PHI) e informazioni di identificazione personale (PII). Ogni identificatore di dati gestito è progettato per rilevare un tipo specifico di dati sensibili, ad esempio chiavi di accesso AWS segrete, numeri di carte di credito o numeri di passaporto per un determinato paese o regione.

Macie è in grado di rilevare le seguenti categorie di dati sensibili utilizzando identificatori di dati gestiti:

- Credenziali, per dati relativi alle credenziali come chiavi private e AWS chiavi di accesso segrete.
- Informazioni finanziarie, per dati finanziari come numeri di carte di credito e numeri di conti bancari.

- Informazioni personali, per PHI come l'assicurazione sanitaria e i numeri di identificazione medica e PII come i numeri di identificazione della patente di guida e i numeri di passaporto.

All'interno di ogni categoria, Macie è in grado di rilevare diversi tipi di dati sensibili. Negli argomenti di questa sezione sono elencati e descritti i vari tipi e tutti i requisiti pertinenti per la rilevazione. Per ogni tipo, vengono indicati anche gli identificatori univoci (ID) degli identificatori di dati gestiti progettati per rilevare i dati. Quando [crei un processo di rilevamento di dati sensibili](#) o [configuri le impostazioni per l'individuazione automatica di dati sensibili](#), puoi utilizzarle IDs per specificare quali identificatori di dati gestiti desideri che Macie utilizzi quando analizza gli oggetti S3.

Argomenti

- [Requisiti delle parole chiave per gli identificatori di dati gestiti](#)
- [Riferimento rapido: identificatori di dati gestiti per tipo](#)
- [Riferimento dettagliato: identificatori di dati gestiti per categoria](#)

Per un elenco degli identificatori di dati gestiti consigliati per i lavori, consulta. [Identificatori di dati gestiti consigliati per i lavori di rilevamento di dati sensibili](#) Per un elenco degli identificatori di dati gestiti consigliati e utilizzati di default per l'individuazione automatica di dati sensibili, consulta. [Impostazioni predefinite per l'individuazione automatica dei dati sensibili](#)

Requisiti delle parole chiave per gli identificatori di dati gestiti

Per rilevare determinati tipi di dati sensibili utilizzando identificatori di dati gestiti, Amazon Macie richiede che una parola chiave si trovi in prossimità dei dati. Se questo è il caso di un particolare tipo di dati, gli argomenti di riferimento in questa sezione indicano i requisiti relativi alle parole chiave per tali dati.

Se una parola chiave deve trovarsi in prossimità di un particolare tipo di dati, in genere la parola chiave deve trovarsi entro 30 caratteri (inclusi) dai dati. I requisiti di prossimità aggiuntivi variano in base al tipo di file o al formato di archiviazione di un oggetto Amazon Simple Storage Service (Amazon S3).

Dati colonnari strutturati

Per i dati colonnari, una parola chiave deve far parte dello stesso valore o deve essere inclusa nel nome della colonna o del campo che memorizza un valore. Questo è il caso delle cartelle di lavoro di Microsoft Excel, dei file CSV e dei file TSV.

Ad esempio, se il valore di un campo contiene sia SSN che un numero a nove cifre che utilizza la sintassi di un codice di previdenza sociale statunitense (SSN), Macie è in grado di rilevare l'SSN nel campo. Analogamente, se il nome di una colonna contiene SSN, Macie è in grado di rilevare ogni SSN nella colonna. Macie considera i valori in quella colonna come se fossero in prossimità della parola chiave SSN.

Dati strutturati basati su record

Per i dati basati sui record, una parola chiave deve far parte dello stesso valore o essere inclusa nel nome di un elemento nel percorso del campo o dell'array che memorizza un valore. Questo è il caso dei contenitori di oggetti Apache Avro, dei file Apache Parquet, dei file JSON e dei file JSON Lines.

Ad esempio, se il valore di un campo contiene sia credenziali che una sequenza di caratteri che utilizza la sintassi di una chiave di accesso AWS segreta, Macie può rilevare la chiave nel campo. Allo stesso modo, se il percorso di un campo è `$.credentials.aws.key`, Macie può rilevare una chiave di accesso AWS segreta nel campo. Macie considera il valore nel campo come se fosse in prossimità delle credenziali della parola chiave.

Dati non strutturati

Per i dati non strutturati, una parola chiave deve in genere trovarsi entro 30 caratteri (inclusi) dai dati. Non ci sono requisiti di prossimità aggiuntivi. È il caso dei file Adobe Portable Document Format, dei documenti Microsoft Word, dei messaggi di posta elettronica e dei file di testo non binari diversi dai file CSV, JSON, JSON Lines e TSV. Ciò include tutti i dati strutturati, come tabelle o XML, in questi tipi di file.

Le parole chiave non distinguono tra maiuscole e minuscole. Inoltre, se una parola chiave contiene uno spazio, Macie corrisponde automaticamente alle varianti di parola chiave che non contengono lo spazio o contengono un carattere di sottolineatura (`_`) o un trattino (`-`) anziché lo spazio. In alcuni casi, Macie amplia o abbrevia anche una parola chiave per rispondere alle varianti più comuni della parola chiave.

Per una dimostrazione di come le parole chiave forniscano un contesto e aiutino Macie a rilevare tipi specifici di dati sensibili, guarda il seguente video: [Come Amazon Macie usa le parole chiave per scoprire dati sensibili](#).

Riferimento rapido: identificatori di dati gestiti per tipo

In Amazon Macie, un identificatore di dati gestito è un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili, ad esempio numeri di carte di credito, chiavi di accesso AWS segrete o numeri di passaporto per un particolare paese o regione. Questi identificatori sono in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili per molti paesi e aree geografiche, inclusi diversi tipi di dati relativi alle credenziali, informazioni finanziarie, informazioni sanitarie personali (PHI) e informazioni di identificazione personale (PII).

La tabella seguente elenca tutti gli identificatori di dati gestiti attualmente forniti da Macie, organizzati per tipo di dati sensibili. Per ogni tipo, fornisce le seguenti informazioni:

- **Categoria di dati sensibili:** specifica la categoria generale di dati sensibili che include il tipo: Credenziali, per dati relativi a credenziali come le chiavi private; Informazioni finanziarie, per dati finanziari come numeri di carte di credito e numeri di conto corrente bancario; Informazioni personali: PHI per informazioni sanitarie personali come l'assicurazione sanitaria e i numeri di identificazione medica; e, Informazioni personali: PII per informazioni di identificazione personale come i numeri di identificazione della patente di guida e numeri di passaporto.
- **ID identificatore di dati gestito:** specifica l'identificatore univoco (ID) per uno o più identificatori di dati gestiti progettati per rilevare i dati. Quando crei un processo di rilevamento di dati sensibili o configuri le impostazioni per l'individuazione automatica di dati sensibili, puoi utilizzarle IDs per specificare quali identificatori di dati gestiti desideri che Macie utilizzi quando analizza i dati. Per un elenco degli identificatori di dati gestiti consigliati per i lavori, consulta. [Identificatori di dati gestiti consigliati per i lavori di rilevamento di dati sensibili](#) Per un elenco degli identificatori di dati gestiti consigliati per il rilevamento automatico di dati sensibili, consulta. [Impostazioni predefinite per l'individuazione automatica dei dati sensibili](#)
- **Parola chiave obbligatoria:** specifica se il rilevamento richiede che una parola chiave si trovi in prossimità dei dati. Per informazioni su come Macie utilizza le parole chiave quando analizza i dati, consulta. [Requisiti delle parole chiave](#)
- **Paesi e aree geografiche:** specifica per quali paesi e aree geografiche sono progettati gli identificatori di dati gestiti applicabili. Se gli identificatori di dati gestiti non sono progettati per particolari paesi e aree geografiche, questo valore è Any.

Per esaminare ulteriori dettagli sugli identificatori di dati gestiti per un particolare tipo di dati sensibili, scegli il tipo.

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
AWS chiave di accesso segreta	Credenziali	AWS_CREDE NTIALS	Sì	Qualsiasi
Numero del conto bancario	Informazioni finanziarie	BANK_ACCO UNT_NUMBE R (sia per il Canada che per gli Stati Uniti)	Sì	Canada, Stati Uniti
Numero di conto bancario di base (BBAN)	Informazioni finanziarie	A seconda del paese o della regione: FRANCE_BA NK_ACCOUN T_NUMBER, GERMANY_B ANK_ACCOU NT_NUMBER , ITALY_BAN K_ACCOUNT _NUMBER, SPAIN_BAN K_ACCOUNT _NUMBER, UK_BANK_A CCOUNT_NU MBER	Sì	Francia, Germania, Italia, Regno Unito, Spagna
Data di nascita	Informazioni personali: PII	DATE_OF_B IRTH	Sì	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Data di scadenza della carta di credito	Informazioni finanziarie	CREDIT_CARD_EXPIRATION	Sì	Qualsiasi
Dati a banda magnetica della carta di credito	Informazioni finanziarie	CREDIT_CARD_MAGNETIC_STRIPE	Sì	Qualsiasi
Numero di carta di credito	Informazioni finanziarie	CREDIT_CARD_NUMBER (per i numeri di carta di credito in prossimità di una parola chiave), CREDIT_CARD_NUMBER_(NO_KEYWORD) (per i numeri di carta di credito non vicini a una parola chiave)	Può variare	Qualsiasi
Codice di verifica della carta di credito	Informazioni finanziarie	CREDIT_CARD_SECURITY_CODE	Sì	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero identificativo della patente di guida	Informazioni personali: PII	A seconda del paese o della regione: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US),	Sì	Australia, Austria, Belgio, Bulgaria, Canada, Croazia, Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, India, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito, USA

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		ESTONIA_D RIVERS_LI CENSE, FINLAND_D RIVERS_LI CENSE, FRANCE_DR IVERS_LIC ENSE, GERMANY_D RIVERS_LI CENSE, GREECE_DR IVERS_LIC ENSE, HUNGARY_D RIVERS_LI CENSE, INDIA_DRI VERS_LICE NSE, IRELAND_D RIVERS_LI CENSE, ITALY_DRI VERS_LICE NSE, LATVIA_DR IVERS_LIC ENSE, LITHUANIA _DRIVERS_ LICENSE, LUXEMBOUR		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		G_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di registrazione della Drug Enforcement Agency (DEA)	Informazioni personali: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Sì	US
Numero di lista elettorale	Informazioni personali: PII	UK_ELECTORAL_ROLL_NUMBER	Sì	UK
Nome completo	Informazioni personali: PII	NAME	No	Qualsiasi, se il nome utilizza un set di caratteri latini
Coordinate GPS (Global Positioning System)	Informazioni personali: PII	LATITUDE_LONGITUDE	Sì	Qualsiasi, se le coordinate sono in prossimità di una parola chiave inglese
Chiave API di Google Cloud	Credenziali	GCP_API_KEY	Sì	Qualsiasi
Numero di richiesta di assicurazione sanitaria (HICN)	Informazioni personali: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Sì	US

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di identificazione medica e assistenza sanitaria	Informazioni personali: PHI	A seconda del paese o della regione: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Sì	Canada, UE, Finlandia, Francia, Regno Unito, USA
Codice HCPCS (Healthcare Common Procedure Coding System)	Informazioni personali: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Sì	US

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Intestazione HTTP Basic Authorization	Credenziali	HTTP_BASIC_AUTH_HEADER	No	Qualsiasi
Cookie HTTP	Informazioni personali: PII	HTTP_COOKIE	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di conto bancario internazionale (IBAN)	Informazioni finanziarie	A seconda del paese o della regione: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT	No	Albania, Andorra, Bosnia-Erzegovina, Brasile, Bulgaria, Costa Rica, Croazia, Cipro, Repubblica Ceca, Danimarca, Repubblica Dominicana, Egitto, Estonia, Isole Faroe, Finlandia, Francia, Georgia, Germania, Grecia, Groenlandia, Ungheria, Islanda, Irlanda, Italia, Giordania, Kosovo, Liechtenstein, Lituania, Malta, Mauritania, Mauritius, Monaco, Montenegro, Paesi Bassi, Macedonia del Nord, Polonia,

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		_NUMBER, DENMARK_B ANK_ACCOU NT_NUMBER , DOMINICAN _REPUBLIC _BANK_ACC COUNT_NUMB ER, EGYPT_BAN K_ACCOUNT _NUMBER, ESTONIA_B ANK_ACCOU NT_NUMBER , FAROE_ISL ANDS_BANK _ACCOUNT_ NUMBER, FINLAND_B ANK_ACCOU NT_NUMBER , FRANCE_BA NK_ACCOUN T_NUMBER, GEORGIA_B ANK_ACCOU NT_NUMBER , GERMANY_B ANK_ACCOU NT_NUMBER , GREECE_BA NK_ACCOUN T_NUMBER,		Portogallo, San Marino, Senegal, Serbia, Slovacchi a, Slovenia, Spagna, Svezia, Svizzera, Timor Est, Tunisia, Türkiye, Regno Unito, Ucraina, Emirati Arabi Uniti, Isole Vergini britannic he

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANI		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		A_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		NT_NUMBER , SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER , TURKIYE_BANK_ACCOUNT_NUMBER , UK_BANK_ACCOUNT_NUMBER, UKRAINE_B		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		ANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (per le Isole Vergini Britanniche)		
Token Web JSON (JWT)	Credenziali	JSON_WEB_TOKEN	No	Qualsiasi
Indirizzo postale	Informazioni personali: PII	ADDRESS, BRAZIL_CEP_CODE (per il Código de Endereçamento Postal del Brasile)	Può variare	Australia, Brasile, Canada, Francia, Germania, Italia, Spagna, Regno Unito, USA
Codice nazionale sulle droghe (NDC)	Informazioni personali: PHI	USA_NATIONAL_DRUG_CODE	Sì	US

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numeri di carta d'identità	Informazioni personali: PII	A seconda del paese o della regione: ARGENTINA_DNI_NUMBER, BRAZIL_RG_NUMBER, CHILE_RUT_NUMBER, COLOMBIA_CITIZENSHIP_CARD_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, MEXICO_CURP_NUMBER, SPAIN_DNI_NUMBER	Sì	Argentina, Brasile, Cile, Colombia, Francia, Germania, India, Italia, Messico, Spagna

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di previdenza nazionale (NINO)	Informazioni personali: PII	UK_NATIONAL_INSURANCE_NUMBER	Sì	UK
National Provider Identifier (NPI)	Informazioni personali: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Sì	US
Chiave privata OpenSSH	Credenziali	OPENSSH_PRIVATE_KEY	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di passaporto	Informazioni personali: PII	A seconda del paese o della regione: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Sì	Canada, Francia, Germania, Italia, Regno Unito, Spagna, Stati Uniti
Numero di residenza permanente (Green Card)	Informazioni personali: PII	CANADA_NATIONAL_IDENTITY_NUMBER	Sì	Canada
Chiave privata PGP	Credenziali	PGP_PRIVATE_KEY	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di telefono	Informazioni personali: PII	A seconda del paese o della regione: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Può variare	Brasile, Canada, Francia, Germania, Italia, Regno Unito, Spagna, Stati Uniti
Chiave privata Public-Key Cryptography Standard (PKCS)	Credenziali	PKCS	No	Qualsiasi
Numero della carta di trasporto pubblico	Informazioni personali: PII	ARGENTINA_TARJETA_SUBE	Sì	Argentina
Chiave privata PuTTY	Credenziali	PUTTY_PRIVATE_KEY	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di previdenza sociale (SIN)	Informazioni personali: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Sì	Canada
Numero di previdenza sociale (SSN)	Informazioni personali: PII	A seconda del paese o della regione: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Sì	Spagna, Stati Uniti
the section called “Chiave API Stripe”	Credenziali	STRIPE_CREDENTIALS	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero identificativo del contribuente o codice fiscale	Informazioni personali: PII	A seconda del paese o della regione: ARGENTINA _INDIVIDU AL_TAX_ID ENTIFICAT ION_NUMBE R, ARGENTINA _ORGANIZA TION_TAX_ IDENTIFIC ATION_NUM BER, AUSTRALIA _TAX_FILE _NUMBER, BRAZIL_CN PJ_NUMBER , BRAZIL_CP F_NUMBER, CHILE_RUT _NUMBER, COLOMBIA_ INDIVIDUA L_NIT_NUM BER, COLOMBIA_ ORGANIZAT ION_NIT_N UMBER, FRANCE_TA X_IDENTIF	Sì	Argentina , Australia, Brasile, Cile, Colombia, Francia, Germania, India, Italia, Messico, Spagna, Regno Unito, USA

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		ICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, MEXICO_INDIVIDUAL_RFC_NUMBER, MEXICO_ORGANIZATION_RFC_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		_IDENTIFICATION_NUMBER		
Identificatore univoco del dispositivo (UDI)	Informazioni personali: PHI	MEDICAL_DEVICE_UDI	Sì	US
Numero di identificazione del veicolo (VIN)	Informazioni personali: PII	VEHICLE_IDENTIFICATION_NUMBER	Sì	Qualsiasi, se il VIN è in prossimità di una parola chiave in una delle seguenti lingue: inglese, francese, tedesco, lituano, polacco, portoghese, rumeno o spagnolo

Riferimento dettagliato: identificatori di dati gestiti per categoria

In Amazon Macie, gli identificatori di dati gestiti sono criteri e tecniche integrati progettati per rilevare tipi specifici di dati sensibili. Sono in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili per molti paesi e regioni, inclusi diversi tipi di dati relativi a credenziali, informazioni finanziarie e informazioni personali. Ogni identificatore di dati gestito è progettato per rilevare un tipo specifico di dati sensibili, ad esempio chiavi di accesso AWS segrete, numeri di carte di credito o numeri di passaporto per un determinato paese o area geografica.

Macie è in grado di rilevare diverse categorie di dati sensibili utilizzando identificatori di dati gestiti. All'interno di ogni categoria, Macie è in grado di rilevare diversi tipi di dati sensibili. Gli argomenti di

questa sezione elencano e descrivono ogni tipo e tutti i requisiti pertinenti per il rilevamento dei dati. Puoi sfogliare gli argomenti per categoria:

- [Credenziali](#): per dati relativi alle credenziali come chiavi private e chiavi di accesso AWS segrete.
- [Informazioni finanziarie](#): per dati finanziari come numeri di carte di credito e numeri di conti bancari.
- [Informazioni personali: PHI](#) — Per informazioni sanitarie personali (PHI) come l'assicurazione sanitaria e i numeri di identificazione medica.
- [Informazioni personali: PII](#) — Per informazioni di identificazione personale (PII) come i numeri di identificazione della patente di guida e i numeri di passaporto.

Oppure scegli un tipo specifico di dati sensibili dalla tabella seguente. La tabella elenca tutti gli identificatori di dati gestiti attualmente forniti da Macie, organizzati per tipo di dati sensibili. La tabella riassume anche i requisiti pertinenti per il rilevamento di ciascun tipo.

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
AWS chiave di accesso segreta	Credenziali	AWS_CREDE NTIALS	Sì	Qualsiasi
Numero del conto bancario	Informazioni finanziarie	BANK_ACCO UNT_NUMBE R (sia per il Canada che per gli Stati Uniti)	Sì	Canada, Stati Uniti
Numero di conto bancario di base (BBAN)	Informazioni finanziarie	A seconda del paese o della regione: FRANCE_BA NK_ACCOUN T_NUMBER, GERMANY_B ANK_ACCOU NT_NUMBER , ITALY_BAN	Sì	Francia, Germania, Italia, Regno Unito, Spagna

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		K_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER		
Data di nascita	Informazioni personali: PII	DATE_OF_BIRTH	Sì	Qualsiasi
Data di scadenza della carta di credito	Informazioni finanziarie	CREDIT_CARD_EXPIRATION	Sì	Qualsiasi
Dati a banda magnetica della carta di credito	Informazioni finanziarie	CREDIT_CARD_MAGNETIC_STRIPE	Sì	Qualsiasi
Numero di carta di credito	Informazioni finanziarie	CREDIT_CARD_NUMBER (per i numeri di carta di credito in prossimità di una parola chiave), CREDIT_CARD_NUMBER_(NO_KEYWORD) (per i numeri di carta di credito non vicini a una parola chiave)	Può variare	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Codice di verifica della carta di credito	Informazioni finanziarie	CREDIT_CARD_SECURITY_CODE	Sì	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero identificativo della patente di guida	Informazioni personali: PII	A seconda del paese o della regione: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US),	Sì	Australia, Austria, Belgio, Bulgaria, Canada, Croazia, Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, India, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito, USA

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		ESTONIA_D RIVERS_LI CENSE, FINLAND_D RIVERS_LI CENSE, FRANCE_DR IVERS_LIC ENSE, GERMANY_D RIVERS_LI CENSE, GREECE_DR IVERS_LIC ENSE, HUNGARY_D RIVERS_LI CENSE, INDIA_DRI VERS_LICE NSE, IRELAND_D RIVERS_LI CENSE, ITALY_DRI VERS_LICE NSE, LATVIA_DR IVERS_LIC ENSE, LITHUANIA _DRIVERS_ LICENSE, LUXEMBOUR		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		G_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di registrazione della Drug Enforcement Agency (DEA)	Informazioni personali: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Sì	US
Numero di lista elettorale	Informazioni personali: PII	UK_ELECTORAL_ROLL_NUMBER	Sì	UK
Nome completo	Informazioni personali: PII	NAME	No	Qualsiasi, se il nome utilizza un set di caratteri latini
Coordinate GPS (Global Positioning System)	Informazioni personali: PII	LATITUDE_LONGITUDE	Sì	Qualsiasi, se le coordinate sono in prossimità di una parola chiave inglese
Chiave API di Google Cloud	Credenziali	GCP_API_KEY	Sì	Qualsiasi
Numero di richiesta di assicurazione sanitaria (HICN)	Informazioni personali: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Sì	US

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di identificazione medica e assistenza sanitaria	Informazioni personali: PHI	A seconda del paese o della regione: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Sì	Canada, UE, Finlandia, Francia, Regno Unito, USA
Codice HCPCS (Healthcare Common Procedure Coding System)	Informazioni personali: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Sì	US

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Intestazione HTTP Basic Authorization	Credenziali	HTTP_BASIC_AUTH_HEADER	No	Qualsiasi
Cookie HTTP	Informazioni personali: PII	HTTP_COOKIE	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di conto bancario internazionale (IBAN)	Informazioni finanziarie	A seconda del paese o della regione: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT	No	Albania, Andorra, Bosnia-Erzegovina, Brasile, Bulgaria, Costa Rica, Croazia, Cipro, Repubblica Ceca, Danimarca, Repubblica Dominicana, Egitto, Estonia, Isole Faroe, Finlandia, Francia, Georgia, Germania, Grecia, Groenlandia, Ungheria, Islanda, Irlanda, Italia, Giordania, Kosovo, Liechtenstein, Lituania, Malta, Mauritania, Mauritius, Monaco, Montenegro, Paesi Bassi, Macedonia del Nord, Polonia,

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		_NUMBER, DENMARK_B ANK_ACCOUNT_NUMBER , DOMINICAN _REPUBLIC _BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_B ANK_ACCOUNT_NUMBER , FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_B ANK_ACCOUNT_NUMBER , FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_B ANK_ACCOUNT_NUMBER , GERMANY_B ANK_ACCOUNT_NUMBER , GREECE_BANK_ACCOUNT_NUMBER, HUNGARY_B ANK_ACCOUNT_NUMBER , ICELAND_BANK_ACCOUNT_NUMBER, INDIA_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JAPAN_BANK_ACCOUNT_NUMBER, KAZAKHSTAN_BANK_ACCOUNT_NUMBER, KENYA_BANK_ACCOUNT_NUMBER, KOREA_BANK_ACCOUNT_NUMBER, KUWAIT_BANK_ACCOUNT_NUMBER, KYRGYZSTAN_BANK_ACCOUNT_NUMBER, LAOS_BANK_ACCOUNT_NUMBER, LATVIA_BANK_ACCOUNT_NUMBER, LEBANON_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, LUXEMBOURG_BANK_ACCOUNT_NUMBER, MACAU_BANK_ACCOUNT_NUMBER, MALAYSIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MEXICO_BANK_ACCOUNT_NUMBER, MOLDOVA_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, MOROCCO_BANK_ACCOUNT_NUMBER, NEPAL_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NEW_ZEALAND_BANK_ACCOUNT_NUMBER, NIGERIA_BANK_ACCOUNT_NUMBER, NORWAY_BANK_ACCOUNT_NUMBER, OMAN_BANK_ACCOUNT_NUMBER, PAKISTAN_BANK_ACCOUNT_NUMBER, PANAMA_BANK_ACCOUNT_NUMBER, PARAGUAY_BANK_ACCOUNT_NUMBER, PERU_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, ROMANIA_BANK_ACCOUNT_NUMBER, RUSSIA_BANK_ACCOUNT_NUMBER, SAUDI_ARABIA_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SINGAPORE_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SOUTH_AFRICA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TAIWAN_BANK_ACCOUNT_NUMBER, TAJIKISTAN_BANK_ACCOUNT_NUMBER, TANZANIA_BANK_ACCOUNT_NUMBER, THAILAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKEY_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, UNITED_KINGDOM_BANK_ACCOUNT_NUMBER, UNITED_STATES_BANK_ACCOUNT_NUMBER, UZBEKISTAN_BANK_ACCOUNT_NUMBER, VIETNAM_BANK_ACCOUNT_NUMBER, YEMEN_BANK_ACCOUNT_NUMBER, ZAMBIA_BANK_ACCOUNT_NUMBER, ZIMBABWE_BANK_ACCOUNT_NUMBER		Portogallo, San Marino, Senegal, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Timor Est, Tunisia, Türkiye, Regno Unito, Ucraina, Emirati Arabi Uniti, Isole Vergini britanniche

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		GREENLAND _BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANI		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		A_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		NT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_B		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		ANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (per le Isole Vergini Britanniche)		
Token Web JSON (JWT)	Credenziali	JSON_WEB_TOKEN	No	Qualsiasi
Indirizzo postale	Informazioni personali: PII	ADDRESS, BRAZIL_CEP_CODE (per il Código de Endereçamento Postal del Brasile)	Può variare	Australia, Brasile, Canada, Francia, Germania, Italia, Spagna, Regno Unito, USA
Codice nazionale sulle droghe (NDC)	Informazioni personali: PHI	USA_NATIONAL_DRUG_CODE	Sì	US

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numeri di carta d'identità	Informazioni personali: PII	A seconda del paese o della regione: ARGENTINA_DNI_NUMBER, BRAZIL_RG_NUMBER, CHILE_RUT_NUMBER, COLOMBIA_CITIZENSHIP_CARD_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, MEXICO_CURP_NUMBER, SPAIN_DNI_NUMBER	Sì	Argentina, Brasile, Cile, Colombia, Francia, Germania, India, Italia, Messico, Spagna

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di previdenza nazionale (NINO)	Informazioni personali: PII	UK_NATIONAL_INSURANCE_NUMBER	Sì	UK
National Provider Identifier (NPI)	Informazioni personali: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Sì	US
Chiave privata OpenSSH	Credenziali	OPENSSH_PRIVATE_KEY	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di passaporto	Informazioni personali: PII	A seconda del paese o della regione: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Sì	Canada, Francia, Germania, Italia, Regno Unito, Spagna, Stati Uniti
Numero di residenza permanente (Green Card)	Informazioni personali: PII	CANADA_NATIONAL_IDENTITY_NUMBER	Sì	Canada
Chiave privata PGP	Credenziali	PGP_PRIVATE_KEY	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di telefono	Informazioni personali: PII	A seconda del paese o della regione: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Può variare	Brasile, Canada, Francia, Germania, Italia, Regno Unito, Spagna, Stati Uniti
Chiave privata Public-Key Cryptography Standard (PKCS)	Credenziali	PKCS	No	Qualsiasi
Numero della carta di trasporto pubblico	Informazioni personali: PII	ARGENTINA_TARJETA_SUBE	Sì	Argentina
Chiave privata PuTTY	Credenziali	PUTTY_PRIVATE_KEY	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero di previdenza sociale (SIN)	Informazioni personali: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Sì	Canada
Numero di previdenza sociale (SSN)	Informazioni personali: PII	A seconda del paese o della regione: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Sì	Spagna, Stati Uniti
the section called “Chiave API Stripe”	Credenziali	STRIPE_CREDENTIALS	No	Qualsiasi

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
Numero identificativo del contribuente o codice fiscale	Informazioni personali: PII	A seconda del paese o della regione: ARGENTINA _INDIVIDU AL_TAX_ID ENTIFICAT ION_NUMBE R, ARGENTINA _ORGANIZA TION_TAX_ IDENTIFIC ATION_NUM BER, AUSTRALIA _TAX_FILE _NUMBER, BRAZIL_CN PJ_NUMBER , BRAZIL_CP F_NUMBER, CHILE_RUT _NUMBER, COLOMBIA_ INDIVIDUA L_NIT_NUM BER, COLOMBIA_ ORGANIZAT ION_NIT_N UMBER, FRANCE_TA X_IDENTIF	Sì	Argentina , Australia, Brasile, Cile, Colombia, Francia, Germania, India, Italia, Messico, Spagna, Regno Unito, USA

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		ICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, MEXICO_INDIVIDUAL_RFC_NUMBER, MEXICO_ORGANIZATION_RFC_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX		

Tipo di dati sensibili	Categoria di dati sensibili	ID identificatore dei dati gestiti	Parola chiave obbligatoria	Paesi e Regioni
		_IDENTIFICATION_NUMBER		
Identificatore univoco del dispositivo (UDI)	Informazioni personali: PHI	MEDICAL_DEVICE_UDI	Sì	US
Numero di identificazione del veicolo (VIN)	Informazioni personali: PII	VEHICLE_IDENTIFICATION_NUMBER	Sì	Qualsiasi, se il VIN è in prossimità di una parola chiave in una delle seguenti lingue: inglese, francese, tedesco, lituano, polacco, portoghese, rumeno o spagnolo

Identificatori di dati gestiti per i dati delle credenziali

Amazon Macie è in grado di rilevare diversi tipi di dati sensibili relativi alle credenziali utilizzando identificatori di dati gestiti. Gli argomenti di questa pagina specificano ogni tipo e forniscono informazioni sull'identificatore di dati gestito progettato per rilevare i dati. Ogni argomento fornisce le seguenti informazioni:

- ID identificatore di dati gestito: specifica l'identificatore univoco (ID) per l'identificatore di dati gestito progettato per rilevare i dati. Quando [crei un processo di rilevamento di dati sensibili](#) o [configuri le impostazioni per l'individuazione automatica di dati sensibili](#), puoi utilizzare questo ID per specificare se desideri che Macie utilizzi l'identificatore di dati gestito quando analizza i dati.

- **Paesi e aree geografiche supportati:** indica per quali paesi o aree geografiche è progettato l'identificatore di dati gestito applicabile. Se l'identificatore di dati gestito non è progettato per un particolare paese o area geografica, questo valore è Any.
- **Parola chiave obbligatoria:** specifica se il rilevamento richiede che una parola chiave sia in prossimità dei dati. Se è richiesta una parola chiave, l'argomento fornisce anche esempi di parole chiave obbligatorie. Per informazioni su come Macie utilizza le parole chiave quando analizza i dati, consulta [Requisiti delle parole chiave](#)
- **Commenti:** fornisce tutti i dettagli pertinenti che potrebbero influire sulla scelta dell'identificatore dei dati gestiti o sull'indagine sulle ricorrenze segnalate dei dati sensibili. I dettagli includono informazioni come gli standard supportati, i requisiti di sintassi e le eccezioni.

Gli argomenti sono elencati in ordine alfabetico per tipo di dati riservati.

Tipi di dati sensibili

- [AWS chiave di accesso segreta](#)
- [Chiave API di Google Cloud](#)
- [Intestazione HTTP Basic Authorization](#)
- [Token Web JSON \(JWT\)](#)
- [Chiave privata OpenSSH](#)
- [Chiave privata PGP](#)
- [Chiave privata Public-Key Cryptography Standard \(PKCS\)](#)
- [Chiave privata PuTTY](#)
- [Chiave API Stripe](#)

AWS chiave di accesso segreta

ID identificatore di dati gestito: AWS_CREDENTIALS

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Sì. Le parole chiave includono: aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

Commenti: Macie non riporta le occorrenze delle seguenti sequenze di caratteri, che sono comunemente usate come esempi fittizi: e. je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

Chiave API di Google Cloud

ID identificatore di dati gestito: GCP_API_KEY

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Sì. Le parole chiave includono: G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

Commenti: Macie può rilevare solo il componente string (keyString) di una chiave API di Google Cloud. Il supporto non include il rilevamento dell'ID o del componente del nome visualizzato di una chiave API di Google Cloud.

Intestazione HTTP Basic Authorization

ID identificatore di dati gestito: HTTP_BASIC_AUTH_HEADER

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: il rilevamento richiede un'intestazione completa, che includa il nome del campo e la direttiva sullo schema di autenticazione, come specificato da [RFC 7617](#). Ad esempio: Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ== ed Proxy-Authorization: Basic dGVzdDoxMjPCow==.

Token Web JSON (JWT)

ID identificatore di dati gestito: JSON_WEB_TOKEN

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Macie è in grado di rilevare JSON Web Tokens (JWTs) che soddisfano i requisiti specificati dalla [RFC 7519](#) per le strutture JSON Web Signature (JWS). I token possono essere firmati o non firmati.

Chiave privata OpenSSH

ID identificatore di dati gestito: OPENSSSH_PRIVATE_KEY

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Nessuno

Chiave privata PGP

ID identificatore di dati gestito: PGP_PRIVATE_KEY

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Nessuno

Chiave privata Public-Key Cryptography Standard (PKCS)

ID identificatore di dati gestito: PKCS

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Nessuno

Chiave privata PuTTY

ID identificatore di dati gestito: PUTTY_PRIVATE_KEY

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Macie è in grado di rilevare le chiavi private PuTTY che utilizzano le seguenti intestazioni e sequenze di intestazioni standard PuTTY-User-Key-File:Encryption,,,, e. Comment Public-Lines Private-Lines Private-MAC I valori dell'intestazione possono contenere caratteri alfanumerici, trattini () e caratteri di nuova riga (o). - \n \r Public-Linese Private-Lines i valori possono contenere anche barre (/), segni più () e segni uguali (+). = Private-MACi valori possono contenere anche segni più (+). Il supporto non include il rilevamento di chiavi private con valori di intestazione che contengono altri caratteri, come spazi o caratteri di sottolineatura ()_. Il supporto non include inoltre il rilevamento di chiavi private che includono intestazioni personalizzate.

Chiave API Stripe

ID identificatore di dati gestito: STRIPE_CREDENTIALS

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Macie non riporta le occorrenze delle seguenti sequenze di caratteri, che sono comunemente usate negli esempi di codice Stripe: e. `sk_test_4eC39HqLyjWDarjtT1zdp7dc`
`pk_test_TYooMQauvdEDq54NiTphI7jx`

Identificatori di dati gestiti per informazioni finanziarie

Amazon Macie è in grado di rilevare diversi tipi di informazioni finanziarie sensibili utilizzando identificatori di dati gestiti. Gli argomenti di questa pagina elencano ogni tipo e forniscono informazioni sugli identificatori di dati gestiti progettati per rilevare i dati. Ogni argomento fornisce le seguenti informazioni:

- **ID identificatore di dati gestito:** specifica l'identificatore univoco (ID) per uno o più identificatori di dati gestiti progettati per rilevare i dati. Quando [crei un processo di rilevamento di dati sensibili o configuri le impostazioni per l'individuazione automatica di dati sensibili](#), puoi utilizzarle IDs per specificare quali identificatori di dati gestiti desideri che Macie utilizzi quando analizza i dati.
- **Paesi e aree geografiche supportati:** indica per quali paesi e aree geografiche sono progettati gli identificatori di dati gestiti applicabili. Se gli identificatori di dati gestiti non sono progettati per particolari paesi o aree geografiche, questo valore è Any.
- **Parola chiave obbligatoria:** specifica se il rilevamento richiede che una parola chiave si trovi in prossimità dei dati. Se è richiesta una parola chiave, l'argomento fornisce anche esempi di parole chiave obbligatorie. Per informazioni su come Macie utilizza le parole chiave quando analizza i dati, consulta [Requisiti delle parole chiave](#).
- **Commenti:** fornisce tutti i dettagli pertinenti che potrebbero influire sulla scelta dell'identificatore dei dati gestiti o sull'indagine sulle ricorrenze segnalate dei dati sensibili. I dettagli includono informazioni come gli standard supportati, i requisiti di sintassi e le eccezioni.

Gli argomenti sono elencati in ordine alfabetico per tipo di dati riservati.

Tipi di dati sensibili

- [Numero del conto bancario](#)
- [Numero di conto bancario di base \(BBAN\)](#)
- [Data di scadenza della carta di credito](#)
- [Dati a banda magnetica della carta di credito](#)
- [Numero di carta di credito](#)

- [Codice di verifica della carta di credito](#)
- [Numero di conto bancario internazionale \(IBAN\)](#)

Numero del conto bancario

Macie è in grado di rilevare numeri di conti bancari canadesi e statunitensi composti da sequenze di 9-17 cifre e non contengono spazi.

ID identificatore di dati gestito: BANK_ACCOUNT_NUMBER

Paesi e aree geografiche supportati: Canada, Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

Commenti: questo identificatore di dati gestito è progettato esplicitamente per rilevare i numeri di conto bancario per il Canada e gli Stati Uniti. [Questi paesi non utilizzano i formati BBAN \(Basic Bank Account Number\) o International Bank Account Number \(IBAN\) definiti dallo standard internazionale ISO per la numerazione dei conti bancari, come specificato dalla ISO 13616.](#) Per rilevare i numeri di conto bancario di altri paesi e aree geografiche, utilizza gli identificatori di dati gestiti progettati per tali formati. Per ulteriori informazioni, consultare [Numero di conto bancario di base \(BBAN\)](#) e [Numero di conto bancario internazionale \(IBAN\)](#).

Numero di conto bancario di base (BBAN)

[Macie è in grado di rilevare i numeri di conto bancari di base \(BBANs\) conformi alla struttura BBAN definita dallo standard internazionale ISO per la numerazione dei conti bancari, come specificato dalla ISO 13616.](#) Ciò include quelli BBANs che non contengono spazi o utilizzano separatori di spazi o trattini, ad esempio, e. NWBK60161331926819 NWBK 6016 1331 9268 19 NWBK-6016-1331-9268-19

ID identificatore di dati gestito: a seconda del paese o dell'area geografica, FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

Paesi e aree geografiche supportati: Francia, Germania, Italia, Spagna, Regno Unito

Parola chiave richiesta: Sì. La tabella seguente elenca le parole chiave che Macie riconosce per paesi e regioni specifici.

Paese o regione	Parole chiave
Francia	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
Germania	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartenummer, kontonummer, kreditkartenummer, sepa
Italia	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
Spagna	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
UK	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

Commenti: questi identificatori di dati gestiti possono anche rilevare i numeri di conto bancario internazionale (IBANs) conformi allo standard ISO 13616. Per ulteriori informazioni, consulta [Numero di conto bancario internazionale \(IBAN\)](#). L'identificatore di dati gestito per il Regno Unito

(UK_BANK_ACCOUNT_NUMBER) può anche rilevare i numeri di conti bancari nazionali del Regno Unito, ad esempio. 60-16-13 31926819

Data di scadenza della carta di credito

ID identificatore di dati gestito: CREDIT_CARD_EXPIRATION

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Sì. Le parole chiave includono: exp d, exp m, exp y, expiration, expiry

Commenti: Il supporto include la maggior parte dei formati di data, come tutte le cifre e le combinazioni di cifre e nomi dei mesi. I componenti della data possono essere separati da barre (/), trattini (-) o parole chiave applicabili. Ad esempio, Macie può rilevare date come 02/26,,,02/2026, Feb 2026 e. 26-Feb expY=2026, expM=02

Dati a banda magnetica della carta di credito

ID identificatore di dati gestito: CREDIT_CARD_MAGNETIC_STRIPE

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Sì. Le parole chiave includono: card data, iso7813, mag, magstripe, stripe, swipe

Commenti: Il supporto include le tracce 1 e 2.

Numero di carta di credito

ID identificatore di dati gestito: CREDIT_CARD_NUMBER per i numeri di carta di credito che si trovano in prossimità di una parola chiave, CREDIT_CARD_NUMBER_(NO_KEYWORD) per i numeri di carte di credito che non si trovano in prossimità di una parola chiave

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Varia. Le parole chiave sono richieste da CREDIT_CARD_NUMBER identificatore di dati gestito. Le parole chiave includono: account number, american express, amex, bank card, c card, card, cc #, ccn, check card, cred card, credit, credit card, credit cards, credit no, credit num, dankort, debit, debit card, debit no, debit num, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, pmnt #, pmnt card, pmnt no, pmnt number, union pay, visa. Le parole chiave non sono richieste dal CREDIT_CARD_NUMBER_(NO_KEYWORD) identificatore di dati gestito.

Commenti: il rilevamento richiede che i dati siano una sequenza di 13-19 cifre che rispetti la formula Luhn check e utilizzi un prefisso numerico di carta standard per uno dei seguenti tipi di carte di credito: American Express, Dankort, Diner's Club, Discover, Electron, Japanese Card Bureau (JCB), Mastercard e Visa. UnionPay

Macie non riporta le occorrenze delle seguenti sequenze, che gli emittenti di carte di credito hanno riservato ai test pubblici: 1220000000000003 2222405343248877 2222990905257051 2223007648726984 2223577120017656 30569309025904 3434343434343528000700000000,3530111333300000,3566002020360505,36148900647913,364012888888818814111111111111,422222222222,4444333322221111,4462030000000000,45204740009900014,5420923878724339,5454545454545454,5455330760000018,55069004900004630490017740292441 630495060000000006331101999990016, 6759649826438453 e. 6799990100000000019 76009244561

Codice di verifica della carta di credito

ID identificatore di dati gestito: CREDIT_CARD_SECURITY_CODE

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Sì. Le parole chiave includono: card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

Commenti: Nessuno

Numero di conto bancario internazionale (IBAN)

Macie è in grado di rilevare i numeri di conto bancari internazionali (IBANs) composti da un massimo di 34 caratteri alfanumerici, inclusi elementi come il codice del paese. [Più specificamente, Macie è in grado di rilevare IBANs che sono conformi allo standard internazionale ISO per la numerazione dei conti bancari, come specificato dalla ISO 13616.](#) Ciò include quelli IBANs che non contengono spazi o utilizzano separatori di spazio o trattino, ad esempio, e. GB29NWBK60161331926819 GB29NWBK 6016 1331 9268 19 GB29-NWBK-6016-1331-9268-19 Il rilevamento include controlli di convalida basati sullo schema Modulus 97.

ID identificatore di dati gestito: a seconda del paese o della regione, ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER,

COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER,
CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER,
DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER,
EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER,
FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER,
FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER,
GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER,
GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER,
ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER,
ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER,
KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER,
LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER,
MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER,
MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER,
NETHERLANDS_BANK_ACCOUNT_NUMBER,
NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER,
PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER,
SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER,
SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER,
SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER,
SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER,
TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER,
UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER,
UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER,
VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (per le Isole Vergini Britanniche)

Paesi e aree geografiche supportati: Albania, Andorra, Bosnia-Erzegovina, Brasile, Bulgaria, Costa Rica, Croazia, Cipro, Repubblica Ceca, Danimarca, Repubblica Dominicana, Egitto, Estonia, Isole Faroe, Finlandia, Francia, Georgia, Germania, Grecia, Groenlandia, Ungheria, Islanda, Irlanda, Italia, Giordania, Kosovo, Liechtenstein, Lituania, Malta, Mauritania, Mauritania, Mauritius, Monaco, Montenegro, Paesi Bassi, Macedonia del Nord, Polonia Sen, Portogallo, San Marino, Senegal, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Timor Est, Tunisia, Türkiye, Regno Unito, Ucraina, Emirati Arabi Uniti Emirates, Isole Vergini (britanniche)

Parola chiave richiesta: No

Commenti: gli identificatori di dati gestiti per Francia, Germania, Italia, Spagna e Regno Unito possono anche rilevare i numeri di conto bancario di base (BBANs) conformi alla struttura BBAN

definita dallo standard ISO 13616, se la sequenza di caratteri è in prossimità di una parola chiave. Per ulteriori informazioni, consulta [Numero di conto bancario di base \(BBAN\)](#).

Identificatori di dati gestiti per PHI

Amazon Macie è in grado di rilevare diversi tipi di informazioni sanitarie personali (PHI) sensibili utilizzando identificatori di dati gestiti. Gli argomenti di questa pagina specificano ogni tipo e forniscono informazioni sull'identificatore di dati gestito progettato per rilevare i dati. Ogni argomento fornisce le seguenti informazioni:

- **ID identificatore di dati gestito:** specifica l'identificatore univoco (ID) per l'identificatore di dati gestito progettato per rilevare i dati. Quando [crei un processo di rilevamento di dati sensibili](#) o [configuri le impostazioni per l'individuazione automatica di dati sensibili](#), puoi utilizzare questo ID per specificare se desideri che Macie utilizzi l'identificatore di dati gestiti quando analizza i dati.
- **Paesi e aree geografiche supportati:** indica per quali paesi o aree geografiche è progettato l'identificatore di dati gestito applicabile. Se l'identificatore di dati gestito non è progettato per un particolare paese o area geografica, questo valore è Any.
- **Parola chiave obbligatoria:** specifica se il rilevamento richiede che una parola chiave sia in prossimità dei dati. Se è richiesta una parola chiave, l'argomento fornisce anche esempi di parole chiave obbligatorie. Per informazioni su come Macie utilizza le parole chiave quando analizza i dati, consulta [Requisiti delle parole chiave](#).
- **Commenti:** fornisce tutti i dettagli pertinenti che potrebbero influire sulla scelta dell'identificatore dei dati gestiti o sull'indagine sulle ricorrenze segnalate dei dati sensibili. I dettagli includono informazioni quali standard supportati, requisiti di sintassi ed eccezioni.

Gli argomenti sono elencati in ordine alfabetico per tipo di dati riservati.

Tipi di dati sensibili

- [Numero di registrazione della Drug Enforcement Agency \(DEA\)](#)
- [Numero di richiesta di assicurazione sanitaria \(HICN\)](#)
- [Numero di identificazione medica e assistenza sanitaria](#)
- [Codice HCPCS \(Healthcare Common Procedure Coding System\)](#)
- [Codice nazionale sulle droghe \(NDC\)](#)
- [National Provider Identifier \(NPI\)](#)
- [Identificatore univoco del dispositivo \(UDI\)](#)

Numero di registrazione della Drug Enforcement Agency (DEA)

ID identificativo dei dati gestiti: US_DRUG_ENFORCEMENT_AGENCY_NUMBER

Paesi e aree geografiche supportati: Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: dea number, dea registration

Commenti: Nessuno

Numero di richiesta di assicurazione sanitaria (HICN)

ID identificativo dei dati gestiti: USA_HEALTH_INSURANCE_CLAIM_NUMBER

Paesi e aree geografiche supportati: Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

Commenti: Nessuno

Numero di identificazione medica e assistenza sanitaria

L'assistenza include i numeri delle tessere sanitarie europee per l'UE e la Finlandia, i numeri di assicurazione sanitaria per la Francia, gli identificativi dei beneficiari Medicare per gli Stati Uniti, i numeri NHS per il Regno Unito e i numeri sanitari personali per il Canada.

ID identificatore di dati gestito: a seconda del paese o dell'area geografica, CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Paesi e aree geografiche supportati: Canada, UE, Finlandia, Francia, Regno Unito, Stati Uniti

Parola chiave richiesta: Sì. La tabella seguente elenca le parole chiave che Macie riconosce per paesi e regioni specifici.

Paese o regione	Parole chiave
Canada	canada healthcare number, msp number, personal healthcare number, phn, soins de santé

Paese o regione	Parole chiave
UE	assicurazione sanitaria numero, carta assicurazione numero, carte d'assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankensicherungsnummer, medical account number, numero conto medico, numéro d'assurance maladie, numéro de carte d'assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausvaikutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
Finlandia	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin, sairausvaikutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomen sairausvakuutus kortti, suomi ehic-numero, terveyskortti
Francia	carte d'assuré social, carte vitale, insurance card
UK	national health service, NHS

Paese o regione	Parole chiave
US	mbi, medicare beneficiary

Commenti: Nessuno

Codice HCPCS (Healthcare Common Procedure Coding System)

ID identificatore di dati gestito: USA_HEALTHCARE_PROCEDURE_CODE

Paesi e aree geografiche supportati: Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: current procedural terminology, hcpcs, healthcare common procedure coding system

Commenti: Nessuno

Codice nazionale sulle droghe (NDC)

ID identificatore di dati gestito: USA_NATIONAL_DRUG_CODE

Paesi e aree geografiche supportati: Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: national drug code, ndc

Commenti: Nessuno

National Provider Identifier (NPI)

ID identificatore di dati gestito: USA_NATIONAL_PROVIDER_IDENTIFIER

Paesi e aree geografiche supportati: Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: hipaa, n.p.i, national provider, npi

Commenti: Nessuno

Identificatore univoco del dispositivo (UDI)

ID identificatore di dati gestito: MEDICAL_DEVICE_UDI

Paesi e aree geografiche supportati: Stati Uniti

Parola chiave richiesta: Sì. Le parole chiave includono: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

Commenti: Macie è in grado di rilevare identificatori univoci di dispositivo (UDIs) conformi ai formati approvati dalla Food and Drug Administration statunitense. Ciò include i formati standard definiti da GS1, HIBCC e ICCBBA. Il supporto ICCBBA è per lo standard ISBT.

Identificatori di dati gestiti per PII

Amazon Macie è in grado di rilevare diversi tipi di informazioni sensibili e di identificazione personale (PII) utilizzando identificatori di dati gestiti. Gli argomenti di questa pagina elencano ogni tipo e forniscono informazioni sugli identificatori di dati gestiti progettati per rilevare i dati. Ogni argomento fornisce le seguenti informazioni:

- **ID identificatore di dati gestito:** specifica l'identificatore univoco (ID) per uno o più identificatori di dati gestiti progettati per rilevare i dati. Quando [crei un processo di rilevamento di dati sensibili](#) o [configuri le impostazioni per l'individuazione automatica di dati sensibili](#), puoi utilizzarle IDs per specificare quali identificatori di dati gestiti desideri che Macie utilizzi quando analizza i dati.
- **Paesi e aree geografiche supportati:** indica per quali paesi e aree geografiche sono progettati gli identificatori di dati gestiti applicabili. Se gli identificatori di dati gestiti non sono progettati per particolari paesi o aree geografiche, questo valore è Any.
- **Parola chiave obbligatoria:** specifica se il rilevamento richiede che una parola chiave si trovi in prossimità dei dati. Se è richiesta una parola chiave, l'argomento fornisce anche esempi di parole chiave obbligatorie. Per informazioni su come Macie utilizza le parole chiave quando analizza i dati, consulta [Requisiti delle parole chiave](#).
- **Commenti:** fornisce tutti i dettagli pertinenti che potrebbero influire sulla scelta dell'identificatore dei dati gestiti o sull'indagine sulle ricorrenze segnalate dei dati sensibili. I dettagli includono informazioni come gli standard supportati, i requisiti di sintassi e le eccezioni.

Gli argomenti sono elencati in ordine alfabetico per tipo di dati riservati.

Tipi di dati sensibili

- [Data di nascita](#)
- [Numero identificativo della patente di guida](#)
- [Numero di lista elettorale](#)
- [Nome completo](#)
- [Coordinate GPS \(Global Positioning System\)](#)
- [Cookie HTTP](#)
- [Indirizzo postale](#)

- [Numeri di carta d'identità](#)
- [Numero di previdenza nazionale \(NINO\)](#)
- [Numero di passaporto](#)
- [Numero di residenza permanente \(Green Card\)](#)
- [Numero di telefono](#)
- [Numero della carta di trasporto pubblico](#)
- [Numero di previdenza sociale \(SIN\)](#)
- [Numero di previdenza sociale \(SSN\)](#)
- [Numero identificativo del contribuente o codice fiscale](#)
- [Numero di identificazione del veicolo \(VIN\)](#)

Data di nascita

ID identificatore di dati gestito: DATE_OF_BIRTH

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: Sì. Le parole chiave includono: bday, b-day, birth date, birthday, date of birth, dob

Commenti: Il supporto include la maggior parte dei formati di data, come tutte le cifre e le combinazioni di cifre e nomi dei mesi. I componenti della data possono essere separati da spazi, barre (/) o trattini (-).

Numero identificativo della patente di guida

ID identificatore di dati gestito: a seconda del paese o della regione, AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE,

SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

Paesi e aree geografiche supportati: Australia, Austria, Belgio, Bulgaria, Canada, Croazia, Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, India, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito, Stati Uniti

Parola chiave richiesta: Sì. La tabella seguente elenca le parole chiave che Macie riconosce per paesi e regioni specifici.

Paese o regione	Parole chiave
Australia	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
Austria	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
Belgio	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
Bulgaria	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
Canada	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence,

Paese o regione	Parole chiave
	drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
Croazia	vozačka dozvola
Cipro	άδεια οδήγησης
Repubblica Ceca	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský průkaz, řidičský průkaz
Danimarca	kørekort, kørekortnummer
Estonia	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
Finlandia	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
Francia	permis de conduire
Germania	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
Grecia	δεια οδήγησης, adeia odigisis
Ungheria	illesztőprogramok lic, jogosítvány, jogsí, licencszám, vezető engedély, vezetői engedély

Paese o regione	Parole chiave
India	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
Irlanda	ceadúnas tiomána
Italia	patente di guida, patente di guida numero, patente guida, patente guida numero
Lettonia	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
Lituania	vairuotojo pažymėjimas
Lussemburgo	fahrerlaubnis, fährerschäin
Malta	licenzja tas-sewqan
Paesi Bassi	permis de conduire, rijbewijs, rijbewijsnummer
Polonia	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
Portogallo	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução
Romania	numărul permisului de conducere, permis de conducere

Paese o regione	Parole chiave
Slovacchia	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
Slovenia	vozniško dovoljenje
Spagna	carnet conductor, el carnet de conductor, licencia conductor, licencia de manejo, número carnet conductor, número de carnet de conductor, número de permiso conductor, número de permiso de conductor, número licencia conductor, número permiso conductor, permiso conducción, permiso conductor, permiso de conducción
Svezia	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.
UK	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

Paese o regione	Parole chiave
US	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

Commenti: Nessuno

Numero di lista elettorale

ID identificatore di dati gestito: UK_ELECTORAL_ROLL_NUMBER

Paesi e aree geografiche supportati: Regno Unito

Parola chiave richiesta: Sì. Le parole chiave includono: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

Commenti: Nessuno

Nome completo

ID identificatore di dati gestito: NAME

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: Macie è in grado di rilevare solo i nomi completi. Il supporto è limitato ai set di caratteri latini.

Coordinate GPS (Global Positioning System)

ID identificatore di dati gestito: LATITUDE_LONGITUDE

Paesi e aree geografiche supportati: Qualsiasi, se le coordinate sono in prossimità di una parola chiave in inglese.

Parola chiave richiesta: Sì. Le parole chiave includono: coordinate, coordinates, lat long, latitude longitude, position

Commenti: Macie è in grado di rilevare le coordinate GPS se le coordinate di latitudine e longitudine sono memorizzate come coppia e sono in formato DD (Decimal Degrees), ad esempio. 41.948614, -87.655311 Il supporto non include il rilevamento delle coordinate nel formato Degrees Decimal Minutes (DDM), ad esempio 41°56.9168'N 87°39.3187'W, o nel formato Degrees, Minutes, Seconds (DMS), ad esempio. 41°56'55.0104"N 87°39'19.1196"W

Cookie HTTP

ID identificatore di dati gestito: HTTP_COOKIE

Paesi e aree geografiche supportati: Qualsiasi

Parola chiave richiesta: No

Commenti: il rilevamento richiede un campo completo Cookie o un'Set-Cookie intestazione. L'intestazione può includere una o più coppie nome-valore, ad esempio: e. Set-Cookie: id=TWlrZQ Cookie: session=3948; lang=en

Indirizzo postale

ID identificatore di dati gestito: ADDRESS (per Australia, Canada, Francia, Germania, Italia, Spagna, Regno Unito e Stati Uniti), BRAZIL_CEP_CODE (per il Código de Endereçamento Postal del Brasile)

Paesi e aree geografiche supportati: Australia, Brasile, Canada, Francia, Germania, Italia, Spagna, Regno Unito, Stati Uniti

Parola chiave richiesta: Varia. Le parole chiave non sono richieste dal ADDRESS identificatore di dati gestito. Le parole chiave sono richieste dal BRAZIL_CEP_CODE identificatore di dati gestito. Le parole chiave includono: cep, código de endereçamento postal, código postal, codigo postal

Commenti: sebbene una parola chiave non sia richiesta dal ADDRESS identificatore di dati gestito, il rilevamento richiede che un indirizzo includa il nome di una città o di un luogo e il codice postale o postale corrispondente in un paese o un'area geografica supportati. Il BRAZIL_CEP_CODE l'identificatore di dati gestito può rilevare solo la parte del Código de Endereçamento Postal (CEP) di un indirizzo.

Numeri di carta d'identità

Il supporto include: numeri Aadhaar per l'India; numeri Cédula de Ciudadanía per la Colombia; numeri Clave Única de Registro de Población (CURP) per il Messico; numeri di Codice Fiscale per l'Italia; numeri del Documento Nacional de Identidad (DNI) per Argentina e Spagna; codici dell'Istituto nazionale francese di statistica e studi economici (INSEE); numeri delle carte d'identità nazionali tedesche; registro Numeri Geral (RG) per il Brasile e numeri Rol Único Nacional (RUN) per il Cile.

ID identificatore di dati gestito: a seconda del paese o della regione,

ARGENTINA_DNI_NUMBER, BRAZIL_RG_NUMBER, CHILE_RUT_NUMBER, COLOMBIA_CITIZENSHIP_CARD_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, MEXICO_CURP_NUMBER, SPAIN_DNI_NUMBER

Paesi e aree geografiche supportati: Argentina, Brasile, Cile, Colombia, Francia, Germania, India, Italia, Messico, Spagna

Parola chiave richiesta: Sì. La tabella seguente elenca le parole chiave che Macie riconosce per paesi e regioni specifici.

Paese o regione	Parole chiave
Argentina	dni, dni#, d.n.i., documento nacional de identidad
Brasile	registro geral, rg
Cile	identidad número, nacional identidad, national unique role, nationaluniqueroleID#, número identificación, rol único nacional, rol único tributario, run, run#, r.u.n., rut, rut#, r.u.t., unique national number, unique national role, unique tax registry, unique tax role, unique tributary number, unique tributary role
Colombia	cédula de ciudadanía, documento de identificación
Francia	assurance sociale, carte nationale d'identité, cni, code sécurité sociale, French social

Paese o regione	Parole chiave
	security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
Germania	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
India	aadhaar, aadhar, adhaar, uidai
Italia	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Messico	clave personal identidad, clave única, clave única de registro de población, clavepersonalidentidad, curp, registration code, registry code, personal identidad clave, population code
Spagna	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationalidno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

Commenti: l'identificatore di dati gestito per il Cile (CHILE_RUT_NUMBER) è progettato per rilevare sia i numeri Rol Único Nacional (RUN) che i numeri Rol Único Tributario (RUT). Per entrambi i tipi di numero, Macie non segnala le occorrenze in cui tutte le cifre sono zero, ad esempio perché sono comunemente usate come esempi. 00000000-K

Sebbene i numeri DNI per Argentina e Spagna abbiano sintassi diverse, esistono delle somiglianze tra loro. Pertanto, Macie potrebbe riportare un numero DNI per l'Argentina come numero DNI per la Spagna o viceversa. Inoltre, Macie non riporta le occorrenze delle seguenti sequenze di caratteri, che vengono comunemente utilizzate come numeri DNI di esempio: e. 99999999 99.999.999 Macie inoltre non segnala le occorrenze costituite solo da zeri, ad esempio, e. 0000000000 00.000.000

Numero di previdenza nazionale (NINO)

ID identificatore di dati gestito: UK_NATIONAL_INSURANCE_NUMBER

Paesi e aree geografiche supportati: Regno Unito

Parola chiave richiesta: Sì. Le parole chiave includono: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenummer, nin, nino

Commenti: Nessuno

Numero di passaporto

ID identificatore di dati gestito: a seconda del paese o della regione, CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

Paesi e aree geografiche supportati: Canada, Francia, Germania, Italia, Spagna, Regno Unito, Stati Uniti

Parola chiave richiesta: Sì. La tabella seguente elenca le parole chiave che Macie riconosce per paesi e regioni specifici.

Paese o regione	Parole chiave
Canada	pasport, pasport#, passport, passport#, passportno, passportno#
Francia	numéro de pasport, pasport, pasport #, pasport n °, pasport non
Germania	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass-nr, reisepassnummer

Paese o regione	Parole chiave
Italia	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
Spagna	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport
UK	pasport #, pasport n °, pasport non, pasportn °, passport #, passport no, passport number, passport#, passportid
US	passport, travel document

Commenti: Nessuno

Numero di residenza permanente (Green Card)

ID identificatore di dati gestito: CANADA_NATIONAL_IDENTIFICATION_NUMBER

Paesi e aree geografiche supportati: Canada

Parola chiave richiesta: Sì. Le parole chiave includono: carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number, permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

Commenti: Nessuno

Numero di telefono

ID identificatore di dati gestito: a seconda del paese o della regione, BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

Paesi e aree geografiche supportati: Brasile, Canada, Francia, Germania, Italia, Spagna, Regno Unito, Stati Uniti

Parola chiave richiesta: Varia. Se una parola chiave si trova in prossimità dei dati, il numero non deve includere il prefisso internazionale. Le parole chiave includono: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. Per il Brasile, le parole chiave includono anche: cel, celular, fone, móvel, número residencial, numero residencial, telefone. Se una parola chiave non si trova in prossimità dei dati, il numero deve includere un prefisso internazionale.

Commenti: per gli Stati Uniti, l'assistenza include numeri verdi.

Numero della carta di trasporto pubblico

ID identificativo dei dati gestiti: ARGENTINA_TARJETA_SUBE

Paesi e aree geografiche supportati: Argentina

Parola chiave richiesta: Sì. Le parole chiave includono: sistema único de boleto electrónico, sube

Commenti: Macie è in grado di rilevare numeri di carta a 16 cifre del Sistema Único de Boleto Electrónico (SUBE) che iniziano con e aderiscono alla formula di controllo Luhn. 6061 I componenti dei numeri di carta possono essere separati da spazi o trattini (-) oppure non utilizzare un separatore, ad esempio, e. 6061 1234 1234 1234 6061-1234-1234-1234 6061123412341234

Numero di previdenza sociale (SIN)

ID identificativo dei dati gestiti: CANADA_SOCIAL_INSURANCE_NUMBER

Paesi e aree geografiche supportati: Canada

Parola chiave richiesta: Sì. Le parole chiave includono: canadian id, numéro d'assurance sociale, sin, social insurance number

Commenti: Nessuno

Numero di previdenza sociale (SSN)

ID identificatore di dati gestito: a seconda del paese o della regione, SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Paesi e aree geografiche supportati: Spagna, Stati Uniti

Parola chiave richiesta: Sì. Per la Spagna, le parole chiave includono: número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#. Per gli Stati Uniti, le parole chiave includono: social security, ss#, ssn.

Commenti: Nessuno

Numero identificativo del contribuente o codice fiscale

Il supporto include: codici CUIL e CUIT per l'Argentina; numeri CIF, NIE e NIF per la Spagna; numeri CNPJ e CPF per il Brasile; numeri Codice Fiscale per l'Italia; per gli Stati Uniti; numeri NIT per la Colombia; ITINs per l' PANs India; numeri RFC per il Messico; numeri RUN e RUT per il Cile; numeri Steueridentifikationsnummer per la Germania; per Australia, per la Francia, e numeri TRN e UTR per il Regno Unito. TFNs TINs

ID identificatore di dati gestito: a seconda del paese o della regione, ARGENTINA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER, ARGENTINA_ORGANIZATION_TAX_IDENTIFICATION_NUMBER, AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, CHILE_RUT_NUMBER, COLOMBIA_INDIVIDUAL_NIT_NUMBER, COLOMBIA_ORGANIZATION_NIT_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, MEXICO_INDIVIDUAL_RFC_NUMBER, MEXICO_ORGANIZATION_RFC_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Paesi e aree geografiche supportati: Argentina, Australia, Brasile, Cile, Colombia, Francia, Germania, India, Italia, Messico, Spagna, Regno Unito, Stati Uniti

Parola chiave richiesta: Sì. La tabella seguente elenca le parole chiave che Macie riconosce per paesi e regioni specifici.

Paese o regione	Parole chiave
Argentina	argentina taxpayer id, clave única de identificación tributaria, cuil, c.u.i.l, cuil, c.u.i.t, número de identificación fiscal, número de contribuyente, unified labor identification code

Paese o regione	Parole chiave
Australia	tax file number, tfn
Brasile	cadastro de pessoa física, cadastro de pessoa física, cadastro de pessoas físicas, cadastro de pessoas físicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa jurídica, cnpj, cpf
Cile	identidad número, nacional identidad, national unique role, nationaluniqueID#, número identificación, rol único nacional, rol único tributario, run, run#, r.u.n., rut, rut#, r.u.t., unique national number, unique national role, unique tax registry, unique tax role, unique tributary number, unique tributary role
Colombia	nit, nit., nit#, n.i.t.
Francia	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
Germania	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
India	e-pan, pan card, pan number, permanent account number
Italia	codice fiscale, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Messico	código del registro federal de contribuyentes, identificación de impuestos, identificación de impuestos, impuesto al valor agregado, iva, iva#, i.v.a., registro federal de contribuyentes, rfc, rfc#, r.f.c.

Paese o regione	Parole chiave
Spagna	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
UK	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
US	i.t.i.n., individual taxpayer identification number, itin

Commenti: l'identificatore di dati gestito per il Cile (CHILE_RUT_NUMBER) è progettato per rilevare sia i numeri Rol Único Nacional (RUN) che i numeri Rol Único Tributario (RUT). Per i numeri del Registro Federal de Contribuyentes (RFC) per il Messico, Macie non riporta le occorrenze delle seguenti sequenze di caratteri, che vengono comunemente utilizzate come numeri RFC di esempio: e. XAXX010101000 XEXX010101000

Per diversi tipi di codice identificativo e di riferimento dei contribuenti, Macie non riporta le occorrenze in cui tutte le cifre sono zero, ad esempio, e. 000000000-K 0000000000 00.000.000 Questo perché l'uso dei soli zeri è comune negli esempi di determinati tipi di identificazione e numeri di riferimento dei contribuenti.

Numero di identificazione del veicolo (VIN)

ID identificativo dei dati gestiti: VEHICLE_IDENTIFICATION_NUMBER

Paesi e aree geografiche supportati: Qualsiasi, se il VIN è in prossimità di una parola chiave in una delle seguenti lingue: inglese, francese, tedesco, lituano, polacco, portoghese, rumeno o spagnolo.

Parola chiave richiesta: Sì. Le parole chiave includono: Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de

Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

Commenti: Macie è in grado di rilevare VINs che consistono in una sequenza di 17 caratteri e aderiscono agli standard ISO 3779 e 3780. Questi standard sono stati progettati per l'uso a livello mondiale.

Creazione di identificatori di dati personalizzati

Oltre a utilizzare gli identificatori di dati gestiti forniti da Amazon Macie, puoi creare e utilizzare identificatori di dati personalizzati. Un identificatore di dati personalizzato è un insieme di criteri che definisci per rilevare dati sensibili negli oggetti Amazon Simple Storage Service (Amazon S3). I criteri sono costituiti da un'espressione regolare (regex) che definisce uno schema di testo da abbinare e, facoltativamente, sequenze di caratteri e una regola di prossimità che perfeziona i risultati. Le sequenze di caratteri possono essere: parole chiave, che sono parole o frasi che devono trovarsi in prossimità di testo che corrisponde all'espressione regolare, oppure parole ignorate, che sono parole o frasi da escludere dai risultati.

Con gli identificatori di dati personalizzati, puoi definire criteri di rilevamento che riflettono scenari particolari, proprietà intellettuale o dati proprietari dell'organizzazione. Ad esempio, è possibile rilevare i numeri di account dei dipendenti IDs, dei clienti o le classificazioni interne dei dati. Se configuri [processi di rilevamento di dati sensibili](#) o di [rilevamento automatico di dati sensibili](#) per utilizzare questi identificatori, puoi integrare gli identificatori di [dati gestiti forniti da Macie](#).

Oltre ai criteri di rilevamento, puoi facoltativamente configurare impostazioni di gravità personalizzate per i risultati prodotti da un identificatore di dati personalizzato. Per impostazione predefinita, Macie assegna la severità Media a tutti i risultati prodotti da un identificatore di dati personalizzato. La severità non cambia in base al numero di occorrenze di testo che corrispondono ai criteri di rilevamento di un identificatore. Se si configurano impostazioni di gravità personalizzate, la gravità può essere basata sul numero di occorrenze di testo che soddisfano i criteri.

Argomenti

- [Opzioni di configurazione per identificatori di dati personalizzati](#)
- [Creazione di un identificatore di dati personalizzato](#)
- [Eliminazione di un identificatore di dati personalizzato](#)

Opzioni di configurazione per identificatori di dati personalizzati

Utilizzando identificatori di dati personalizzati, puoi definire criteri personalizzati per rilevare dati sensibili negli oggetti Amazon Simple Storage Service (Amazon S3). Puoi integrare gli [identificatori di dati gestiti forniti](#) da Amazon Macie e rilevare dati sensibili che riflettono scenari particolari, proprietà intellettuale o dati proprietari della tua organizzazione.

Ogni identificatore di dati personalizzato specifica i criteri di rilevamento e, facoltativamente, le impostazioni di gravità per i risultati prodotti dall'identificatore. I criteri di rilevamento specificano un'espressione regolare che definisce uno schema di testo da abbinare in un oggetto S3. I criteri possono anche specificare sequenze di caratteri e una regola di prossimità che perfeziona i risultati. Le impostazioni di severità specificano quale severità assegnare ai risultati. La severità può essere basata sul numero di occorrenze di testo che corrispondono ai criteri di rilevamento dell'identificatore.

Argomenti

- [Criteri di rilevamento](#)
- [Impostazioni di gravità per i risultati](#)

Criteri di rilevamento

Quando si crea un identificatore di dati personalizzato, si specifica un'espressione regolare (regex) che definisce uno schema di testo da abbinare. Puoi anche specificare sequenze di caratteri, come parole e frasi, e una regola di prossimità che perfeziona i risultati. Le sequenze di caratteri possono essere: parole chiave, che sono parole o frasi che devono trovarsi in prossimità di testo che corrisponde all'espressione regolare, oppure ignorare le parole, che sono parole o frasi da escludere dai risultati.

Per l'espressione regolare, Amazon Macie supporta un sottoinsieme della sintassi del pattern fornita dalla libreria [Perl Compatible Regular Expressions](#) (PCRE). Tra i costrutti forniti dalla libreria PCRE, Macie non supporta i seguenti elementi del pattern:

- Riferimenti all'indietro
- Acquisizione di gruppi
- Modelli condizionali
- Codice incorporato
- Bandiere con pattern globali, ad esempio `/i/m`, e `/x`

- Schemi ricorsivi
- Asserzioni a larghezza zero positive e negative e look-ahead, ad esempio,, e `?= ?! ?<= ?<!`

L'espressione regolare può contenere fino a 512 caratteri.

Per creare un modello regex efficace per un identificatore di dati personalizzato, tieni presente i seguenti suggerimenti e raccomandazioni:

- Utilizzate gli anchors (`^` or `$`) solo se vi aspettate che il pattern appaia all'inizio o alla fine di un file, non all'inizio o alla fine di una riga.
- Per motivi di prestazioni, Macie limita la dimensione dei gruppi di ripetizioni limitati. Ad esempio, `\d{100,1000}` non verrà compilato in Macie. Per approssimare questa funzionalità, puoi usare una ripetizione aperta come. `\d{100,}`
- Per fare in modo che alcune parti di un pattern non facciano distinzione tra maiuscole e minuscole, potete usare il `(?i)` costruito anziché il flag. `/i`
- Non è necessario ottimizzare manualmente i prefissi o le alternanze. Ad esempio, passare `/hello|hi|hey/` a non `/h(?:ello|i|ey)/` migliorerà le prestazioni.
- Per motivi di prestazioni, Macie limita il numero di jolly ripetuti. Ad esempio, `a*b*a*` non verrà compilato in Macie.

Per proteggersi da espressioni malformate o di lunga durata, Macie testa automaticamente i modelli regex rispetto a una raccolta di testo di esempio quando crei un identificatore di dati personalizzato. Se c'è un problema con l'espressione regolare, Macie restituisce un errore che descrive il problema.

Oltre all'espressione regolare, puoi facoltativamente specificare sequenze di caratteri e una regola di prossimità per rifinire i risultati.

Parole chiave

Si tratta di sequenze di caratteri specifiche che devono trovarsi in prossimità del testo che corrisponde al modello regex. I requisiti di prossimità variano in base al formato di archiviazione o al tipo di file di un oggetto S3:

- **Dati colonnari strutturati:** Macie include un risultato se il testo corrisponde allo schema regex e una parola chiave è nel nome del campo o della colonna che memorizza il testo, oppure se il testo è preceduto da ed entro la distanza massima di corrispondenza di una parola chiave nello stesso campo o valore di cella. Questo è il caso delle cartelle di lavoro di Microsoft Excel, dei file CSV e dei file TSV.

- **Dati strutturati basati su record:** Macie include un risultato se il testo corrisponde allo schema regex e se il testo si trova entro la distanza di corrispondenza massima di una parola chiave. La parola chiave può essere contenuta nel nome di un elemento nel percorso del campo o dell'array che memorizza il testo, oppure può precedere e far parte dello stesso valore nel campo o nell'array che memorizza il testo. Questo è il caso dei contenitori di oggetti Apache Avro, dei file Apache Parquet, dei file JSON e dei file JSON Lines.
- **Dati non strutturati:** Macie include un risultato se il testo corrisponde allo schema regex e il testo è preceduto da e entro la distanza di corrispondenza massima di una parola chiave. È il caso dei file Adobe Portable Document Format, dei documenti Microsoft Word, dei messaggi di posta elettronica e dei file di testo non binari diversi dai file CSV, JSON, JSON Lines e TSV. Ciò include tutti i dati strutturati, come le tabelle, in questi tipi di file.

È possibile specificare fino a 50 parole chiave. Ogni parola chiave può contenere da 3 a 90 caratteri UTF-8. Le parole chiave non distinguono tra maiuscole e minuscole.

Distanza massima della partita

Questa è una regola di prossimità basata su caratteri per le parole chiave. Macie usa questa impostazione per determinare se una parola chiave precede il testo che corrisponde allo schema regex. L'impostazione definisce il numero massimo di caratteri che possono esistere tra la fine di una parola chiave completa e la fine del testo che corrisponde allo schema regex. Macie include un risultato del testo:

- Corrisponde al modello regex,
- Si verifica dopo almeno una parola chiave completa e
- Si verifica entro la distanza specificata dalla parola chiave.

Altrimenti, Macie esclude il testo dai risultati.

È possibile specificare una distanza di 1—300 caratteri. La distanza predefinita è di 50 caratteri. Per ottenere risultati ottimali, questa distanza deve essere maggiore del numero minimo di caratteri di testo che l'espressione regolare è progettata per rilevare. Se solo una parte del testo rientra nella distanza massima di corrispondenza di una parola chiave, Macie non la include nei risultati.

Ignora le parole

Si tratta di sequenze di caratteri specifiche da escludere dai risultati. Se il testo corrisponde allo schema regex ma contiene una parola da ignorare, Macie non la include nei risultati.

Puoi specificare fino a 10 parole da ignorare. Ogni parola da ignorare può contenere da 4 a 90 caratteri UTF-8. Le parole da ignorare distinguono tra maiuscole e minuscole.

Note

Prima di creare un identificatore di dati personalizzato, ti consigliamo vivamente di testarne e perfezionarne i criteri di rilevamento con dati di esempio. Poiché gli identificatori di dati personalizzati vengono utilizzati dai processi di rilevamento di dati sensibili, non è possibile modificare un identificatore di dati personalizzato dopo averlo creato. Ciò contribuisce a garantire una cronologia immutabile delle rilevazioni e dei risultati delle scoperte di dati sensibili per i controlli o le indagini sulla privacy e la protezione dei dati da te eseguiti. Puoi testare i criteri di rilevamento utilizzando la console Amazon Macie o l'API Amazon Macie. Per testare i criteri utilizzando la console, utilizza le opzioni nella sezione Valuta durante la creazione dell'identificatore di dati personalizzato. Per testare i criteri a livello di codice, utilizza il [TestCustomDataIdentifier](#) funzionamento dell'API Amazon Macie. Se utilizzi il AWS Command Line Interface, esegui il [test-custom-data-identifier](#) comando per testare i criteri.

Per una dimostrazione di come le parole chiave possono aiutarti a trovare dati sensibili ed evitare falsi positivi, guarda il seguente video: [Come Amazon Macie utilizza le parole chiave per scoprire dati sensibili](#).

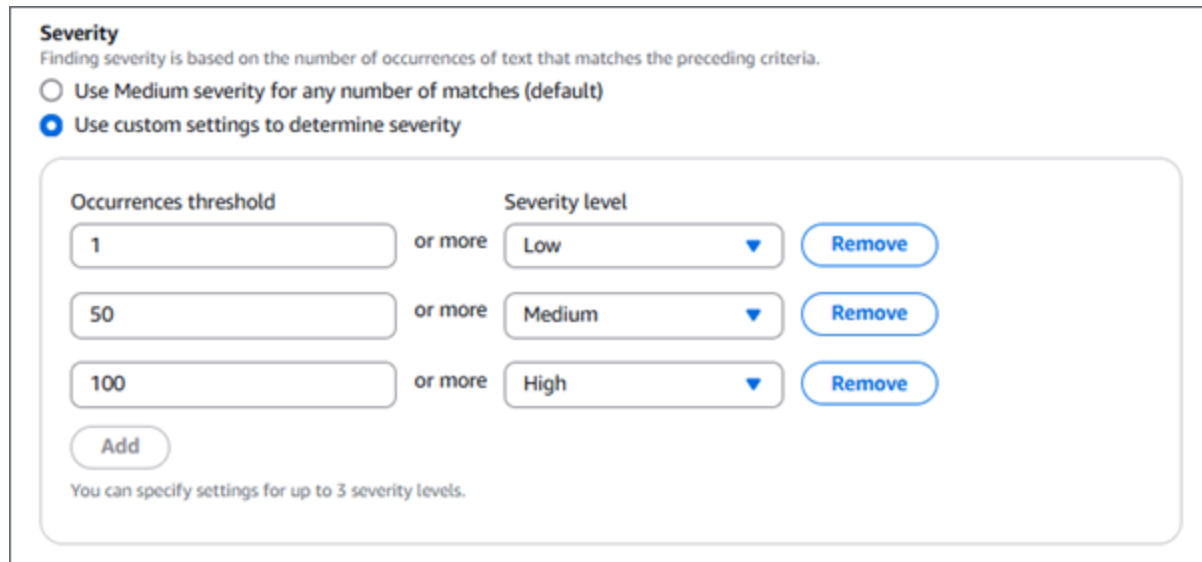
Impostazioni di gravità per i risultati

Quando crei un identificatore di dati personalizzato, puoi anche specificare impostazioni di gravità personalizzate per le rilevazioni di dati sensibili prodotte dall'identificatore. Per impostazione predefinita, Amazon Macie assegna la gravità Media a tutti i risultati prodotti da un identificatore di dati personalizzato. Se un oggetto S3 contiene almeno un'occorrenza di testo che corrisponde ai criteri di rilevamento, Macie assegna automaticamente la severità Media al risultato risultante.

Con le impostazioni di gravità personalizzate, si specifica quale severità assegnare in base al numero di occorrenze di testo che corrispondono ai criteri di rilevamento. È possibile definire soglie di occorrenza per un massimo di tre livelli di gravità: Basso (meno grave), Medio e Alto (più grave). Una soglia di occorrenza è il numero minimo di corrispondenze che devono esistere in un oggetto S3

per produrre un risultato con la gravità specificata. Se si specifica più di una soglia, le soglie devono essere in ordine crescente per gravità, passando da Bassa a Alta.

Ad esempio, l'immagine seguente mostra le impostazioni di gravità che specificano tre soglie di occorrenza, una per ogni livello di gravità supportato da Macie.



Severity
Finding severity is based on the number of occurrences of text that matches the preceding criteria.

☐ Use Medium severity for any number of matches (default)

☒ Use custom settings to determine severity

Occurrences threshold		Severity level	
1	or more	Low	Remove
50	or more	Medium	Remove
100	or more	High	Remove

Add

You can specify settings for up to 3 severity levels.

La tabella seguente indica la gravità dei risultati prodotti dall'identificatore di dati personalizzato.

Soglia di occorrenze	Livello di gravità	Risultato
1	Bassa	Se un oggetto S3 contiene da 1 a 49 occorrenze di testo che corrispondono ai criteri di rilevamento, la gravità del risultato risultante è Bassa.
50	Media	Se un oggetto S3 contiene 50-99 occorrenze di testo che corrispondono ai criteri di rilevamento, la gravità del risultato risultante è Media.
100	Elevata	Se un oggetto S3 contiene 100 o più occorrenze di testo che corrispondono ai criteri

Soglia di occorrenze	Livello di gravità	Risultato
		di rilevamento, la gravità del risultato risultante è Alta.

Puoi anche utilizzare le impostazioni di gravità per specificare se creare o meno un risultato. Se un oggetto S3 contiene un numero di occorrenze inferiore alla soglia di occorrenze più bassa, Macie non crea un risultato.

Creazione di un identificatore di dati personalizzato

Un identificatore di dati personalizzato è un insieme di criteri che definisci per rilevare dati sensibili negli oggetti Amazon Simple Storage Service (Amazon S3). Quando crei un identificatore di dati personalizzato, specifichi un'espressione regolare (regex) che definisce uno schema di testo da abbinare in un oggetto S3. Puoi anche specificare sequenze di caratteri e una regola di prossimità che perfezionano i risultati. Le sequenze di caratteri possono essere: parole chiave, che sono parole o frasi che devono trovarsi in prossimità di testo che corrisponde all'espressione regolare, oppure ignorare le parole, che sono parole o frasi da escludere dai risultati. Utilizzando identificatori di dati personalizzati, puoi integrare gli [identificatori di dati gestiti forniti](#) da Amazon Macie e rilevare dati sensibili che riflettono scenari particolari, proprietà intellettuale o dati proprietari della tua organizzazione.

Ad esempio, molte aziende hanno una sintassi specifica per i dipendenti. IDs Una di queste sintassi potrebbe essere: una lettera maiuscola che indica se un dipendente è un dipendente a tempo pieno (F) o part-time (P), seguita da un trattino (—), seguita da una sequenza di otto cifre che identifica il dipendente. Alcuni esempi sono: F—12345678 per un dipendente a tempo pieno e P—87654321 per un dipendente a tempo parziale. Per rilevare i dipendenti IDs che utilizzano questa sintassi, è possibile creare un identificatore di dati personalizzato che specifichi la seguente espressione regolare: `[A-Z]-\d{8}` Per affinare l'analisi ed evitare falsi positivi, puoi anche configurare l'identificatore per utilizzare parole chiave (employeeandemployee ID) e una distanza di corrispondenza massima di 20 caratteri. In base a questi criteri, i risultati includono il testo che corrisponde all'espressione regolare se il testo si trova dopo la parola chiave employee o employee ID e tutto il testo si trova entro 20 caratteri da una di tali parole chiave.

Per una dimostrazione di come le parole chiave possono aiutarti a trovare dati sensibili ed evitare falsi positivi, guarda il seguente video: [Come Amazon Macie utilizza le parole chiave per scoprire dati sensibili](#).

Oltre ai criteri di rilevamento, puoi facoltativamente specificare impostazioni di gravità personalizzate per i risultati prodotti da un identificatore di dati personalizzato. La severità può essere basata sul numero di occorrenze di testo che corrispondono ai criteri di rilevamento dell'identificatore. Se non specifichi queste impostazioni, Macie assegna automaticamente la severità Media a tutti i risultati prodotti dall'identificatore. La severità non cambia in base al numero di occorrenze di testo che corrispondono ai criteri di rilevamento dell'identificatore.

Per informazioni dettagliate su queste e altre impostazioni, consulta [Opzioni di configurazione per identificatori di dati personalizzati](#)

Per creare un identificatore di dati personalizzato

Puoi creare un identificatore di dati personalizzato utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per creare un identificatore di dati personalizzato utilizzando la console Amazon Macie.

Per creare un identificatore di dati personalizzato

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Identificatori di dati personalizzati.
3. Scegli Create (Crea) .
4. In Nome, inserisci un nome per l'identificatore di dati personalizzato. Il nome può contenere fino a un massimo di 128 caratteri.
5. Per Descrizione, inserisci facoltativamente una breve descrizione dell'identificatore di dati personalizzato. La descrizione può contenere fino a 512 caratteri.

Note

Evita di includere dati sensibili nel nome o nella descrizione di un identificatore di dati personalizzato. Altri utenti del tuo account potrebbero essere in grado di accedere al nome o alla descrizione, a seconda delle azioni che possono eseguire in Macie.

6. Per Espressione regolare, inserisci l'espressione regolare (regex) che definisce lo schema di testo da abbinare. L'espressione regolare può contenere fino a 512 caratteri.

Macie supporta un sottoinsieme della sintassi del pattern fornita dalla libreria [Perl Compatible Regular Expressions](#) (PCRE). Per ulteriori dettagli e suggerimenti, consultate [Criteri di rilevamento](#) per identificatori di dati personalizzati.

7. Per Parole chiave, inserisci facoltativamente fino a 50 sequenze di caratteri (separate da virgole) per definire un testo specifico che deve essere in prossimità del testo che corrisponde allo schema regex.

Macie include un'occorrenza nei risultati solo se il testo corrisponde al modello regex e il testo si trova entro la distanza di corrispondenza massima di una di queste parole chiave. Ogni parola chiave può contenere da 3 a 90 caratteri UTF-8. Le parole chiave non distinguono tra maiuscole e minuscole.

8. Per Ignora parole, inserisci facoltativamente fino a 10 sequenze di caratteri (separate da virgole) che definiscono un testo specifico da escludere dai risultati.

Macie esclude un'occorrenza dai risultati se il testo corrisponde al modello regex ma contiene una di queste parole da ignorare. Ogni parola da ignorare può contenere da 4 a 90 caratteri UTF-8. Le parole da ignorare distinguono tra maiuscole e minuscole.

9. Per Distanza massima di corrispondenza, inserisci facoltativamente il numero massimo di caratteri che possono esistere tra la fine di una parola chiave e la fine del testo che corrisponde al modello regex.

Macie include un'occorrenza nei risultati solo se il testo corrisponde al modello regex e il testo si trova entro questa distanza da una parola chiave completa. La distanza può essere compresa tra 1 e 300 caratteri. La distanza predefinita è di 50 caratteri.

10. Per Severità, scegli come determinare la gravità dei dati sensibili rilevati dall'identificatore di dati personalizzato:
 - Per assegnare automaticamente la severità media a tutti i risultati, scegli Usa la severità media per un numero qualsiasi di corrispondenze (impostazione predefinita). Con questa opzione, Macie assegna automaticamente la gravità Media a un risultato se l'oggetto S3 interessato contiene una o più occorrenze di testo che corrispondono ai criteri di rilevamento.
 - Per assegnare la gravità in base alle soglie di occorrenze specificate, scegliete Usa impostazioni personalizzate per determinare la gravità. Utilizza quindi le opzioni Soglia di occorrenze e Livello di gravità per specificare il numero minimo di corrispondenze che devono esistere in un oggetto S3 per produrre un risultato con una gravità selezionata.

È possibile specificare fino a tre soglie di occorrenza, una per ogni livello di gravità supportato da Macie: Bassa (meno grave), Media o Alta (più grave). Se ne specifichi più di una, le soglie devono essere in ordine crescente per gravità, passando da Basso ad Alto. Se un oggetto S3 contiene un numero di occorrenze inferiore alla soglia più bassa, Macie non crea un risultato.

11. (Facoltativo) Per Tag, scegli Aggiungi tag, quindi inserisci fino a 50 tag da assegnare all'identificatore di dati personalizzato.

Un tag è un'etichetta che definisci e assegni a determinati tipi di risorse. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

12. (Facoltativo) Per Evaluate, inserite fino a 1.000 caratteri nella casella Dati di esempio, quindi scegliete Test per verificare i criteri di rilevamento. Macie valuta i dati di esempio e riporta il numero di occorrenze di testo che corrispondono ai criteri. Puoi ripetere questo passaggio tutte le volte che vuoi per rifinire e ottimizzare i criteri.

 Note

Ti consigliamo vivamente di testare e perfezionare i criteri di rilevamento con dati di esempio. Poiché gli identificatori di dati personalizzati vengono utilizzati dai processi di rilevamento di dati sensibili, non è possibile modificare un identificatore di dati personalizzato dopo averlo creato. Questo aiuta a garantire una cronologia immutabile delle scoperte e delle scoperte di dati sensibili.

13. Al termine, scegli Submit (Invia).

Macie verifica le impostazioni e verifica che sia in grado di compilare l'espressione regolare. Se c'è un problema con un'impostazione o con l'espressione regolare, Macie visualizza un errore che descrive il problema. Dopo aver risolto eventuali problemi, puoi salvare l'identificatore di dati personalizzato.

API

Per creare un identificatore di dati personalizzato a livello di codice, utilizza il [CreateCustomDataIdentifier](#) funzionamento dell'API Amazon Macie. Oppure, se utilizzi il AWS Command Line Interface (AWS CLI), esegui il comando. [create-custom-data-identifier](#)

Note

Prima di creare un identificatore di dati personalizzato, ti consigliamo vivamente di testarne e perfezionarne i criteri di rilevamento con dati di esempio. Poiché gli identificatori di dati personalizzati vengono utilizzati dai processi di rilevamento di dati sensibili, non è possibile modificare un identificatore di dati personalizzato dopo averlo creato. Questo aiuta a garantire una cronologia immutabile delle scoperte e delle scoperte di dati sensibili.

Per testare i criteri a livello di codice, puoi utilizzare il [TestCustomDataIdentifier](#) funzionamento dell'API Amazon Macie. Questa operazione fornisce un ambiente per la valutazione di dati di esempio con criteri di rilevamento. Se si utilizza il AWS CLI, è possibile eseguire il [test-custom-data-identifier](#) comando per testare i criteri.

Quando sei pronto per creare l'identificatore di dati personalizzato, utilizza i seguenti parametri per definirne i criteri di rilevamento:

- **regex**— Specificate l'espressione regolare (regex) che definisce il modello di testo da abbinare. L'espressione regolare può contenere fino a 512 caratteri.

Macie supporta un sottoinsieme della sintassi del pattern fornita dalla libreria [Perl Compatible Regular Expressions](#) (PCRE). Per ulteriori dettagli e suggerimenti, consultate [Criteri di rilevamento](#) per identificatori di dati personalizzati.

- **keywords**— Specificate facoltativamente sequenze da 1 a 50 caratteri (parole chiave) che devono trovarsi in prossimità del testo che corrisponde allo schema regex.

Macie include un'occorrenza nei risultati solo se il testo corrisponde allo schema regex e il testo si trova entro la distanza di corrispondenza massima di una di queste parole chiave. Ogni parola chiave può contenere da 3 a 90 caratteri UTF-8. Le parole chiave non distinguono tra maiuscole e minuscole.

- `maximumMatchDistance`— Specificate facoltativamente il numero massimo di caratteri che possono esistere tra la fine di una parola chiave e la fine del testo che corrisponde allo schema regex. Se si utilizza il AWS CLI, utilizzare il `maximum-match-distance` parametro per specificare questo valore.

Macie include un'occorrenza nei risultati solo se il testo corrisponde allo schema regex e il testo si trova entro questa distanza da una parola chiave completa. La distanza può essere compresa tra 1 e 300 caratteri. La distanza predefinita è di 50 caratteri.

- `ignoreWords`— Specificate facoltativamente sequenze da 1 a 10 caratteri (ignorate le parole) da escludere dai risultati. Se utilizzate il AWS CLI, utilizzate il `ignore-words` parametro per specificare queste sequenze di caratteri.

Macie esclude un'occorrenza dai risultati se il testo corrisponde al modello regex, ma contiene una di queste parole da ignorare. Ogni parola da ignorare può contenere da 4 a 90 caratteri UTF-8. Le parole da ignorare distinguono tra maiuscole e minuscole.

Per specificare la gravità dei dati sensibili rilevati dall'identificatore di dati personalizzato, utilizza il `severityLevels` parametro o, se utilizzi il, il parametro: `AWS CLIseverity-levels`

- Per assegnare automaticamente la MEDIUM gravità a tutti i risultati, ometti questo parametro. Macie utilizza quindi l'impostazione predefinita. Per impostazione predefinita, Macie assegna la MEDIUM gravità a un risultato se l'oggetto S3 interessato contiene una o più occorrenze di testo che corrispondono ai criteri di rilevamento.
- Per assegnare la gravità in base alle soglie di occorrenze specificate, specifica il numero minimo di corrispondenze che devono esistere in un oggetto S3 per produrre un risultato con una gravità specificata.

È possibile specificare fino a tre soglie di occorrenza, una per ogni livello di gravità supportato da Macie: LOW (meno grave) o (più grave). MEDIUM HIGH Se ne specifichi più di una, le soglie devono essere in ordine crescente per gravità, passando da a. LOW HIGH Se un oggetto S3 contiene un numero di occorrenze inferiore alla soglia più bassa, Macie non crea un risultato.

Utilizza parametri aggiuntivi per specificare un nome e altre impostazioni, come i tag, per l'identificatore di dati personalizzato. Evita di includere dati sensibili in queste impostazioni. Altri utenti del tuo account potrebbero essere in grado di accedere a questi valori, a seconda delle azioni che possono eseguire in Macie.

Quando invii la richiesta, Macie verifica le impostazioni e verifica che sia in grado di compilare l'espressione regolare. Se c'è un problema con un'impostazione o con l'espressione regolare, la richiesta fallisce e Macie restituisce un messaggio che descrive il problema. Se la richiesta ha esito positivo, riceverai un output simile al seguente:

```
{
  "customDataIdentifierId": "393950aa-82ea-4bdc-8f7b-e5be3example"
}
```

Dove `customDataIdentifierId` specifica l'identificatore univoco (ID) per l'identificatore di dati personalizzato che è stato creato.

Per recuperare e rivedere successivamente le impostazioni per l'identificatore di dati personalizzato, utilizza l'[GetCustomDataIdentifier](#) operazione o, se utilizzi il, esegui il AWS CLI comando. [get-custom-data-identifier](#) Per il `id` parametro, specifica l'ID dell'identificatore di dati personalizzato.

Gli esempi seguenti mostrano come utilizzare per AWS CLI creare un identificatore di dati personalizzato. Gli esempi creano un identificatore di dati personalizzato progettato per rilevare i dipendenti IDs che utilizzano una sintassi specifica e si trovano in prossimità di una parola chiave specificata. Gli esempi definiscono anche impostazioni di gravità personalizzate per i risultati prodotti dall'identificatore.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 create-custom-data-identifier \
--name "EmployeeIDs" \
--regex "[A-Z]-\d{8}" \
--keywords '["employee","employee ID"]' \
--maximum-match-distance 20 \
--severity-levels '[{"occurrencesThreshold":1,"severity":"LOW"},
{"occurrencesThreshold":50,"severity":"MEDIUM"},
{"occurrencesThreshold":100,"severity":"HIGH"}]' \
--description "Detects employee IDs in proximity of a keyword." \
--tags '{"Stack":"Production"}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws macie2 create-custom-data-identifier ^
--name "EmployeeIDs" ^
--regex "[A-Z]-\d{8}" ^
--keywords ["employee","employee ID"] ^
--maximum-match-distance 20 ^
--severity-levels "[{"occurrencesThreshold":1,"severity":"LOW"},
{"occurrencesThreshold":50,"severity":"MEDIUM"},{"occurrencesThreshold":100,
"severity":"HIGH"}]" ^
--description "Detects employee IDs in proximity of a keyword." ^
--tags={"Stack":"Production"}
```

Dove:

- *EmployeeIDs* è il nome dell'identificatore di dati personalizzato.
- *[A-Z]-\d{8}* è l'espressione regolare per il modello di testo a cui corrispondere.
- *employee* e *employee ID* sono parole chiave che devono trovarsi in prossimità del testo che corrisponde al modello regex.
- *20* è il numero massimo di caratteri che possono esistere tra la fine di una parola chiave e la fine del testo che corrisponde allo schema regex.
- *description* specifica una breve descrizione dell'identificatore di dati personalizzato.
- *severity-levels* definisce soglie di occorrenze personalizzate per la gravità dei risultati prodotti dall'identificatore di dati personalizzato: *LOW* per 1-49 occorrenze, per 50-99 occorrenze e *MEDIUM* per 100 o più occorrenze. *HIGH*
- *Stack* è la chiave del tag da assegnare all'identificatore di dati personalizzato. *Production* è il valore del tag per la chiave di tag specificata.

Dopo aver creato l'identificatore di dati personalizzato, puoi [creare e configurare processi di rilevamento di dati sensibili](#) per utilizzarlo o [aggiungerlo alle impostazioni per l'individuazione automatica dei dati sensibili](#).

Eliminazione di un identificatore di dati personalizzato

Dopo aver creato un identificatore di dati personalizzato, puoi eliminarlo. In tal caso, Amazon Macie soft elimina l'identificatore di dati personalizzato. Ciò significa che un record dell'identificatore di dati personalizzato rimane per il tuo account, ma è contrassegnato come eliminato. Se un identificatore di dati personalizzato ha questo stato, non puoi configurare nuovi processi di rilevamento di dati

sensibili per utilizzarlo o aggiungerlo alle impostazioni per il rilevamento automatico dei dati sensibili. Inoltre, non puoi più accedervi utilizzando la console Amazon Macie. Tuttavia, puoi recuperarne le impostazioni utilizzando l'API Amazon Macie. Se elimini un identificatore di dati personalizzato, questo non viene conteggiato nella quota di identificatori di dati personalizzati per il tuo account.

Se configuri un processo di rilevamento di dati sensibili per utilizzare un identificatore di dati personalizzato che successivamente elimini, il processo verrà eseguito come pianificato e continuerà a utilizzare l'identificatore di dati personalizzato. Ciò significa che i risultati del lavoro, sia quelli relativi ai dati sensibili che quelli relativi all'individuazione di dati sensibili, riporteranno un testo che corrisponde ai criteri dell'identificatore. Ciò contribuisce a garantire una cronologia immutabile delle rilevazioni e dei risultati delle scoperte di dati sensibili per i controlli o le indagini sulla privacy e la protezione dei dati da voi eseguiti.

Allo stesso modo, se configuri l'individuazione automatica dei dati sensibili per utilizzare un identificatore di dati personalizzato che successivamente elimini, i cicli di analisi giornalieri proseguiranno e continueranno a utilizzare l'identificatore di dati personalizzato. Ciò significa che le rilevazioni di dati sensibili, le statistiche e altri tipi di risultati continueranno a riportare il testo che corrisponde ai criteri dell'identificatore.

Prima di eliminare un identificatore di dati personalizzato, procedi come segue per impedire a Macie di utilizzarlo durante i cicli di analisi e le esecuzioni dei lavori successivi:

- Controlla le tue impostazioni per il rilevamento automatico dei dati sensibili. Se hai aggiunto l'identificatore di dati personalizzato a queste impostazioni, rimuovilo. Per ulteriori informazioni, consulta [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#).
- Esamina l'inventario dei lavori per identificare i lavori che utilizzano l'identificatore di dati personalizzato e che sono programmati per essere eseguiti in futuro. Se desideri che un lavoro smetta di utilizzare l'identificatore di dati personalizzato, puoi annullarlo. Quindi crea una copia del lavoro, modifica le impostazioni per la copia e salva la copia come nuovo lavoro. Per ulteriori informazioni, consulta [Gestione dei processi di rilevamento di dati sensibili](#).

È anche una buona idea annotare l'identificatore univoco (ID) che Macie ha assegnato all'identificatore di dati personalizzato. Questo ID ti servirà se in seguito desideri rivedere le impostazioni dell'identificatore di dati personalizzato.

Dopo aver completato le attività precedenti, elimina l'identificatore di dati personalizzato.

Per eliminare un identificatore di dati personalizzato

Puoi eliminare un identificatore di dati personalizzato utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per eliminare un identificatore di dati personalizzato utilizzando la console Amazon Macie.

Per eliminare un identificatore di dati personalizzato

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Identificatori di dati personalizzati.
3. Per annotare l'identificatore univoco (ID) per l'identificatore di dati personalizzato che desideri eliminare, scegli il nome dell'identificatore di dati personalizzato. Nella pagina visualizzata, la casella Id mostra questo ID. Dopo aver annotato l'ID, scegli nuovamente Identificatori di dati personalizzati nel riquadro di navigazione.
4. Nella pagina Identificatori di dati personalizzati, seleziona la casella di controllo relativa all'identificatore di dati personalizzato da eliminare.
5. Dal menu Actions (Operazioni), scegli Delete (Elimina).
6. Quando viene richiesta la conferma, scegli Ok.

API

Per eliminare un identificatore di dati personalizzato a livello di codice, utilizza il [DeleteCustomDataIdentifier](#) funzionamento dell'API Amazon Macie. Oppure, se utilizzi il AWS Command Line Interface (AWS CLI), esegui il comando. [delete-custom-data-identifier](#)

Per il `id` parametro, specifica l'identificatore univoco (ID) per l'identificatore di dati personalizzato che desideri eliminare. È possibile ottenere questo ID utilizzando l'[ListCustomDataIdentifiers](#) operazione. Questa operazione recupera un sottoinsieme di informazioni sugli identificatori di dati personalizzati per il tuo account. Se utilizzi il AWS CLI, puoi eseguire il [list-custom-data-identifiers](#) comando per recuperare queste informazioni.

L'esempio seguente mostra come eliminare un identificatore di dati personalizzato utilizzando AWS CLI

```
$ aws macie2 delete-custom-data-identifier --id 393950aa-82ea-4bdc-8f7b-e5be3example
```


393950aa-82ea-4bdc-8f7b-e5be3example Dov'è l'ID dell'identificatore di dati personalizzato da eliminare.

Se la richiesta ha esito positivo, Macie restituisce una risposta HTTP 200 vuota. Altrimenti, Macie restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui la richiesta non è riuscita.

Per rivedere le impostazioni di un identificatore di dati personalizzato dopo averlo eliminato, utilizza il [GetCustomDataIdentifier](#) funzionamento dell'API Amazon Macie. Oppure, se utilizzi il AWS CLI, esegui il comando. [get-custom-data-identifier](#) Per il `id` parametro, specifica l'ID dell'identificatore di dati personalizzato. Dopo aver eliminato un identificatore di dati personalizzato, non puoi accedere alle sue impostazioni utilizzando la console Amazon Macie.

Definizione delle eccezioni relative ai dati sensibili con elenchi consentiti

Con gli elenchi di autorizzazioni in Amazon Macie, puoi definire testo e modelli di testo specifici che desideri che Macie ignori quando ispeziona gli oggetti Amazon Simple Storage Service (Amazon S3) alla ricerca di dati sensibili. Si tratta in genere di eccezioni relative ai dati sensibili per scenari o ambienti particolari. Se i dati corrispondono al testo o a uno schema di testo in un elenco consentito, Macie non riporta i dati. Questo è il caso anche se i dati corrispondono ai criteri di un identificatore di [dati gestito o di un identificatore](#) di [dati personalizzato](#). Utilizzando gli elenchi consentiti, puoi affinare l'analisi dei dati di Amazon S3 e ridurre il rumore.

Puoi creare e utilizzare due tipi di elenchi di autorizzazioni in Macie:

- **Testo predefinito:** per questo tipo di elenco, si specificano determinate sequenze di caratteri da ignorare. Ad esempio, è possibile specificare i nomi dei rappresentanti pubblici dell'organizzazione, numeri di telefono specifici o dati di esempio specifici che l'organizzazione utilizza per i test. Se utilizzate questo tipo di elenco, Macie ignora il testo che corrisponde esattamente a una voce dell'elenco.

Questo tipo di elenco consentito è utile se desideri specificare parole, frasi e altri tipi di sequenze di caratteri che non sono sensibili, che non sono suscettibili di modifiche e che non rispettano necessariamente uno schema comune.

- **Espressione regolare:** per questo tipo di elenco, si specifica un'espressione regolare (regex) che definisce uno schema di testo da ignorare. Ad esempio, è possibile specificare lo schema per i numeri di telefono pubblici dell'organizzazione, gli indirizzi e-mail per il dominio dell'organizzazione

o modelli di dati di esempio che l'organizzazione utilizza per i test. Se si utilizza questo tipo di elenco, Macie ignora il testo che corrisponde completamente allo schema definito dall'elenco.

Questo tipo di elenco consentito è utile se desideri specificare un testo che non è sensibile ma che varia o è suscettibile di modifiche, pur rispettando uno schema comune.

Dopo aver creato un elenco consentito, puoi [creare e configurare processi di rilevamento di dati sensibili](#) per utilizzarlo o [aggiungerlo alle impostazioni per l'individuazione automatica dei dati sensibili](#). Macie utilizza quindi l'elenco per analizzare i dati. Se Macie trova del testo che corrisponde a una voce o a uno schema in un elenco consentito, Macie non segnala la presenza di testo nelle rilevazioni di dati sensibili, nelle statistiche e in altri tipi di risultati.

Puoi gestire e utilizzare gli elenchi consentiti in tutte le aree in Regioni AWS cui Macie è attualmente disponibile, ad eccezione della regione Asia Pacifico (Osaka).

Argomenti

- [Opzioni di configurazione e requisiti per gli elenchi di autorizzazioni](#)
- [Creazione di un elenco di autorizzazioni](#)
- [Verifica dello stato di un elenco consentito](#)
- [Modifica di un elenco consentito](#)
- [Eliminazione di un elenco consentito](#)

Opzioni di configurazione e requisiti per gli elenchi di autorizzazioni

In Amazon Macie, puoi utilizzare gli elenchi di autorizzazione per specificare testo o modelli di testo che desideri che Macie ignori quando ispeziona gli oggetti Amazon Simple Storage Service (Amazon S3) alla ricerca di dati sensibili. Macie offre opzioni per due tipi di elenchi di autorizzazioni, testo predefinito ed espressioni regolari.

Un elenco di testo predefinito è utile se vuoi che Macie ignori parole, frasi e altri tipi di sequenze di caratteri specifiche che non consideri sensibili. Alcuni esempi sono: i nomi dei rappresentanti pubblici dell'organizzazione, numeri di telefono specifici o dati di esempio specifici che l'organizzazione utilizza per i test. Se Macie trova del testo che corrisponde ai criteri di un identificatore di dati gestito o personalizzato e il testo corrisponde anche a una voce in un elenco consentito, Macie non segnala la presenza di testo nelle rilevazioni di dati sensibili, nelle statistiche e in altri tipi di risultati.

Un'espressione regolare (regex) è utile se vuoi che Macie ignori il testo che varia o è suscettibile di modifiche, pur aderendo a uno schema comune. L'espressione regolare specifica uno schema di testo da ignorare. Alcuni esempi sono: numeri di telefono pubblici dell'organizzazione, indirizzi e-mail per il dominio dell'organizzazione o esempi di dati modellati che l'organizzazione utilizza per i test. Se Macie trova del testo che corrisponde ai criteri di un identificatore di dati gestito o personalizzato e il testo corrisponde anche a uno schema regex in un elenco consentito, Macie non segnala la presenza di testo nei risultati relativi a dati sensibili, nelle statistiche e in altri tipi di risultati.

Puoi creare e utilizzare entrambi i tipi di elenchi consentiti in tutti i paesi in Regioni AWS cui Macie è attualmente disponibile, ad eccezione della regione Asia Pacifico (Osaka). Durante la creazione e la gestione degli elenchi consentiti, tieni presenti le opzioni e i requisiti seguenti. Tieni inoltre presente che le voci degli elenchi e gli schemi regex per gli indirizzi postali non sono supportati.

Argomenti

- [Opzioni e requisiti per gli elenchi di testo predefinito](#)
 - [Requisiti di sintassi](#)
 - [Requisiti di storage](#)
 - [Requisiti di crittografia/decriptografia](#)
 - [Considerazioni e consigli sulla progettazione](#)
- [Opzioni e requisiti per le espressioni regolari](#)
 - [Supporto e consigli sulla sintassi](#)
 - [Esempi](#)

Opzioni e requisiti per gli elenchi di testo predefinito

Per questo tipo di elenco consentito, si fornisce un file di testo semplice delimitato da righe che elenca sequenze di caratteri specifiche da ignorare. Le voci dell'elenco sono in genere parole, frasi e altri tipi di sequenze di caratteri che non consideri sensibili, che non sono suscettibili di modifica e che non seguono necessariamente uno schema specifico. Se utilizzi questo tipo di elenco, Amazon Macie non segnala le occorrenze di testo che corrispondono esattamente a una voce dell'elenco. Macie tratta ogni voce dell'elenco come un valore letterale di stringa.

Per utilizzare questo tipo di elenco consentito, inizia creando l'elenco in un editor di testo e salvandolo come file di testo semplice. Quindi carica l'elenco in un bucket generico S3. Assicurati inoltre che le impostazioni di archiviazione e crittografia per il bucket e l'oggetto consentano a Macie di recuperare e decrittografare l'elenco. Quindi [crea e configura le impostazioni per](#) l'elenco in Macie.

Dopo aver configurato le impostazioni in Macie, ti consigliamo di testare l'elenco degli indirizzi consentiti con un piccolo set di dati rappresentativo per il tuo account o la tua organizzazione. Per testare un elenco, puoi [creare un lavoro occasionale](#). Configura il processo per utilizzare l'elenco oltre agli identificatori di dati gestiti e personalizzati che in genere utilizzi per analizzare i dati. È quindi possibile esaminare i risultati del lavoro: risultati relativi a dati sensibili, risultati della scoperta di dati sensibili o entrambi. Se i risultati del lavoro sono diversi da quelli previsti, puoi modificare e testare l'elenco fino a ottenere i risultati attesi.

Dopo aver completato la configurazione e il test di un elenco consentito, puoi creare e configurare processi aggiuntivi per utilizzarlo o aggiungerlo alle impostazioni per l'individuazione automatica dei dati sensibili. Quando questi processi iniziano a essere eseguiti o inizia il successivo ciclo di analisi del rilevamento automatico, Macie recupera l'ultima versione dell'elenco da Amazon S3 e la archivia nella memoria temporanea. Macie utilizza quindi questa copia temporanea dell'elenco per ispezionare gli oggetti S3 alla ricerca di dati sensibili. Al termine dell'esecuzione di un lavoro o al termine del ciclo di analisi, Macie elimina definitivamente la copia dell'elenco dalla memoria. L'elenco non persiste in Macie. Solo le impostazioni dell'elenco persistono in Macie.

Important

Poiché gli elenchi di testo predefinito non persistono in Macie, è importante [controllare periodicamente lo stato degli elenchi di](#) contenuti consentiti. Se Macie non riesce a recuperare o analizzare un elenco per il quale hai configurato un processo o un rilevamento automatico, Macie non utilizza l'elenco. Ciò potrebbe produrre risultati imprevisti, ad esempio il rilevamento di dati sensibili per il testo specificato nell'elenco.

Argomenti

- [Requisiti di sintassi](#)
- [Requisiti di storage](#)
- [Requisiti di crittografia/decriptografia](#)
- [Considerazioni e consigli sulla progettazione](#)

Requisiti di sintassi

Quando create questo tipo di elenco consentito, tenete presente i seguenti requisiti per il file dell'elenco:

- L'elenco deve essere archiviato come file di testo semplice (text/plain), ad esempio un file.txt, .text o .plain.
- L'elenco deve utilizzare interruzioni di riga per separare le singole voci. Per esempio:

```
Akua Mansa  
John Doe  
Martha Rivera  
425-555-0100  
425-555-0101  
425-555-0102
```

Macie tratta ogni riga come una voce singola e distinta nell'elenco. Il file può contenere anche righe vuote per migliorare la leggibilità. Macie salta le righe vuote quando analizza il file.

- Ogni voce può contenere 1—90 UTF—8 caratteri.
- Ogni voce deve corrispondere esattamente al testo da ignorare. Macie non supporta l'uso di caratteri jolly o valori parziali per le voci. Macie considera ogni voce come un valore letterale di stringa. Le corrispondenze non distinguono tra maiuscole e minuscole.
- Il file può contenere da 1 a 100.000 voci.
- La dimensione totale di archiviazione del file non può superare i 35 MB.

Requisiti di storage

Quando aggiungi e gestisci elenchi di dati consentiti in Amazon S3, tieni presente i seguenti requisiti di storage e consigli:

- Assistenza regionale: un elenco di utenti consentiti deve essere archiviato in un bucket che si trova nello stesso del tuo Regione AWS account Macie. Macie non può accedere a un elenco consentito se è memorizzato in una regione diversa.
- Proprietà dei bucket: un elenco consentito deve essere archiviato in un bucket di proprietà dell'utente. Account AWS Se desideri che altri account utilizzino lo stesso elenco di dati consentiti, prendi in considerazione la creazione di una regola di replica Amazon S3 per replicare l'elenco nei bucket di proprietà di tali account. Per informazioni sulla replica di oggetti S3, consulta [Replicating objects](#) nella Amazon Simple Storage Service User Guide.

Inoltre, la tua identità AWS Identity and Access Management (IAM) deve avere accesso in lettura al bucket e all'oggetto che memorizzano l'elenco. Altrimenti, non ti sarà consentito creare o aggiornare le impostazioni dell'elenco o controllarne lo stato utilizzando Macie.

- Tipi e classi di archiviazione: un elenco consentito deve essere archiviato in un bucket generico, non in un bucket di directory. Inoltre, deve essere archiviato utilizzando una delle seguenti classi di storage: Reduced Redundancy (RRS), S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Standard o S3 Standard-IA.
- Politiche bucket: se memorizzi un elenco consentito in un bucket con una politica restrittiva del bucket, assicurati che la politica consenta a Macie di recuperare l'elenco. A tale scopo, puoi aggiungere una condizione per il ruolo collegato al servizio Macie alla policy del bucket. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Assicurati inoltre che la policy consenta alla tua identità IAM di avere accesso in lettura al bucket. Altrimenti, non ti sarà permesso di creare o aggiornare le impostazioni dell'elenco o controllare lo stato dell'elenco utilizzando Macie.

- Percorsi degli oggetti: se memorizzi più di un elenco consentito in Amazon S3, il percorso dell'oggetto per ogni elenco deve essere univoco. In altre parole, ogni elenco consentito deve essere archiviato separatamente nel proprio oggetto S3.
- Controllo delle versioni: quando aggiungi un elenco consentito a un bucket, ti consigliamo di abilitare anche il controllo delle versioni per il bucket. È quindi possibile utilizzare valori di data e ora per correlare le versioni dell'elenco con i risultati dei processi di rilevamento di dati sensibili e dei cicli automatici di rilevamento dei dati sensibili che utilizzano l'elenco. Questo può aiutarti con i controlli o le indagini sulla privacy e la protezione dei dati che esegui.
- Object Lock: per evitare che un elenco consentito venga eliminato o sovrascritto per un determinato periodo di tempo o a tempo indeterminato, puoi abilitare Object Lock per il bucket che memorizza l'elenco. L'attivazione di questa impostazione non impedisce a Macie di accedere all'elenco. Per informazioni su questa impostazione, consulta [Locking objects with Object Lock](#) nella Amazon Simple Storage Service User Guide.

Requisiti di crittografia/decriptografia

Se si crittografa un elenco di elementi consentiti in Amazon S3, la politica di autorizzazione per [il ruolo collegato al servizio Macie in genere concede a Macie](#) le autorizzazioni necessarie per decriptografare l'elenco. Tuttavia, ciò dipende dal tipo di crittografia utilizzato:

- Se un elenco è crittografato utilizzando la crittografia lato server con una chiave gestita Amazon S3 (SSE-S3), Macie può decriptografare l'elenco. Il ruolo collegato al servizio per il tuo account Macie concede a Macie le autorizzazioni di cui ha bisogno.

- Se un elenco è crittografato utilizzando la crittografia lato server con un metodo AWS gestito AWS KMS key (DSSE-KMS o SSE-KMS), Macie può decrittografare l'elenco. Il ruolo collegato al servizio per il tuo account Macie concede a Macie le autorizzazioni di cui ha bisogno.
- Se un elenco è crittografato utilizzando la crittografia lato server con una crittografia gestita dal cliente AWS KMS key (DSSE-KMS o SSE-KMS), Macie può decrittografare l'elenco solo se consenti a Macie di utilizzare la chiave. Per informazioni su come effettuare questa operazione, consulta [Consentire a Macie di utilizzare un servizio gestito dal cliente AWS KMS key](#).

Note

È possibile crittografare un elenco con un cliente gestito in un archivio di chiavi esterno. AWS KMS key Tuttavia, la chiave potrebbe quindi essere più lenta e meno affidabile di una chiave gestita interamente all'interno. AWS KMS Se la latenza o un problema di disponibilità impediscono a Macie di decifrare l'elenco, Macie non utilizza l'elenco quando analizza gli oggetti S3. Ciò potrebbe produrre risultati imprevisti, come il rilevamento di dati sensibili per il testo specificato nell'elenco. Per ridurre questo rischio, prendi in considerazione la possibilità di archiviare l'elenco in un bucket S3 configurato per utilizzare la chiave come chiave S3 Bucket.

Per informazioni sull'utilizzo delle chiavi KMS negli archivi di chiavi esterni, consulta Archivi di [chiavi esterni](#) nella Guida per gli sviluppatori. AWS Key Management Service Per informazioni sull'uso di S3 Bucket Keys, consulta [Ridurre il costo di SSE-KMS con Amazon S3 Bucket Keys nella Guida per l'utente di Amazon](#) Simple Storage Service.

- Se un elenco è crittografato utilizzando la crittografia lato server con una chiave fornita dal cliente (SSE-C) o la crittografia lato client, Macie non può decrittografare l'elenco. Prendi in considerazione invece l'utilizzo della crittografia SSE-S3, DSSE-KMS o SSE-KMS.

Se un elenco è crittografato con una chiave KMS AWS gestita o una chiave KMS gestita dal cliente, anche la tua identità AWS Identity and Access Management (IAM) deve poter utilizzare la chiave. Altrimenti, non ti sarà consentito creare o aggiornare le impostazioni dell'elenco o controllarne lo stato utilizzando Macie. Per sapere come controllare o modificare le autorizzazioni per una chiave KMS, consulta [le politiche chiave AWS KMS nella Guida](#) per gli AWS Key Management Service sviluppatori.

Per informazioni dettagliate sulle opzioni di crittografia per i dati di Amazon S3, consulta [Protecting data with encryption](#) nella Amazon Simple Storage Service User Guide.

Considerazioni e consigli sulla progettazione

In generale, Macie considera ogni voce in un elenco consentito come un valore letterale di stringa. Vale a dire, Macie ignora ogni occorrenza di testo che corrisponde esattamente a una voce completa in un elenco consentito. Le corrispondenze non distinguono tra maiuscole e minuscole.

Tuttavia, Macie utilizza le voci come parte di un più ampio framework di estrazione e analisi dei dati. Il framework include funzioni di machine learning e pattern matching che tengono conto di dimensioni come le variazioni grammaticali e sintattiche e, in molti casi, la prossimità delle parole chiave. Il framework tiene conto anche del tipo di file o del formato di archiviazione di un oggetto S3. Pertanto, tenete a mente le seguenti considerazioni e raccomandazioni quando aggiungete e gestite le voci in un elenco consentito.

Preparati per diversi tipi di file e formati di archiviazione

Per i dati non strutturati, come il testo in un file Adobe Portable Document Format (.pdf), Macie ignora il testo che corrisponde esattamente a una voce completa in un elenco consentito, incluso il testo che si estende su più righe o pagine.

Per i dati strutturati, come i dati colonnari in un file CSV o i dati basati su record in un file JSON, Macie ignora il testo che corrisponde esattamente a una voce completa in un elenco consentito se tutto il testo è memorizzato in un singolo campo, cella o matrice. Questo requisito non si applica ai dati strutturati archiviati in un file altrimenti non strutturato, come una tabella in un file.pdf.

Ad esempio, considera il seguente contenuto in un file CSV:

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

Se Akua Mansa e John Doe sono voci in un elenco consentito, Macie ignora tali nomi nel file CSV. Il testo completo di ogni voce dell'elenco viene memorizzato in un unico campo. Name

Al contrario, considera un file CSV che contenga le colonne e i campi seguenti:

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```


Se Akua Mansa e John Doe sono voci in un elenco consentito, Macie non ignora quei nomi nel file CSV. Nessuno dei campi del file CSV contiene il testo completo di una voce nell'elenco delle voci consentite.

Includi varianti comuni

Aggiungi voci per variazioni comuni di dati numerici, nomi propri, termini e sequenze di caratteri alfanumerici. Ad esempio, se aggiungi nomi o frasi che contengono solo uno spazio tra le parole, aggiungi anche varianti che includono due spazi tra le parole. Allo stesso modo, aggiungi parole e frasi che contengono e non contengono caratteri speciali e valuta la possibilità di includere variazioni sintattiche e semantiche comuni.

Per il numero di telefono statunitense 425-555-0100, ad esempio, puoi aggiungere queste voci a un elenco consentito:

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

Per la data del 1° febbraio 2022 in un contesto multinazionale, potresti aggiungere voci che includono variazioni sintattiche comuni per l'inglese e il francese, comprese le varianti che includono e non includono caratteri speciali:

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

Per i nomi delle persone, includi le voci relative a varie forme di nome che non consideri sensibili. Ad esempio, includi: il nome seguito dal cognome, il cognome seguito dal nome, il nome e il cognome separati da uno spazio, il nome e il cognome separati da due spazi e i soprannomi.

Per il nome Martha Rivera, ad esempio, potresti aggiungere:

```
Martha Rivera
```

```
Martha Rivera  
Rivera, Martha  
Rivera, Martha  
Rivera Martha  
Rivera Martha
```

Se desideri ignorare le varianti di un nome specifico che contiene molte parti, crea invece un elenco di elementi consentiti che utilizzi un'espressione regolare. Ad esempio, per il nome Dr. Martha Lyda Rivera, PhD, potresti usare la seguente espressione regolare: `^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`

Opzioni e requisiti per le espressioni regolari

Per questo tipo di elenco consentito, si specifica un'espressione regolare (regex) che definisce uno schema di testo da ignorare. Ad esempio, è possibile specificare lo schema per i numeri di telefono pubblici dell'organizzazione, gli indirizzi e-mail per il dominio dell'organizzazione o modelli di dati di esempio che l'organizzazione utilizza per i test. L'espressione regolare definisce uno schema comune per un tipo specifico di dati che non consideri sensibili. Se utilizzi questo tipo di elenco consentito, Amazon Macie non segnala le occorrenze di testo che corrispondono completamente allo schema specificato. A differenza di un elenco consentito che specifica il testo predefinito da ignorare, l'espressione regolare e tutte le altre impostazioni dell'elenco vengono create e archiviate in Macie.

Quando crei o aggiorni questo tipo di elenco consentito, puoi testare l'espressione regolare dell'elenco con dati di esempio prima di salvare l'elenco. Ti consigliamo di eseguire questa operazione con più set di dati di esempio. Se crei un'espressione regolare troppo generica, Macie potrebbe ignorare le occorrenze di testo che consideri riservate. Se un'espressione regolare è troppo specifica, Macie potrebbe non ignorare le occorrenze di testo che non consideri sensibili. Per proteggerti da espressioni non corrette o di lunga durata, Macie inoltre compila e testa automaticamente l'espressione regolare rispetto a una raccolta di testo di esempio e ti avvisa dei problemi da risolvere.

Per ulteriori test, ti consigliamo di testare anche l'espressione regolare dell'elenco con un piccolo set di dati rappresentativo per il tuo account o la tua organizzazione. A tale scopo, puoi [creare un lavoro occasionale](#). Configura il processo per utilizzare l'elenco oltre agli identificatori di dati gestiti e personalizzati che in genere utilizzi per analizzare i dati. È quindi possibile esaminare i risultati del lavoro: risultati relativi a dati sensibili, risultati della scoperta di dati sensibili o entrambi. Se i risultati del lavoro sono diversi da quelli previsti, puoi modificare e testare l'espressione regolare fino a ottenere i risultati attesi.

Dopo aver configurato e testato un elenco consentito, puoi creare e configurare processi aggiuntivi per utilizzarlo o aggiungerlo alle impostazioni per l'individuazione automatica dei dati sensibili. Quando questi processi vengono eseguiti o Macie esegue il rilevamento automatico, Macie utilizza l'ultima versione dell'espressione regolare dell'elenco per analizzare i dati.

Argomenti

- [Supporto e consigli sulla sintassi](#)
- [Esempi](#)

Supporto e consigli sulla sintassi

Un elenco consentito può specificare un'espressione regolare (regex) che contiene fino a 512 caratteri. Macie supporta un sottoinsieme della sintassi del pattern regex fornita dalla libreria [Perl Compatible Regular Expressions \(PCRE\)](#). Tra i costrutti forniti dalla libreria PCRE, Macie non supporta i seguenti elementi del pattern:

- Riferimenti all'indietro
- Acquisizione di gruppi
- Modelli condizionali
- Codice incorporato
- Bandiere con pattern globali, ad esempio `/i/m`, e `/x`
- Schemi ricorsivi
- Asserzioni a larghezza zero positive e negative e look-ahead, ad esempio, `?`, `?! ?<= ?<!`

Per creare modelli di espressioni regolari efficaci per gli elenchi di espressioni consentite, tenete presente i seguenti suggerimenti e raccomandazioni:

- Ancoraggi: utilizzate gli anchors (`^` o `$`) solo se vi aspettate che il pattern appaia all'inizio o alla fine di un file, non all'inizio o alla fine di una riga.
- Ripetizioni limitate: per motivi di prestazioni, Macie limita la dimensione dei gruppi di ripetizioni limitati. Ad esempio, `\d{100,1000}` non verrà compilato in Macie. Per approssimare questa funzionalità, puoi usare una ripetizione aperta come `\d{100,}`
- Indistinzione tra maiuscole e minuscole: per rendere insensibili le lettere maiuscole e minuscole alle parti di un pattern, puoi usare il `(?i)` costrutto anziché il flag `/i`

- **Prestazioni:** non è necessario ottimizzare manualmente i prefissi o le alternanze. Ad esempio, passare `/hello|hi|hey/` a non `/h(?:ello|i|ey)/` migliorerà le prestazioni.
- **Wild card:** per motivi di prestazioni, Macie limita il numero di jolly ripetuti. Ad esempio, `a*b*a*` non verrà compilato in Macie.
- **Alternazione:** per specificare più di un modello in un unico elenco consentito, puoi utilizzare l'operatore di alternazione (`|`) per concatenare i modelli. Se lo fai, Macie usa la logica OR per combinare i pattern e formare un nuovo pattern. Ad esempio, se lo specifichi (`apple|orange`), Macie riconosce sia la mela che l'arancia come corrispondenze e ignora le occorrenze di entrambe le parole. Se concatenate dei pattern, assicuratevi di limitare la lunghezza totale dell'espressione concatenata a 512 caratteri o meno.

Infine, quando sviluppate l'espressione regolare, progettate per adattarsi a diversi tipi di file e formati di archiviazione. Macie utilizza l'espressione regolare come parte di un più ampio framework di estrazione e analisi dei dati. Il framework tiene conto del tipo di file o del formato di archiviazione di un oggetto S3. Per i dati strutturati, come i dati colonnari in un file CSV o i dati basati su record in un file JSON, Macie ignora il testo che corrisponde completamente al modello solo se tutto il testo è memorizzato in un singolo campo, cella o matrice. Questo requisito non si applica ai dati strutturati archiviati in un file altrimenti non strutturato, come una tabella in un file Adobe Portable Document Format (.pdf). Per i dati non strutturati, come il testo in un file.pdf, Macie ignora il testo che corrisponde completamente allo schema, incluso il testo che si estende su più righe o pagine.

Esempi

Gli esempi seguenti mostrano modelli regex validi per alcuni scenari comuni.

Indirizzi e-mail

Se utilizzi un identificatore di dati personalizzato per rilevare gli indirizzi e-mail, puoi ignorare gli indirizzi e-mail che non consideri sensibili, come gli indirizzi e-mail della tua organizzazione.

Per ignorare gli indirizzi e-mail di un particolare dominio di secondo e primo livello, puoi utilizzare questo schema:

```
[a-zA-Z0-9_+\\-]+@example\\.com
```

example Dov'è il nome del dominio di secondo livello ed *com* è il dominio di primo livello. In questo caso, Macie abbina e ignora indirizzi come `johndoe@example.com` e `john.doe@example.com`.

Per ignorare gli indirizzi e-mail di un determinato dominio in qualsiasi dominio generico di primo livello (gTLD), ad esempio.com o .gov, puoi utilizzare questo schema:

```
[a-zA-Z0-9_.\-]+\@example\[a-zA-Z]{2,}
```

example Dov'è il nome del dominio. In questo caso, Macie corrisponde e ignora indirizzi come johndoe@example.com, john.doe@example.gov e johndoe@example.edu.

Per ignorare gli indirizzi e-mail di un determinato dominio in qualsiasi dominio di primo livello nazionale (ccTLD), ad esempio.ca per il Canada o .au per l'Australia, puoi utilizzare questo schema:

```
[a-zA-Z0-9_.\-]+\@example\.(ca|au)
```

example Dov'è il nome del dominio *ca* e i cc specifici da *au* ignorare. TLDs In questo caso, Macie abbina e ignora indirizzi come johndoe@example.ca e john.doe@example.au.

Per ignorare gli indirizzi e-mail relativi a un determinato dominio e gTLD e includere domini di terzo e quarto livello, puoi utilizzare questo schema:

```
[a-zA-Z0-9_.\-]+\@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\@example.com
```

example Dov'è il nome del dominio ed *com* è il gTLD. In questo caso, Macie abbina e ignora indirizzi come johndoe@www.example.com e john.doe@www.team.example.com.

Numeri di telefono

Macie fornisce identificatori di dati gestiti in grado di rilevare i numeri di telefono di diversi paesi e aree geografiche. Per ignorare determinati numeri di telefono, come i numeri verdi o i numeri di telefono pubblici dell'organizzazione, puoi utilizzare schemi come i seguenti.

Per ignorare i numeri di telefono statunitensi gratuiti che utilizzano il prefisso 800 e sono formattati come (800) ###-####:

```
^\(800\)?[ -]?\d{3}[ -]?\d{4}$
```

Per ignorare i numeri verdi statunitensi che utilizzano il prefisso 888 e sono formattati come (888) ###-####:

```
^\(888\)?[ -]?\d{3}[ -]?\d{4}$
```

Per ignorare i numeri di telefono francesi a 10 cifre che includono il prefisso internazionale 33 e sono formattati come +33 ## ## ## ##:

```
^\+33 \d( \d\d){4}$
```

Per ignorare i numeri di telefono statunitensi e canadesi che utilizzano codici di area e di scambio particolari, non includono un prefisso internazionale e sono formattati come (###) ###-####:

```
^\((?123\)?[ -]?555[ -]?\d{4}$
```

Dov'è il prefisso **123** e il codice di scambio. **555**

Per ignorare i numeri di telefono statunitensi e canadesi che utilizzano codici di area e di scambio particolari, includono un prefisso internazionale e sono formattati come +1 (###) ###-####:

```
^\+1\((?123\)?[ -]?555[ -]?\d{4}$
```

Dov'è il prefisso **123** e il codice di scambio. **555**

Creazione di un elenco di autorizzazioni

In Amazon Macie, un elenco di elementi consentiti definisce un testo specifico o un pattern di testo che vuoi che Macie ignori quando ispeziona gli oggetti Amazon Simple Storage Service (Amazon S3) alla ricerca di dati sensibili. Se il testo corrisponde a una voce o a uno schema in un elenco consentito, Macie non riporta il testo nelle rilevazioni di dati sensibili, nelle statistiche o in altri tipi di risultati. Questo vale anche se il testo corrisponde ai criteri di un identificatore di [dati gestito o di un identificatore](#) di [dati personalizzato](#).

È possibile creare i seguenti tipi di elenchi consentiti in Macie.

Testo predefinito

Utilizzate questo tipo di elenco per specificare parole, frasi e altri tipi di sequenze di caratteri che non sono sensibili, non sono suscettibili di modifiche e non necessariamente aderiscono a uno schema comune. Alcuni esempi sono: i nomi dei rappresentanti pubblici dell'organizzazione, numeri di telefono specifici e dati di esempio specifici utilizzati dall'organizzazione per i test. Se usi questo tipo di elenco, Macie ignora il testo che corrisponde esattamente a una voce dell'elenco.

Per questo tipo di elenco, si crea un file di testo semplice delimitato da righe che elenca il testo specifico da ignorare. Quindi memorizzi il file in un bucket S3 e configuri le impostazioni per consentire a Macie di accedere all'elenco nel bucket. È quindi possibile creare e configurare processi di rilevamento di dati sensibili per utilizzare l'elenco o aggiungere l'elenco alle impostazioni per l'individuazione automatica dei dati sensibili. Quando ogni processo inizia a

essere eseguito o inizia il successivo ciclo di analisi del rilevamento automatico, Macie recupera l'ultima versione dell'elenco da Amazon S3. Macie utilizza quindi quella versione dell'elenco quando ispeziona gli oggetti S3 alla ricerca di dati sensibili. Se Macie trova del testo che corrisponde esattamente a una voce dell'elenco, Macie non segnala tale presenza di testo come dati sensibili.

Espressione regolare

Usa questo tipo di elenco per specificare un'espressione regolare (regex) che definisce uno schema di testo da ignorare. Alcuni esempi sono: numeri di telefono pubblici dell'organizzazione, indirizzi e-mail per il dominio dell'organizzazione e esempi di dati modellati utilizzati dall'organizzazione per i test. Se utilizzi questo tipo di elenco, Macie ignora il testo che corrisponde completamente allo schema regex definito dall'elenco.

Per questo tipo di elenco, si crea un'espressione regolare che definisce uno schema comune per il testo che non è sensibile ma varia o è suscettibile di modifiche. A differenza di un elenco di testo predefinito, l'espressione regolare e tutte le altre impostazioni dell'elenco vengono create e memorizzate in Macie. È quindi possibile creare e configurare processi di rilevamento di dati sensibili per utilizzare l'elenco o aggiungere l'elenco alle impostazioni per l'individuazione automatica dei dati sensibili. Quando questi processi vengono eseguiti o Macie esegue il rilevamento automatico, Macie utilizza l'ultima versione dell'espressione regolare dell'elenco per analizzare i dati. Se Macie trova del testo che corrisponde completamente allo schema definito dall'elenco, Macie non segnala la presenza di testo come dati sensibili.

Per requisiti dettagliati, consigli ed esempi di ogni tipo, vedi. [Opzioni di configurazione e requisiti per gli elenchi di autorizzazioni](#)

È possibile creare fino a 10 elenchi di autorizzazioni per ogni elenco supportato Regione AWS: fino a cinque elenchi di autorizzazioni che specificano testo predefinito e fino a cinque elenchi di autorizzazioni che specificano espressioni regolari. Puoi creare e utilizzare gli elenchi consentiti in tutte le aree in Regioni AWS cui Macie è attualmente disponibile, ad eccezione della regione Asia Pacifico (Osaka).

Per creare un elenco di prodotti consentiti

Il modo in cui si crea un elenco consentito dipende dal tipo di elenco che si desidera creare: un file che elenca il testo predefinito da ignorare o un'espressione regolare che definisce uno schema di testo da ignorare. Le seguenti sezioni forniscono istruzioni per ogni tipo. Scegli la sezione per il tipo di elenco che desideri creare.

Testo predefinito

Prima di creare questo tipo di elenco di autorizzazioni in Macie, procedi come segue:

1. Utilizzando un editor di testo, create un file di testo semplice delimitato da righe che elenchi il testo specifico da ignorare, ad esempio un file.txt, .text o.plain. Per ulteriori informazioni, consulta [Requisiti di sintassi](#).
2. Carica il file in un bucket S3 generico e annota il nome del bucket e dell'oggetto. Dovrai inserire questi nomi quando configuri le impostazioni in Macie.
3. Assicurati che le impostazioni per il bucket e l'oggetto S3 consentano a te e Macie di recuperare l'elenco dal bucket. Per ulteriori informazioni, consulta [Requisiti di storage](#).
4. Se hai crittografato l'oggetto S3, assicurati che sia crittografato con una chiave che tu e Macie possiate usare. Per ulteriori informazioni, consulta [Requisiti di crittografia/decriptografia](#).

Dopo aver completato queste attività, sei pronto per configurare le impostazioni dell'elenco in Macie. Puoi configurare le impostazioni utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per configurare le impostazioni per un elenco di prodotti consentiti utilizzando la console Amazon Macie.

Per configurare le impostazioni degli elenchi consentiti in Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Consenti elenchi.
3. Nella pagina Consenti elenchi, scegli Crea.
4. In Seleziona un tipo di elenco, scegli Testo predefinito.
5. In Impostazioni elenco, utilizzate le seguenti opzioni per inserire impostazioni aggiuntive per l'elenco consentito:
 - Per Nome, inserisci un nome per l'elenco. Il nome può contenere fino a un massimo di 128 caratteri.
 - Per Descrizione, inserisci facoltativamente una breve descrizione dell'elenco. La descrizione può contenere fino a 512 caratteri.
 - Per il nome del bucket S3, inserisci il nome del bucket che memorizza l'elenco.

In Amazon S3, puoi trovare questo valore nel campo Nome delle proprietà del bucket. Questo valore prevede la distinzione tra lettere maiuscole e minuscole. Inoltre, non utilizzare caratteri jolly o valori parziali quando inserisci il nome.

- Per il nome dell'oggetto S3, inserisci il nome dell'oggetto S3 che memorizza l'elenco.

In Amazon S3, puoi trovare questo valore nel campo Chiave delle proprietà dell'oggetto. Se il nome include un percorso, assicurati di includere il percorso completo quando inserisci il nome, ad esempio **allowlists/macie/mylist.txt**. Questo valore prevede la distinzione tra lettere maiuscole e minuscole. Inoltre, non utilizzate caratteri jolly o valori parziali quando inserite il nome.

6. (Facoltativo) In Tag, scegli Aggiungi tag, quindi inserisci fino a 50 tag da assegnare all'elenco dei tag consentiti.

Un tag è un'etichetta che definisci e assegni a determinati tipi di AWS risorse. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

7. Al termine, scegli Save (Salva).

Macie verifica le impostazioni dell'elenco. Macie verifica inoltre di poter recuperare l'elenco da Amazon S3 e analizzarne il contenuto. Se si verifica un errore, Macie visualizza un messaggio che descrive l'errore. Per informazioni dettagliate che possono aiutarti a risolvere l'errore, consulta [Opzioni e requisiti per gli elenchi di testo predefinito](#). Dopo aver corretto gli errori, puoi salvare le impostazioni dell'elenco.

API

Per configurare le impostazioni degli elenchi di autorizzazioni a livello di codice, utilizza il [CreateAllowList](#) funzionamento dell'API Amazon Macie e specifica i valori appropriati per i parametri richiesti.

Per il `criteria` parametro, usa un `s3WordsList` oggetto per specificare il nome del bucket S3 (`bucketName`) e il nome dell'oggetto S3 (`objectKey`) che memorizza l'elenco. Per determinare il nome del bucket, consulta il Name campo in Amazon S3. Per determinare il nome dell'oggetto, consulta il Key campo in Amazon S3. Tieni presente che questi valori fanno distinzione tra

maiuscole e minuscole. Inoltre, non utilizzate caratteri jolly o valori parziali quando specificate questi nomi.

Per configurare le impostazioni utilizzando il AWS CLI, esegui il [create-allow-list](#) comando e specifica i valori appropriati per i parametri richiesti. Gli esempi seguenti mostrano come configurare le impostazioni per un elenco di dati consentiti archiviato in un bucket S3 denominato. *amzn-s3-demo-bucket* Il nome dell'oggetto S3 che memorizza l'elenco è. *allowlists/macie/mylist.txt*

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"amzn-s3-demo-bucket","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 create-allow-list ^
--criteria={"s3WordsList":{"bucketName\":\"amzn-s3-demo-bucket\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

Quando invii la richiesta, Macie verifica le impostazioni dell'elenco. Macie verifica inoltre di poter recuperare l'elenco da Amazon S3 e analizzarne il contenuto. Se si verifica un errore, la richiesta non va a buon fine e Macie restituisce un messaggio che descrive l'errore. Per informazioni dettagliate che possono aiutarti a risolvere l'errore, consulta. [Opzioni e requisiti per gli elenchi di testo predefinito](#)

Se Macie riesce a recuperare e analizzare l'elenco, la tua richiesta ha esito positivo e riceverai un risultato simile al seguente.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
  "id": "nkr81bmtu2542yyexample"
```

```
}
```

arnDov'è l'Amazon Resource Name (ARN) dell'elenco consentito che è stato creato ed id è l'identificatore univoco dell'elenco.

Dopo aver salvato le impostazioni dell'elenco, puoi [creare e configurare processi di rilevamento di dati sensibili](#) per utilizzare l'elenco o [aggiungere l'elenco alle impostazioni per il rilevamento automatico dei dati sensibili](#). Ogni volta che questi processi iniziano a essere eseguiti o inizia un ciclo di analisi del rilevamento automatico, Macie recupera l'ultima versione dell'elenco da Amazon S3. Macie utilizza quindi quella versione dell'elenco per analizzare i dati.

Espressione regolare

Quando crei un elenco consentito che specifica un'espressione regolare (regex), definisci l'espressione regolare e tutte le altre impostazioni dell'elenco direttamente in Macie. Per quanto riguarda l'espressione regolare, Macie supporta un sottoinsieme della sintassi del pattern fornita dalla libreria [Perl Compatible Regular Expressions \(PCRE\)](#). Per ulteriori informazioni, consulta [Supporto e consigli sulla sintassi](#).

Puoi creare questo tipo di elenco utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per creare un elenco di autorizzazioni utilizzando la console Amazon Macie.

Per creare un elenco di elementi consentiti utilizzando la console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Consenti elenchi.
3. Nella pagina Consenti elenchi, scegli Crea.
4. In Seleziona un tipo di elenco, scegli Espressione regolare.
5. In Impostazioni elenco, utilizzate le seguenti opzioni per inserire impostazioni aggiuntive per l'elenco consentito:
 - Per Nome, inserisci un nome per l'elenco. Il nome può contenere fino a un massimo di 128 caratteri.
 - Per Descrizione, inserisci facoltativamente una breve descrizione dell'elenco. La descrizione può contenere fino a 512 caratteri.

- Per Espressione regolare, inserite l'espressione regolare che definisce lo schema di testo da ignorare. L'espressione regolare può contenere fino a 512 caratteri.
6. (Facoltativo) Per Evaluate, inserite fino a 1.000 caratteri nella casella Dati di esempio, quindi scegliete Test per testare l'espressione regolare. Macie valuta i dati di esempio e riporta il numero di occorrenze di testo che corrispondono all'espressione regolare. Puoi ripetere questo passaggio tutte le volte che vuoi per rifinire e ottimizzare l'espressione regolare.

 Note

Ti consigliamo di testare e perfezionare l'espressione regolare con più set di dati di esempio. Se crei un'espressione regolare troppo generica, Macie potrebbe ignorare le occorrenze di testo che consideri riservate. Se un'espressione regolare è troppo specifica, Macie potrebbe non ignorare le occorrenze di testo che non consideri sensibili.

7. (Facoltativo) In Tag, scegli Aggiungi tag, quindi inserisci fino a 50 tag da assegnare all'elenco dei tag consentiti.

Un tag è un'etichetta che definisci e assegni a determinati tipi di AWS risorse. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

8. Al termine, scegli Save (Salva).

Macie verifica le impostazioni dell'elenco. Macie verifica anche l'espressione regolare per verificare che sia in grado di compilare l'espressione. Se si verifica un errore, Macie visualizza un messaggio che descrive l'errore. Per informazioni dettagliate che possono aiutarti a risolvere l'errore, consulta [Opzioni e requisiti per le espressioni regolari](#). Dopo aver corretto gli errori, puoi salvare l'elenco degli errori consentiti.

API

Prima di creare questo tipo di elenco di dati consentiti in Macie, ti consigliamo di testare e perfezionare l'espressione regolare con più set di dati di esempio. Se crei un'espressione regolare troppo generica, Macie potrebbe ignorare le occorrenze di testo che consideri sensibili. Se un'espressione regolare è troppo specifica, Macie potrebbe non ignorare le occorrenze di testo che non consideri sensibili.

Per testare un'espressione con Macie, puoi utilizzare il [TestCustomDataIdentifier](#) funzionamento dell'API Amazon Macie o, in alternativa, eseguire AWS CLI [test-custom-data-identifier](#) comando. Macie utilizza lo stesso codice sottostante per compilare espressioni per elenchi di autorizzazioni e identificatori di dati personalizzati. Se testate un'espressione in questo modo, assicuratevi di specificare i valori solo per i `regex` parametri `and.sampleText`. In caso contrario, riceverai risultati imprecisi.

Quando sei pronto per creare questo tipo di elenco di autorizzazioni, utilizza il [CreateAllowList](#) funzionamento dell'API Amazon Macie e specifica i valori appropriati per i parametri richiesti. Per il `criteria` parametro, usa il `regex` campo per specificare l'espressione regolare che definisce lo schema di testo da ignorare. L'espressione può contenere fino a un massimo di 512 caratteri.

Per creare questo tipo di elenco utilizzando AWS CLI, esegui il [create-allow-list](#) comando e specifica i valori appropriati per i parametri richiesti. Negli esempi seguenti viene creato un elenco di elementi consentiti denominato `my_allow_list`. L'espressione regolare è progettata per ignorare tutti gli indirizzi e-mail che un identificatore di dati personalizzato potrebbe altrimenti rilevare per il `example.com` dominio.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 create-allow-list \
--criteria '{"regex":"[a-z]@example.com"}' \
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws macie2 create-allow-list ^
--criteria={"regex\"":["a-z]@example.com\""} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

Quando invii la richiesta, Macie verifica le impostazioni dell'elenco. Macie verifica anche l'espressione regolare per verificare che sia in grado di compilare l'espressione. Se si verifica un errore, la richiesta fallisce e Macie restituisce un messaggio che descrive l'errore. Per informazioni

dettagliate che possono aiutarti a risolvere l'errore, consulta. [Opzioni e requisiti per le espressioni regolari](#)

Se Macie è in grado di compilare l'espressione, la richiesta ha esito positivo e si riceve un output simile al seguente:

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
  "id": "km2d4y22hp6rv05example"
}
```

`arnDov` è l'Amazon Resource Name (ARN) dell'elenco consentito che è stato creato ed `id` è l'identificatore univoco dell'elenco.

Dopo aver salvato l'elenco, puoi [creare e configurare processi di rilevamento di dati sensibili](#) per utilizzarlo o [aggiungerlo alle tue impostazioni per il rilevamento automatico dei dati sensibili](#). Quando questi processi vengono eseguiti o Macie esegue il rilevamento automatico, Macie utilizza l'ultima versione dell'espressione regolare dell'elenco per analizzare i dati.

Verifica dello stato di un elenco consentito

Se crei un elenco consentito, è importante controllarne periodicamente lo stato. In caso contrario, gli errori potrebbero far sì che Amazon Macie produca risultati di analisi imprevisti per i dati di Amazon Simple Storage Service (Amazon S3). Ad esempio, Macie potrebbe creare rilevamenti di dati sensibili per il testo specificato in un elenco di dati consentiti.

Se configuri un processo di rilevamento di dati sensibili per utilizzare un elenco di dati consentiti e Macie non può accedere o utilizzare l'elenco quando il lavoro inizia a essere eseguito, il lavoro continua a funzionare. Tuttavia, Macie non utilizza l'elenco quando analizza gli oggetti S3. Allo stesso modo, se inizia un ciclo di analisi per l'individuazione automatica di dati sensibili e Macie non riesce ad accedere o utilizzare un elenco consentito specificato, l'analisi continua ma Macie non utilizza l'elenco.

È improbabile che si verifichino errori per un elenco consentito che specifica un'espressione regolare (regex). Ciò è dovuto in parte al fatto che Macie verifica automaticamente l'espressione regolare quando crei o aggiorni le impostazioni dell'elenco. Inoltre, memorizzi l'espressione regolare e tutte le altre impostazioni dell'elenco in Macie.

Tuttavia, possono verificarsi errori per un elenco di elementi consentiti che specifica un testo predefinito, in parte perché l'elenco viene archiviato in Amazon S3 anziché in Macie. Le cause più comuni di errore sono:

- Il bucket o l'oggetto S3 viene eliminato.
- Il bucket o l'oggetto S3 viene rinominato e le impostazioni dell'elenco in Macie non specificano il nuovo nome.
- Le impostazioni delle autorizzazioni del bucket S3 vengono modificate e Macie perde l'accesso al bucket e all'oggetto.
- Le impostazioni di crittografia per il bucket S3 vengono modificate e Macie non può decrittografare l'oggetto che memorizza l'elenco.
- La politica per la chiave di crittografia viene modificata e Macie perde l'accesso alla chiave. Macie non può decifrare l'oggetto S3 che memorizza l'elenco.

Important

Poiché questi errori influiscono sui risultati delle analisi, ti consigliamo di controllare periodicamente lo stato di tutte le tue liste consentite. Ti consigliamo di farlo anche se modifichi le autorizzazioni o le impostazioni di crittografia per un bucket S3 che memorizza un elenco consentito o modifichi la politica per una chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare un elenco.

Per informazioni dettagliate che possono aiutarti a risolvere gli errori che si verificano, consulta.

[Opzioni e requisiti per gli elenchi di testo predefinito](#)

Per verificare lo stato di un elenco consentito

Puoi controllare lo stato di un elenco di prodotti consentiti utilizzando la console Amazon Macie o l'API Amazon Macie. Sulla console, puoi utilizzare un'unica pagina per controllare lo stato di tutti gli elenchi di utenti consentiti contemporaneamente. Se utilizzi l'API Amazon Macie, puoi controllare lo stato dei singoli elenchi di autorizzazioni, uno alla volta.

Console

Segui questi passaggi per verificare lo stato delle tue liste consentite utilizzando la console Amazon Macie.

Per verificare lo stato delle tue liste consentite

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Consenti elenchi.
3. Nella pagina Consenti elenchi, scegli refresh



).

Macie verifica le impostazioni di tutti gli elenchi consentiti e aggiorna il campo Stato per indicare lo stato corrente di ogni elenco.

Se un elenco specifica un'espressione regolare, il suo stato è in genere OK. Ciò significa che Macie può compilare l'espressione. Se un elenco specifica un testo predefinito, il suo stato può essere uno dei seguenti valori.

OK

Macie può recuperare e analizzare il contenuto dell'elenco.

Accesso negato

A Macie non è consentito accedere all'oggetto S3 che memorizza l'elenco. Amazon S3 ha negato la richiesta di recupero dell'oggetto. Un elenco può avere questo stato anche se l'oggetto è crittografato con un client gestito AWS KMS key che Macie non può utilizzare.

Per risolvere questo errore, esamina la policy del bucket e le altre impostazioni di autorizzazione per il bucket e l'oggetto. Assicurati che Macie sia autorizzato ad accedere e recuperare l'oggetto. Se l'oggetto è crittografato con una AWS KMS chiave gestita dal cliente, rivedi anche la politica sulla chiave e assicurati che Macie sia autorizzato a usare la chiave.

Errore

Si è verificato un errore temporaneo o interno quando Macie ha tentato di recuperare o analizzare il contenuto dell'elenco. Un elenco consentito può avere questo stato anche se è crittografato con una chiave di crittografia a cui Amazon S3 e Macie non possono accedere o utilizzare.

Per risolvere questo errore, attendi qualche minuto e poi scegli nuovamente refresh



Se lo stato continua a essere Errore, controlla le impostazioni di crittografia per l'oggetto

S3. Assicurati che l'oggetto sia crittografato con una chiave accessibile e utilizzabile da Amazon S3 e Macie.

L'oggetto è vuoto

Macie può recuperare l'elenco da Amazon S3 ma l'elenco non contiene alcun contenuto.

Per risolvere questo errore, scarica l'oggetto da Amazon S3 e assicurati che contenga le voci corrette. Se le voci sono corrette, controlla le impostazioni dell'elenco in Macie. Assicurati che i nomi dei bucket e degli oggetti specificati siano corretti.

Oggetto non trovato

L'elenco non esiste in Amazon S3.

Per risolvere questo errore, controlla le impostazioni dell'elenco in Macie. Assicurati che i nomi dei bucket e degli oggetti specificati siano corretti.

Quota superata

Macie può accedere all'elenco in Amazon S3. Tuttavia, il numero di voci nell'elenco o le dimensioni di archiviazione dell'elenco superano la quota prevista per un elenco consentito.

Per risolvere questo errore, suddividi l'elenco in più file. Assicurati che ogni file contenga meno di 100.000 voci. Assicurati inoltre che la dimensione di ogni file sia inferiore a 35 MB. Quindi, carica ogni file su Amazon S3. Al termine, configura le impostazioni degli elenchi consentiti in Macie per ogni file. Puoi avere fino a cinque elenchi di testo predefinito per ogni lista supportata. Regione AWS

Limitato

Amazon S3 ha limitato la richiesta di recupero dell'elenco.

Per risolvere questo errore, attendi qualche minuto e poi scegli nuovamente refresh ().



Accesso utente negato

Amazon S3 ha negato la richiesta di recupero dell'oggetto. Se l'oggetto specificato esiste, non ti è consentito accedervi o è crittografato con una AWS KMS chiave che non sei autorizzato a utilizzare.

Per risolvere questo errore, collabora con l'AWS amministratore per assicurarti che le impostazioni dell'elenco specifichino i nomi corretti del bucket e degli oggetti e che tu disponga dell'accesso in lettura al bucket e all'oggetto. Se l'oggetto è crittografato, assicurati che sia crittografato con una chiave che sei autorizzato a utilizzare.

4. Per rivedere le impostazioni e lo stato di un elenco specifico, scegli il nome dell'elenco.

API

Per verificare lo stato di un elenco di prodotti consentiti a livello di programmazione, utilizza il [GetAllowList](#) funzionamento dell'API Amazon Macie. Oppure, se utilizzi il AWS CLI, esegui il comando. [get-allow-list](#)

Per il `id` parametro, specificate l'identificatore univoco per l'elenco consentito di cui desiderate controllare lo stato. Per ottenere questo identificatore, puoi usare l'[ListAllowLists](#) operazione. L'[ListAllowLists](#) operazione recupera informazioni su tutti gli elenchi consentiti per il tuo account. Se utilizzi il AWS CLI, puoi eseguire il [list-allow-lists](#) comando per recuperare queste informazioni.

Quando invii una [GetAllowList](#) richiesta, Macie verifica tutte le impostazioni dell'elenco consentito. Se le impostazioni specificano un'espressione regolare (`regex`), Macie verifica che sia in grado di compilare l'espressione. Se le impostazioni specificano un elenco di testo predefinito (`s3WordsList`), Macie verifica di poter recuperare e analizzare l'elenco.

Macie restituisce quindi un `GetAllowListResponse` oggetto che fornisce i dettagli dell'elenco consentito. `GetAllowListResponse` Nell'oggetto, l'`status` oggetto indica lo stato corrente dell'elenco: un codice di stato (`code`) e, a seconda del codice di stato, una breve descrizione dello status (`description`) dell'elenco.

Se l'elenco consentito specifica un'espressione regolare, il codice di stato è in genere OK e non è associata una descrizione. Ciò significa che Macie ha compilato l'espressione con successo.

Se l'elenco degli elementi consentiti specifica un testo predefinito, il codice di stato varia in base ai risultati del test:

- Se Macie ha recuperato e analizzato l'elenco correttamente, il codice di stato è valido OK e non c'è una descrizione associata.
- Se un errore ha impedito a Macie di recuperare o analizzare l'elenco, il codice di stato e la descrizione indicano la natura dell'errore che si è verificato.

Per un elenco di possibili codici di stato e una descrizione di ciascuno di essi, consulta [AllowListStatus](#) Amazon Macie API Reference.

Modifica di un elenco consentito

Dopo aver creato un elenco consentito, puoi modificare la maggior parte delle impostazioni dell'elenco in Amazon Macie. Ad esempio, puoi modificare il nome e la descrizione dell'elenco. Puoi anche aggiungere e modificare i tag per l'elenco. L'unica impostazione che non puoi modificare è il tipo di elenco. Ad esempio, se un elenco esistente specifica un'espressione regolare (regex), non è possibile cambiarne il tipo in testo predefinito.

Se un elenco consentito specifica un testo predefinito, puoi anche modificare le voci nell'elenco. A tale scopo, aggiorna il file che contiene le voci. Quindi carica la nuova versione del file su Amazon Simple Storage Service (Amazon S3). La prossima volta che Macie si prepara a utilizzare l'elenco, Macie recupera l'ultima versione del file da Amazon S3. Quando carichi il nuovo file, assicurati di archiviarlo nello stesso bucket e oggetto S3. Oppure, se modifichi il nome del bucket o dell'oggetto, assicurati di aggiornare le impostazioni dell'elenco in Macie.

Per modificare le impostazioni di un elenco consentito

Puoi modificare le impostazioni per un elenco di prodotti consentiti utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per modificare le impostazioni di un elenco consentito utilizzando la console Amazon Macie.

Per modificare le impostazioni di un elenco consentito utilizzando la console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Consenti elenchi.
3. Nella pagina Consenti elenchi, scegli il nome dell'elenco consentito che desideri modificare. Viene visualizzata la pagina dell'elenco degli elenchi consentiti in cui sono visualizzate le impostazioni correnti dell'elenco.
4. Per aggiungere o modificare i tag per l'elenco consentito, scegli Gestisci tag nella sezione Tag. Quindi, se necessario, modifica i tag. Al termine, scegli Salva.

5. Per modificare altre impostazioni per l'elenco dei file consentiti, scegli **Modifica** nella sezione **Impostazioni elenco**. Quindi modifica le impostazioni che desideri:

- **Nome:** inserisci un nuovo nome per l'elenco. Il nome può contenere fino a un massimo di 128 caratteri.
- **Descrizione:** immettere una nuova descrizione dell'elenco. La descrizione può contenere fino a 512 caratteri.
- Se l'elenco consentito specifica un testo predefinito:
 - **Nome del bucket S3:** inserisci il nome del bucket che memorizza l'elenco.

In Amazon S3, puoi trovare questo valore nel campo **Nome delle proprietà del bucket**. Questo valore prevede la distinzione tra lettere maiuscole e minuscole. Inoltre, non utilizzare caratteri jolly o valori parziali quando inserisci il nome.

- **Nome dell'oggetto S3:** inserisci il nome dell'oggetto S3 che memorizza l'elenco.

In Amazon S3, puoi trovare questo valore nel campo **Chiave delle proprietà dell'oggetto**. Se il nome include un percorso, assicurati di includere il percorso completo quando inserisci il nome, ad esempio `allowlists/macie/mylist.txt`. Questo valore prevede la distinzione tra lettere maiuscole e minuscole. Inoltre, non utilizzate caratteri jolly o valori parziali quando inserite il nome.

- Se l'elenco consentito specifica un'espressione regolare (regex), inserite una nuova espressione regolare nella casella **Espressione regolare**. L'espressione regolare può contenere fino a 512 caratteri.

Dopo aver inserito la nuova espressione regolare, opzionalmente testala. A tale scopo, inserisci fino a 1.000 caratteri nella casella **Dati di esempio**, quindi scegli **Test**. Macie valuta i dati di esempio e riporta il numero di occorrenze di testo che corrispondono all'espressione regolare. Puoi ripetere questo passaggio tutte le volte che vuoi per rifinire e ottimizzare l'espressione regolare prima di salvare le modifiche.

6. Al termine, scegli **Salva**.

Macie verifica le impostazioni dell'elenco. Per un elenco di testo predefinito, Macie verifica inoltre di poter recuperare l'elenco da Amazon S3 e analizzarne il contenuto. Per quanto riguarda l'espressione regolare, Macie verifica anche di poter compilare l'espressione. Se si verifica un errore, Macie visualizza un messaggio che descrive l'errore. Per informazioni dettagliate che

possono aiutarti a risolvere l'errore, consulta. [Opzioni di configurazione e requisiti per gli elenchi di autorizzazioni](#) Dopo aver corretto gli errori, puoi salvare le modifiche.

API

Per modificare le impostazioni di un elenco di autorizzazioni a livello di codice, utilizza il [UpdateAllowList](#) funzionamento dell'API Amazon Macie. Oppure, se utilizzi il AWS CLI, esegui il comando. [update-allow-list](#) Nella richiesta, utilizza i parametri supportati per specificare un nuovo valore per ogni impostazione che desideri modificare. Nota che i name parametri `criteriaid`, e sono obbligatori. Se non desiderate modificare il valore di un parametro obbligatorio, specificate il valore corrente per il parametro.

Ad esempio, il comando seguente modifica il nome e la descrizione di un elenco di autorizzazioni esistente. L'esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 update-allow-list ^  
--id km2d4y22hp6rv05example ^  
--name my_allow_list-email ^  
--criteria={"regex\":"[a-z]@example.com\"} ^  
--description "Ignores all email addresses for the example.com domain"
```

Dove:

- *km2d4y22hp6rv05example* è l'identificatore univoco dell'elenco.
- *my_allow_list-email* è il nuovo nome dell'elenco.
- *[a-z]@example.com* è il criterio della lista, un'espressione regolare.
- *Ignores all email addresses for the example.com domain* è la nuova descrizione dell'elenco.

Quando invii la richiesta, Macie verifica le impostazioni dell'elenco. Se l'elenco specifica un testo predefinito (`s3WordsList`), ciò include la verifica che Macie possa recuperare l'elenco da Amazon S3 e analizzarne il contenuto. Se l'elenco specifica una regex (`regex`), ciò include la verifica che Macie sia in grado di compilare l'espressione.

Se si verifica un errore durante il test delle impostazioni da parte di Macie, la richiesta ha esito negativo e Macie restituisce un messaggio che descrive l'errore. Per informazioni dettagliate che possono aiutarti a risolvere l'errore, consulta. [Opzioni di configurazione e requisiti per gli elenchi di](#)

[autorizzazioni](#) Se la richiesta fallisce per un altro motivo, Macie restituisce una risposta HTTP 4xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Se la richiesta ha esito positivo, Macie aggiorna le impostazioni dell'elenco e ricevi un output simile al seguente.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
  "id": "km2d4y22hp6rv05example"
}
```

`arn` è l'Amazon Resource Name (ARN) dell'elenco consentito che è stato aggiornato ed `id` è l'identificatore univoco dell'elenco.

Eliminazione di un elenco consentito

Quando elimini un elenco di prodotti consentiti in Amazon Macie, elimini definitivamente tutte le impostazioni dell'elenco. Queste impostazioni non possono essere ripristinate dopo essere state eliminate. Se le impostazioni specificano un elenco di testo predefinito che memorizzi in Amazon Simple Storage Service (Amazon S3), Macie non elimina l'oggetto S3 che memorizza l'elenco. Vengono eliminate solo le impostazioni di Macie.

Se configuri i processi di rilevamento dei dati sensibili per utilizzare un elenco di dati consentiti che successivamente elimini, i processi verranno eseguiti come pianificato. Tuttavia, i risultati dei processi, sia quelli rilevati con dati sensibili che quelli relativi all'individuazione di dati sensibili, potrebbero riportare il testo precedentemente specificato nell'elenco dei dati consentiti. Allo stesso modo, se configuri l'individuazione automatica dei dati sensibili per utilizzare un elenco che successivamente elimini, continueranno i cicli di analisi giornalieri. Tuttavia, le rilevazioni di dati sensibili, le statistiche e altri tipi di risultati potrebbero riportare il testo specificato in precedenza nell'elenco dei dati consentiti.

Prima di eliminare un elenco consentito, ti consigliamo di [esaminare l'inventario dei lavori](#) per identificare i lavori che utilizzano l'elenco e che sono programmati per essere eseguiti in futuro. Nell'inventario, il pannello dei dettagli indica se un lavoro è configurato per utilizzare elenchi consentiti e, in caso affermativo, quali. Ti consigliamo di [controllare anche le impostazioni per il rilevamento automatico dei dati sensibili](#). Potresti decidere che è meglio modificare un elenco anziché eliminarlo.

Come ulteriore protezione, Macie controlla le impostazioni di tutti i tuoi lavori quando tenti di eliminare un elenco consentito. Se hai configurato dei lavori per utilizzare l'elenco e uno di questi lavori ha uno stato diverso da Completato o Annullato, Macie non elimina l'elenco a meno che tu non fornisca un'ulteriore conferma.

Per eliminare un elenco consentito

Puoi eliminare un elenco di prodotti consentiti utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per eliminare un elenco di prodotti consentiti utilizzando la console Amazon Macie.

Per eliminare un elenco di elementi consentiti utilizzando la console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, in Impostazioni, scegli Consenti elenchi.
3. Nella pagina Consenti elenchi, seleziona la casella di controllo relativa all'elenco consentito che desideri eliminare.
4. Dal menu Actions (Operazioni), scegli Delete (Elimina).
5. Quando viene richiesta la conferma, inserisci **delete** e scegli Delete (Elimina).

API

Per eliminare un elenco di prodotti consentiti a livello di programmazione, utilizza il [DeleteAllowList](#) funzionamento dell'API Amazon Macie. Per il `id` parametro, specifica l'identificatore univoco per l'elenco consentito da eliminare. È possibile ottenere questo identificatore utilizzando l'[ListAllowLists](#) operazione. L'[ListAllowLists](#) operazione recupera informazioni su tutti gli elenchi consentiti per il tuo account. Se utilizzi il AWS CLI, puoi eseguire il [list-allow-lists](#) comando per recuperare queste informazioni.

Per il `ignoreJobChecks` parametro, specifica se forzare l'eliminazione dell'elenco, anche se i processi di rilevamento di dati sensibili sono configurati per utilizzare l'elenco:

- Se lo specifichi `false`, Macie controlla le impostazioni di tutti i tuoi lavori con uno stato diverso da COMPLETE o CANCELLED. Se nessuno di questi lavori è configurato per utilizzare l'elenco,

Macie elimina l'elenco in modo permanente. Se uno di questi lavori è configurato per utilizzare l'elenco, Macie rifiuta la richiesta e restituisce un errore HTTP 400 (). `ValidationException` Il messaggio di errore indica il numero di lavori applicabili per un massimo di 200 lavori.

- Se `loSpecificit>true`, Macie elimina definitivamente l'elenco senza controllare le impostazioni per nessuno dei tuoi lavori.

Per eliminare un elenco consentito utilizzando il AWS CLI, esegui il comando. [delete-allow-list](#) Per esempio:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks false
```

nkr81bmtu2542yyexample Dov'è l'identificatore univoco dell'elenco consentito da eliminare.

Se la richiesta ha esito positivo, Macie restituisce una risposta HTTP 200 vuota. Altrimenti, Macie restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Se l'elenco degli elementi consentiti specificava un testo predefinito, puoi facoltativamente eliminare l'oggetto S3 che memorizza l'elenco. Tuttavia, la conservazione di questo oggetto può contribuire a garantire una cronologia immutabile delle rilevazioni e dei risultati delle scoperte di dati sensibili per controlli o indagini sulla privacy e sulla protezione dei dati.

Esecuzione del rilevamento automatico di dati sensibili

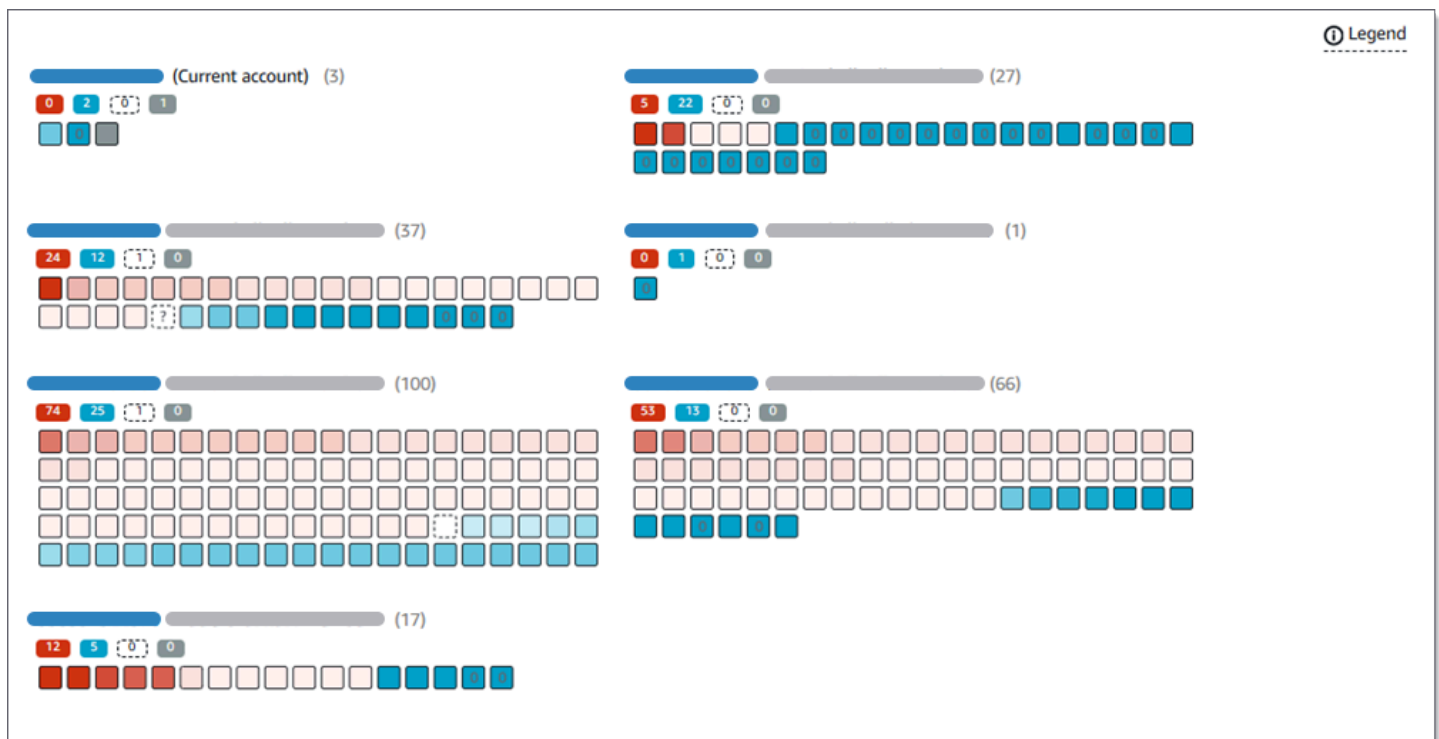
Per un'ampia visibilità su dove potrebbero risiedere i dati sensibili nel tuo patrimonio di dati Amazon Simple Storage Service (Amazon S3), configura Amazon Macie per eseguire il rilevamento automatico dei dati sensibili per il tuo account o la tua organizzazione. Grazie al rilevamento automatico dei dati sensibili, Macie valuta continuamente l'inventario dei bucket S3 e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi nei bucket. Macie quindi recupera e analizza gli oggetti selezionati, ispezionandoli alla ricerca di dati sensibili.

Per impostazione predefinita, Macie seleziona e analizza gli oggetti da tutti i bucket generici S3. Se sei l'amministratore Macie di un'organizzazione, questo include gli oggetti nei bucket di proprietà dei tuoi account membro. Puoi modificare l'ambito delle analisi escludendo bucket specifici. Ad esempio, è possibile escludere i bucket che in genere AWS memorizzano i dati di registrazione. Se sei un amministratore di Macie, un'opzione aggiuntiva consiste nell'abilitare o disabilitare l'individuazione

automatica dei dati sensibili per i singoli account dell'organizzazione su base individuale. case-by-case

Puoi personalizzare le analisi per concentrarti su tipi specifici di dati sensibili. Per impostazione predefinita, Macie analizza gli oggetti S3 utilizzando il set di identificatori di dati gestiti che consigliamo per il rilevamento automatico di dati sensibili. Per personalizzare le analisi, puoi configurare Macie in modo che utilizzi identificatori di [dati gestiti specifici forniti da Macie, identificatori di dati personalizzati definiti dall'utente o una combinazione dei due](#). [Puoi anche perfezionare le analisi configurando Macie in modo che utilizzi gli elenchi di autorizzazioni da te specificati](#).

Man mano che l'analisi procede ogni giorno, Macie registra i dati sensibili che trova e le analisi che esegue: i risultati dei dati sensibili, che riportano i dati sensibili che Macie trova nei singoli oggetti S3, e i risultati della scoperta dei dati sensibili, che registrano i dettagli sull'analisi dei singoli oggetti S3. Macie aggiorna anche statistiche, dati di inventario e altre informazioni che fornisce sui dati di Amazon S3. Ad esempio, una mappa termica interattiva sulla console fornisce una rappresentazione visiva della sensibilità dei dati in tutto il tuo patrimonio di dati:



Queste funzionalità sono progettate per aiutarti a valutare la sensibilità dei dati in tutto il tuo patrimonio di dati Amazon S3 e ad approfondire l'analisi e la valutazione di singoli account, bucket e oggetti. Possono anche aiutarti a determinare dove eseguire analisi più approfondite e immediate [eseguendo processi di rilevamento di dati sensibili](#). Oltre alle informazioni fornite da Macie sulla sicurezza e la privacy dei dati di Amazon S3, puoi anche utilizzare queste funzionalità per identificare

i casi in cui potrebbe essere necessaria una correzione immediata, ad esempio un bucket accessibile al pubblico in cui Macie ha trovato dati sensibili.

Per configurare e gestire l'individuazione automatica dei dati sensibili, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo.

Argomenti

- [Come funziona l'individuazione automatica dei dati sensibili](#)
- [Configurazione del rilevamento automatico dei dati sensibili](#)
- [Revisione dei risultati automatizzati del rilevamento di dati sensibili](#)
- [Valutazione della copertura automatizzata del rilevamento di dati sensibili](#)
- [Regolazione dei punteggi di sensibilità per i bucket S3](#)
- [Punteggio di sensibilità per i bucket S3](#)
- [Impostazioni predefinite per l'individuazione automatica dei dati sensibili](#)

Come funziona l'individuazione automatica dei dati sensibili

Quando abiliti Amazon Macie per il tuo account Account AWS, Macie crea un [ruolo collegato al servizio AWS Identity and Access Management](#) (IAM) per il tuo account nella versione corrente. Regione AWS La politica di autorizzazione per questo ruolo consente a Macie di chiamare altri utenti Servizi AWS e monitorare le risorse per tuo conto. AWS Utilizzando questo ruolo, Macie genera e gestisce un inventario dei tuoi bucket generici Amazon Simple Storage Service (Amazon S3) nella regione. L'inventario include informazioni su ciascuno dei bucket S3 e degli oggetti in essi contenuti. Se sei l'amministratore Macie di un'organizzazione, il tuo inventario include informazioni sui bucket di proprietà dei tuoi account membro. Per ulteriori informazioni, consulta [Gestione di più account](#).

Se abiliti il rilevamento automatico dei dati sensibili, Macie valuta i dati dell'inventario su base giornaliera per identificare gli oggetti S3 idonei per il rilevamento automatico. Come parte della valutazione, Macie seleziona anche un campione di oggetti rappresentativi da analizzare. Macie recupera e analizza quindi la versione più recente di ogni oggetto selezionato, ispezionandolo alla ricerca di dati sensibili.

Man mano che l'analisi procede ogni giorno, Macie aggiorna le statistiche, i dati di inventario e altre informazioni che fornisce sui dati di Amazon S3. Macie registra anche i dati sensibili che trova e le analisi che esegue. I dati risultanti forniscono informazioni su dove Macie ha trovato dati sensibili nel tuo patrimonio di dati Amazon S3, che possono riguardare tutti i bucket S3 generici del tuo account.

I dati possono aiutarti a valutare la sicurezza e la privacy dei tuoi dati Amazon S3, determinare dove eseguire un'indagine più approfondita e identificare i casi in cui è necessaria una correzione.

Per una breve dimostrazione di come funziona il rilevamento automatico di dati sensibili, guarda il seguente video: [Panoramica del rilevamento automatizzato dei dati di Amazon Macie](#).

Per configurare e gestire il rilevamento automatico di dati sensibili, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo. Se il tuo account fa parte di un'organizzazione, solo l'amministratore Macie dell'organizzazione può abilitare o disabilitare il rilevamento automatico degli account dell'organizzazione. Inoltre, solo l'amministratore Macie può configurare e gestire le impostazioni di rilevamento automatico per gli account. Ciò include impostazioni che definiscono l'ambito e la natura delle analisi eseguite da Macie. Se disponi di un account membro in un'organizzazione, contatta l'amministratore di Macie per conoscere le impostazioni del tuo account e della tua organizzazione.

Argomenti

- [Componenti chiave](#)
- [Considerazioni](#)

Componenti chiave

Amazon Macie utilizza una combinazione di caratteristiche e tecniche per eseguire il rilevamento automatico di dati sensibili. Questi funzionano insieme alle funzionalità fornite da Macie per aiutarti a [monitorare i dati di Amazon S3 per motivi di sicurezza e](#) controllo degli accessi.

Selezione degli oggetti S3 da analizzare

Su base giornaliera, Macie valuta i dati dell'inventario Amazon S3 per identificare gli oggetti S3 idonei all'analisi mediante rilevamento automatico di dati sensibili. Se sei l'amministratore Macie di un'organizzazione, per impostazione predefinita la valutazione include i dati per i bucket S3 di proprietà dei tuoi account membro.

Come parte della valutazione, Macie utilizza tecniche di campionamento per selezionare oggetti S3 rappresentativi da analizzare. Le tecniche definiscono gruppi di oggetti che hanno metadati simili e che probabilmente hanno contenuti simili. I gruppi si basano su dimensioni quali il nome del bucket, il prefisso, la classe di archiviazione, l'estensione del nome di file e la data dell'ultima modifica. Macie seleziona quindi un set rappresentativo di campioni da ciascun gruppo, recupera la versione più recente di ogni oggetto selezionato da Amazon S3 e analizza ogni oggetto

selezionato per determinare se l'oggetto contiene dati sensibili. Quando l'analisi è completa, Macie scarta la sua copia dell'oggetto.

La strategia di campionamento dà priorità alle analisi distribuite. In generale, utilizza un approccio innovativo al tuo patrimonio di dati Amazon S3. Ogni giorno, viene selezionato un set rappresentativo di oggetti S3 dal maggior numero possibile di bucket generici in base alla dimensione totale di storage di tutti gli oggetti classificabili nel tuo patrimonio di dati Amazon S3. Ad esempio, se Macie ha già analizzato e trovato dati sensibili negli oggetti in un bucket e non ha ancora analizzato gli oggetti in un altro bucket, quest'ultimo bucket ha una priorità maggiore per l'analisi. Con questo approccio, ottieni più rapidamente informazioni dettagliate sulla sensibilità dei tuoi dati Amazon S3. A seconda della dimensione del patrimonio di dati, i risultati dell'analisi possono iniziare a comparire entro 48 ore.

La strategia di campionamento dà inoltre priorità all'analisi di diversi tipi di oggetti S3 e oggetti che sono stati creati o modificati di recente. Non è garantito che ogni singolo campione di oggetto sia conclusivo. Pertanto, l'analisi di un insieme diversificato di oggetti può fornire una migliore comprensione dei tipi e della quantità di dati sensibili che un bucket S3 potrebbe contenere. Inoltre, dare priorità agli oggetti nuovi o modificati di recente aiuta l'analisi ad adattarsi alle modifiche all'inventario dei bucket. Ad esempio, se gli oggetti vengono creati o modificati dopo un'analisi precedente, tali oggetti hanno una priorità maggiore per l'analisi successiva. Al contrario, se un oggetto è stato analizzato in precedenza e non è cambiato da quell'analisi, Macie non lo analizza nuovamente. Questo approccio consente di stabilire linee di base di sensibilità per i singoli bucket S3. Quindi, man mano che le analisi continue e incrementalmente procedono per il tuo account, le valutazioni di sensibilità dei singoli bucket possono diventare sempre più approfondite e dettagliate a un ritmo prevedibile.

Definizione dell'ambito delle analisi

Per impostazione predefinita, Macie include tutti i bucket S3 generici per l'account quando valuta i dati dell'inventario e seleziona gli oggetti S3 da analizzare. Se sei l'amministratore Macie di un'organizzazione, questo include i bucket di proprietà dei tuoi account membro.

Puoi modificare l'ambito delle analisi escludendo specifici bucket S3 dal rilevamento automatico dei dati sensibili. Ad esempio, potresti voler escludere i bucket che in genere memorizzano i dati di AWS registrazione, come i registri degli eventi. AWS CloudTrail Per escludere un bucket, puoi modificare le impostazioni di rilevamento automatico per il tuo account o per il bucket. Se lo fai, Macie inizia a escludere il bucket all'inizio del successivo ciclo giornaliero di valutazione e analisi. Puoi escludere fino a 1.000 bucket dalle analisi. Se escludi un bucket S3, puoi includerlo di nuovo in un secondo momento. Per fare ciò, modifica nuovamente le impostazioni del tuo account o

del bucket. Macie inizia quindi a includere il bucket quando inizia il successivo ciclo giornaliero di valutazione e analisi.

Se sei l'amministratore Macie di un'organizzazione, puoi anche abilitare o disabilitare il rilevamento automatico dei dati sensibili per i singoli account dell'organizzazione. Se disabiliti il rilevamento automatico per un account, Macie esclude tutti i bucket S3 di proprietà dell'account. Se successivamente riattivi il rilevamento automatico per l'account, Macie ricomincia a includere i bucket.

Determinazione dei tipi di dati sensibili da rilevare e segnalare

Per impostazione predefinita, Macie ispeziona gli oggetti S3 utilizzando il set di identificatori di dati gestiti che consigliamo per l'individuazione automatica dei dati sensibili. Per un elenco di questi identificatori di dati gestiti, consulta [Impostazioni predefinite per l'individuazione automatica dei dati sensibili](#)

Puoi personalizzare le analisi per concentrarti su tipi specifici di dati sensibili. A tale scopo, modifica le impostazioni di rilevamento automatico in uno dei seguenti modi:

- Aggiungere o rimuovere identificatori di dati gestiti: un identificatore di dati gestito è un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili, come numeri di carte di credito, chiavi di accesso AWS segrete o numeri di passaporto per un determinato paese o area geografica. Per ulteriori informazioni, consulta [Utilizzo di identificatori di dati gestiti](#).
- Aggiungere o rimuovere identificatori di dati personalizzati: un identificatore di dati personalizzato è un insieme di criteri definiti per rilevare dati sensibili. Con gli identificatori di dati personalizzati, puoi rilevare dati sensibili che riflettono scenari particolari, proprietà intellettuale o dati proprietari della tua organizzazione. Ad esempio, puoi rilevare i numeri di account dei dipendenti IDs, dei clienti o le classificazioni interne dei dati. Per ulteriori informazioni, consulta [Creazione di identificatori di dati personalizzati](#).
- Aggiungere o rimuovi elenchi consentiti: in Macie, un elenco di elementi consentiti specifica il testo o uno schema di testo che desideri che Macie ignori negli oggetti S3. Si tratta in genere di eccezioni relative ai dati sensibili per scenari o ambienti particolari, come nomi pubblici o numeri di telefono dell'organizzazione o dati di esempio utilizzati dall'organizzazione per i test. Per ulteriori informazioni, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).

Se modifichi un'impostazione, Macie applica la modifica all'inizio del successivo ciclo di analisi giornaliero. Se sei l'amministratore Macie di un'organizzazione, Macie utilizza le impostazioni del tuo account quando analizza gli oggetti S3 per altri account dell'organizzazione.

Puoi anche configurare impostazioni a livello di bucket che determinano se tipi specifici di dati sensibili sono inclusi nelle valutazioni della sensibilità di un bucket. Per scoprire come, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Calcolo dei punteggi di sensibilità

Per impostazione predefinita, Macie calcola automaticamente un punteggio di sensibilità per ogni bucket S3 generico del tuo account. Se sei l'amministratore Macie di un'organizzazione, questo include i bucket di proprietà dei tuoi account membro.

In Macie, un punteggio di sensibilità è una misura quantitativa dell'intersezione di due dimensioni principali: la quantità di dati sensibili che Macie ha trovato in un bucket e la quantità di dati che Macie ha analizzato in un bucket. Il punteggio di sensibilità di un bucket determina l'etichetta di sensibilità che Macie assegna al bucket. Un'etichetta di sensibilità è una rappresentazione qualitativa del punteggio di sensibilità di un bucket, ad esempio Sensibile, Non sensibile e Non ancora analizzato. Per dettagli sulla gamma di punteggi di sensibilità ed etichette definiti da Macie, consulta [Punteggi di sensibilità per i bucket S3](#)

Important

Il punteggio di sensibilità e l'etichetta di un bucket S3 non implicano o indicano in altro modo la criticità o l'importanza che il bucket o gli oggetti del bucket potrebbero avere per te o la tua organizzazione. Al contrario, hanno lo scopo di fornire punti di riferimento che possono aiutarti a identificare e monitorare i potenziali rischi per la sicurezza.

Quando abiliti il rilevamento automatico dei dati sensibili per la prima volta, Macie assegna automaticamente un punteggio di sensibilità di 50 e l'etichetta Non ancora analizzato a ciascun bucket S3. L'eccezione sono i bucket vuoti. Un bucket vuoto è un bucket che non memorizza alcun oggetto o che tutti gli oggetti del bucket contengono zero (0) byte di dati. Se questo è il caso di un bucket, Macie assegna un punteggio pari a 1 al bucket e gli assegna l'etichetta Non sensibile.

Man mano che la scoperta automatica dei dati sensibili progredisce, Macie aggiorna i punteggi e le etichette di sensibilità per riflettere i risultati delle sue analisi. Per esempio:

- Se Macie non trova dati sensibili in un oggetto, Macie riduce il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario.
- Se Macie trova dati sensibili in un oggetto, Macie aumenta il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario.

- Se Macie trova dati sensibili in un oggetto che viene successivamente modificato, Macie rimuove i rilevamenti di dati sensibili per l'oggetto dal punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario.
- Se Macie trova dati sensibili in un oggetto che viene successivamente eliminato, Macie rimuove i rilevamenti di dati sensibili per l'oggetto dal punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario.

Puoi regolare le impostazioni del punteggio di sensibilità per i singoli bucket S3 includendo o escludendo tipi specifici di dati sensibili dal punteggio di un bucket. Puoi anche sovrascrivere il punteggio calcolato di un bucket assegnando manualmente il punteggio massimo (100) al bucket. Se assegni il punteggio massimo, l'etichetta del bucket è Sensibile. Per ulteriori informazioni, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Generazione di metadati, statistiche e altri tipi di risultati

Quando abiliti il rilevamento automatico dei dati sensibili, Macie genera e inizia a gestire dati di inventario aggiuntivi, statistiche e altre informazioni sui bucket S3 per uso generico per il tuo account. Se sei l'amministratore Macie di un'organizzazione, per impostazione predefinita sono inclusi i bucket di proprietà dei tuoi account membro.

Le informazioni aggiuntive raccolgono i risultati delle attività automatizzate di rilevamento di dati sensibili che Macie ha svolto finora. Inoltre, integra altre informazioni fornite da Macie sui tuoi dati Amazon S3, come le impostazioni di accesso pubblico e accesso condiviso per i singoli bucket. Le informazioni aggiuntive includono:

- Una rappresentazione visiva e interattiva della sensibilità dei dati in tutto il tuo patrimonio di dati Amazon S3.
- Statistiche aggregate sulla sensibilità dei dati, ad esempio il numero totale di bucket in cui Macie ha trovato dati sensibili e quanti di questi bucket sono accessibili al pubblico.
- Dettagli a livello di bucket che indicano lo stato attuale delle analisi. Ad esempio, un elenco di oggetti che Macie ha analizzato in un bucket, i tipi di dati sensibili che Macie ha trovato in un bucket e il numero di occorrenze di ogni tipo di dati sensibili trovati da Macie.

Le informazioni includono anche statistiche e dettagli che possono aiutarti a valutare e monitorare la copertura dei tuoi dati Amazon S3. Puoi controllare lo stato delle analisi per il tuo patrimonio di dati in generale e per i singoli bucket S3. Puoi anche identificare i problemi che impedivano a Macie di analizzare gli oggetti in bucket specifici. Se risolvi i problemi, puoi aumentare la copertura dei dati di Amazon S3 durante i cicli di analisi successivi. Per ulteriori informazioni, consulta [Valutazione della copertura automatizzata del rilevamento di dati sensibili](#).

Macie ricalcola e aggiorna automaticamente queste informazioni mentre esegue il rilevamento automatico dei dati sensibili. Ad esempio, se Macie trova dati sensibili in un oggetto S3 che viene successivamente modificato o eliminato, Macie aggiorna i metadati del bucket applicabile: rimuove l'oggetto dall'elenco degli oggetti analizzati; rimuove le occorrenze di dati sensibili che Macie ha trovato nell'oggetto; ricalcola il punteggio di sensibilità, se il punteggio viene calcolato automaticamente; e aggiorna l'etichetta di sensibilità se necessario per riflettere il nuovo punteggio.

Oltre ai metadati e alle statistiche, Macie produce registrazioni dei dati sensibili che trova e delle analisi che esegue: rilevamenti di dati sensibili, che riportano i dati sensibili che Macie trova nei singoli oggetti S3, e risultati di rilevamento dei dati sensibili, che registrano i dettagli sull'analisi dei singoli oggetti S3.

Per ulteriori informazioni, consulta [Revisione dei risultati automatizzati del rilevamento di dati sensibili](#).

Considerazioni

Quando configuri e utilizzi Amazon Macie per eseguire il rilevamento automatico di dati sensibili per i tuoi dati Amazon S3, tieni presente quanto segue:

- Le tue impostazioni di rilevamento automatico si applicano solo a quelle correnti. Regione AWS Di conseguenza, le analisi e i dati risultanti si applicano solo ai bucket e agli oggetti generici S3 nella regione corrente. Per eseguire il rilevamento automatico e accedere ai dati risultanti in altre regioni, abilita e configura il rilevamento automatico in ogni regione aggiuntiva.
- Se sei l'amministratore Macie di un'organizzazione:
 - Puoi eseguire l'individuazione automatica di un account membro solo se Macie è abilitato per l'account nella regione corrente. Inoltre, devi abilitare il rilevamento automatico per l'account in quella regione. I membri non possono abilitare o disabilitare il rilevamento automatico per i propri account.
 - Se abiliti il rilevamento automatico per un account membro, Macie utilizza le impostazioni di rilevamento automatico per il tuo account amministratore quando analizza i dati relativi all'account membro. Le impostazioni applicabili sono: l'elenco dei bucket S3 da escludere dalle analisi e gli identificatori di dati gestiti, gli identificatori di dati personalizzati e gli elenchi di dati consentiti da utilizzare per l'analisi degli oggetti S3. I membri non possono rivedere o modificare queste impostazioni.

- I membri non possono accedere alle impostazioni di rilevamento automatico per i singoli bucket S3 di loro proprietà. Ad esempio, un membro non può rivedere o modificare le impostazioni del punteggio di sensibilità per uno dei propri bucket. Solo l'amministratore di Macie può accedere a queste impostazioni.
- I membri hanno accesso in lettura alle statistiche sulla scoperta di dati sensibili e ad altri risultati che Macie fornisce direttamente per i loro bucket S3. Ad esempio, un membro può utilizzare Macie per esaminare i punteggi di sensibilità e i dati di copertura per i propri bucket S3. L'eccezione è rappresentata dai rilevamenti di dati sensibili. Solo l'amministratore di Macie ha accesso diretto ai risultati prodotti dal rilevamento automatico.
- Se le impostazioni delle autorizzazioni di un bucket S3 impediscono a Macie di accedere o recuperare informazioni sul bucket o sugli oggetti del bucket, Macie non può eseguire il rilevamento automatico del bucket. Macie può fornire solo un sottoinsieme di informazioni sul bucket, come l'ID account del proprietario del Account AWS bucket, il nome del bucket e l'ultima data in cui Macie ha recuperato i metadati del bucket e dell'oggetto per il bucket come parte del [ciclo di aggiornamento giornaliero](#). Nel tuo inventario dei bucket, il punteggio di sensibilità per questi bucket è 50 e la loro etichetta di sensibilità Non è ancora stata analizzata. Per identificare i bucket S3 in cui ciò si verifica, puoi fare riferimento ai dati di copertura. Per ulteriori informazioni, consulta [Valutazione della copertura automatizzata del rilevamento di dati sensibili](#).
- Per essere idoneo alla selezione e all'analisi, un oggetto S3 deve essere archiviato in un bucket generico e deve essere classificabile. Un oggetto classificabile utilizza una classe di storage Amazon S3 supportata e ha un'estensione del nome di file per un file o un formato di storage supportato. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).
- Se un oggetto S3 è crittografato, Macie può analizzarlo solo se è crittografato con una chiave a cui Macie può accedere e che può usare. Per ulteriori informazioni, consulta [Analisi di oggetti S3 crittografati](#). Per identificare i casi in cui le impostazioni di crittografia hanno impedito a Macie di analizzare uno o più oggetti in un bucket, puoi fare riferimento ai dati di copertura. Per ulteriori informazioni, consulta [Valutazione della copertura automatizzata del rilevamento di dati sensibili](#).

Configurazione del rilevamento automatico dei dati sensibili

Per ottenere un'ampia visibilità su dove potrebbero risiedere i dati sensibili nel tuo patrimonio di dati Amazon Simple Storage Service (Amazon S3), abilita e configura il rilevamento automatico dei dati sensibili per il tuo account o la tua organizzazione. Amazon Macie valuta quindi l'inventario dei bucket S3 su base giornaliera e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi dai bucket. Macie recupera e analizza gli oggetti selezionati, ispezionandoli

alla ricerca di dati sensibili. Se sei l'amministratore Macie di un'organizzazione, per impostazione predefinita questo include gli oggetti nei bucket S3 di proprietà dei tuoi account membro.

Man mano che l'analisi procede ogni giorno, Macie registra i dati sensibili che trova e le analisi che esegue. Macie aggiorna anche statistiche, dati di inventario e altre informazioni che fornisce sui dati di Amazon S3. I dati risultanti forniscono informazioni su dove Macie ha trovato dati sensibili nel tuo patrimonio di dati Amazon S3, che possono riguardare tutti i bucket S3 del tuo account o della tua organizzazione. Per ulteriori informazioni, consulta [Come funziona l'individuazione automatica dei dati sensibili](#).

Se disponi di un account Macie autonomo o sei l'amministratore Macie di un'organizzazione, puoi configurare e gestire l'individuazione automatica dei dati sensibili per il tuo account o la tua organizzazione. Ciò include l'abilitazione e la disabilitazione del rilevamento automatico e la configurazione di impostazioni che definiscono l'ambito e la natura delle analisi eseguite da Macie. Se disponi di un account membro in un'organizzazione, contatta l'amministratore di Macie per conoscere le impostazioni del tuo account e della tua organizzazione.

Argomenti

- [Prerequisiti per la configurazione del rilevamento automatico dei dati sensibili](#)
- [Abilitare l'individuazione automatica dei dati sensibili](#)
- [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#)
- [Disabilitazione del rilevamento automatico di dati sensibili](#)

Prerequisiti per la configurazione del rilevamento automatico dei dati sensibili

Prima di abilitare o configurare le impostazioni per l'individuazione automatica dei dati sensibili, completa le seguenti attività. Questo aiuta a garantire che tu disponga delle risorse e delle autorizzazioni di cui hai bisogno.

Per completare queste attività, devi essere l'amministratore di Amazon Macie di un'organizzazione o disporre di un account Macie autonomo. Se il tuo account fa parte di un'organizzazione, solo l'amministratore Macie dell'organizzazione può abilitare o disabilitare l'individuazione automatica dei dati sensibili per gli account dell'organizzazione. Inoltre, solo l'amministratore Macie può configurare le impostazioni di rilevamento automatico per gli account.

Attività

- [Fase 1: Configurare un archivio per i risultati del rilevamento dei dati sensibili](#)

- [Passaggio 2: verifica le tue autorizzazioni](#)
- [Passaggi successivi](#)

Fase 1: Configurare un archivio per i risultati del rilevamento dei dati sensibili

Quando Amazon Macie esegue il rilevamento automatico di dati sensibili, crea un record di analisi per ogni oggetto Amazon Simple Storage Service (Amazon S3) selezionato per l'analisi. Questi record, denominati risultati del rilevamento di dati sensibili, registrano dettagli sull'analisi di singoli oggetti S3. Ciò include oggetti in cui Macie non trova dati sensibili e oggetti che Macie non può analizzare a causa di errori o problemi come le impostazioni delle autorizzazioni. Se Macie trova dati sensibili in un oggetto, il risultato della scoperta dei dati sensibili include informazioni sui dati sensibili trovati da Macie. I risultati dell'individuazione di dati sensibili forniscono record di analisi che possono essere utili per controlli o indagini sulla privacy e sulla protezione dei dati.

Macie archivia i risultati della scoperta dei dati sensibili per soli 90 giorni. Per accedere ai risultati e consentirne l'archiviazione e la conservazione a lungo termine, configura Macie in modo che memorizzi i risultati in un bucket S3. Il bucket può fungere da archivio definitivo a lungo termine per tutti i risultati della scoperta di dati sensibili. Se sei l'amministratore Macie di un'organizzazione, questo include i risultati del rilevamento di dati sensibili per gli account dei membri per i quali abiliti il rilevamento automatico dei dati sensibili.

Per verificare di aver configurato questo repository, scegli Risultati Discovery nel riquadro di navigazione sulla console Amazon Macie. Se preferisci eseguire questa operazione a livello di codice, utilizza il [GetClassificationExportConfiguration](#) funzionamento dell'API Amazon Macie. Per ulteriori informazioni sui risultati della scoperta di dati sensibili e su come configurare questo repository, consulta. [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#)

Se hai configurato il repository, Macie crea una cartella denominata `automated-sensitive-data-discovery` nel repository quando abiliti il rilevamento automatico di dati sensibili per la prima volta. Questa cartella memorizza i risultati dell'individuazione dei dati sensibili creati da Macie durante l'esecuzione del rilevamento automatico del tuo account o della tua organizzazione.

Se usi Macie in più di un'area Regioni AWS, verifica di aver configurato il repository per ognuna di queste regioni.

Passaggio 2: verifica le tue autorizzazioni

Per verificare le tue autorizzazioni, utilizza AWS Identity and Access Management (IAM) per esaminare le policy IAM allegate alla tua identità IAM. Quindi confronta le informazioni contenute in tali policy con il seguente elenco di azioni che devi essere autorizzato a eseguire:

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`
- `macie2:ListClassificationScopes`
- `macie2:UpdateClassificationScope`
- `macie2:ListSensitivityInspectionTemplates`
- `macie2:UpdateSensitivityInspectionTemplate`

La prima azione ti consente di accedere al tuo account Amazon Macie. La seconda azione ti consente di abilitare o disabilitare il rilevamento automatico dei dati sensibili per il tuo account o la tua organizzazione. Per un'organizzazione, consente inoltre di abilitare automaticamente il rilevamento automatico degli account dell'organizzazione. Le azioni rimanenti consentono di identificare e modificare le impostazioni di configurazione.

Se prevedi di rivedere o modificare le impostazioni di configurazione utilizzando la console Amazon Macie, devi inoltre avere il permesso di eseguire le seguenti azioni:

- `macie2:GetAutomatedDiscoveryConfiguration`
- `macie2:GetClassificationScope`
- `macie2:GetSensitivityInspectionTemplate`

Queste azioni ti consentono di recuperare le impostazioni di configurazione correnti e lo stato del rilevamento automatico dei dati sensibili per il tuo account o la tua organizzazione. L'autorizzazione a eseguire queste azioni è facoltativa se si prevede di modificare le impostazioni di configurazione a livello di codice.

Se sei l'amministratore Macie di un'organizzazione, devi anche avere il permesso di eseguire le seguenti azioni:

- `macie2:ListAutomatedDiscoveryAccounts`
- `macie2:BatchUpdateAutomatedDiscoveryAccounts`

La prima azione ti consente di recuperare lo stato del rilevamento automatico dei dati sensibili per i singoli account dell'organizzazione. La seconda azione consente di abilitare o disabilitare l'individuazione automatica per i singoli account dell'organizzazione.

Se non sei autorizzato a eseguire le azioni richieste, chiedi assistenza AWS all'amministratore.

Passaggi successivi

Dopo aver completato le attività precedenti, sei pronto per abilitare e configurare le impostazioni per il tuo account o la tua organizzazione:

- [Abilitare l'individuazione automatica dei dati sensibili](#)
- [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#)

Abilitare l'individuazione automatica dei dati sensibili

Quando abiliti il rilevamento automatico di dati sensibili, Amazon Macie inizia a valutare i dati di inventario di Amazon Simple Storage Service (Amazon S3) e a eseguire altre attività di rilevamento automatizzato per il tuo account attualmente disponibili. Regione AWS Se sei l'amministratore Macie di un'organizzazione, per impostazione predefinita la valutazione e le attività includono i bucket S3 di proprietà dei tuoi account membro. A seconda delle dimensioni del tuo patrimonio di dati Amazon S3, le statistiche e altri risultati possono iniziare a comparire entro 48 ore.

Dopo aver abilitato il rilevamento automatico dei dati sensibili, puoi configurare impostazioni che perfezionano l'ambito e la natura delle analisi eseguite da Macie. Queste impostazioni specificano tutti i bucket S3 da escludere dalle analisi. Specificano inoltre gli identificatori di dati gestiti, gli identificatori di dati personalizzati e consentono gli elenchi che desideri che Macie utilizzi quando analizza gli oggetti S3. Per informazioni su queste impostazioni, consulta [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#). Se sei l'amministratore Macie di un'organizzazione, puoi anche affinare l'ambito delle analisi abilitando o disabilitando di volta in volta il rilevamento automatico dei dati sensibili per i singoli account dell'organizzazione. case-by-case

Per abilitare l'individuazione automatica dei dati sensibili, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo. Se hai un account membro in un'organizzazione, collabora con il tuo amministratore Macie per abilitare il rilevamento automatico dei dati sensibili per il tuo account.

Per abilitare l'individuazione automatica dei dati sensibili

Se sei l'amministratore Macie di un'organizzazione o disponi di un account Macie autonomo, puoi abilitare il rilevamento automatico dei dati sensibili utilizzando la console Amazon Macie o l'API Amazon Macie. [Se lo abiliti per la prima volta, inizia completando le attività prerequisite.](#) Questo aiuta a garantire che tu disponga delle risorse e delle autorizzazioni di cui hai bisogno.

Console

Segui questi passaggi per abilitare l'individuazione automatica dei dati sensibili utilizzando la console Amazon Macie.

Per abilitare l'individuazione automatica dei dati sensibili

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri abilitare il rilevamento automatico dei dati sensibili.
3. Nel riquadro di navigazione, in Impostazioni, scegli Rilevamento automatico dei dati sensibili.
4. Se hai un account Macie autonomo, scegli Abilita nella sezione Stato.
5. Se sei l'amministratore Macie di un'organizzazione, scegli un'opzione nella sezione Stato per specificare gli account per abilitare il rilevamento automatico dei dati sensibili per:
 - Per abilitarlo per tutti gli account della tua organizzazione, scegli Abilita. Nella finestra di dialogo che appare, scegli La mia organizzazione. Per un'organizzazione in AWS Organizations, seleziona Abilita automaticamente per i nuovi account per abilitarlo automaticamente anche per gli account che successivamente entrano a far parte della tua organizzazione. Al termine, scegli Abilita.
 - Per abilitarlo solo per determinati account membro, scegli Gestisci account. Quindi, nella tabella della pagina Account, seleziona la casella di controllo relativa a ciascun account per cui abilitarlo. Al termine, scegli Abilita il rilevamento automatico dei dati sensibili nel menu Azioni.
 - Per abilitarlo solo per il tuo account amministratore Macie, scegli Abilita. Nella finestra di dialogo che appare, scegli Il mio account e deseleziona Abilita automaticamente per nuovi account. Al termine, scegli Abilita.

Se usi Macie in più regioni e desideri abilitare l'individuazione automatica dei dati sensibili in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Per controllare o modificare successivamente lo stato del rilevamento automatico dei dati sensibili per i singoli account di un'organizzazione, scegli Account nel riquadro di navigazione. Nella pagina Account, il campo Rilevamento automatico dei dati sensibili nella tabella indica lo stato attuale del rilevamento automatico di un account. Per modificare lo stato di un account, seleziona la casella di controllo relativa all'account. Utilizza quindi il menu Azioni per abilitare o disabilitare il rilevamento automatico per l'account.

API

Per abilitare l'individuazione automatica dei dati sensibili a livello di codice, sono disponibili diverse opzioni:

- Per abilitarlo per un account amministratore Macie, un'organizzazione o un account Macie autonomo, usa l'operazione. [UpdateAutomatedDiscoveryConfiguration](#) Oppure, se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando. [update-automated-discovery-configuration](#)
- Per abilitarlo solo per determinati account membro in un'organizzazione, usa l'[BatchUpdateAutomatedDiscoveryAccounts](#) operazione. In alternativa, se utilizzi il AWS CLI, esegui il comando [batch-update-automated-discovery-accounts](#). Per abilitare l'individuazione automatica di un account membro, devi prima abilitarlo per l'account o l'organizzazione di amministratore.

Le opzioni e i dettagli aggiuntivi variano a seconda del tipo di account di cui disponi.

Se sei un amministratore di Macie, utilizza l'UpdateAutomatedDiscoveryConfiguration operazione o esegui il update-automated-discovery-configuration comando per abilitare l'individuazione automatica dei dati sensibili per il tuo account o la tua organizzazione. Nella richiesta, specifica ENABLED il status parametro. Per il autoEnableOrganizationMembers parametro, specifica gli account per cui abilitarlo. Se utilizzi il AWS CLI, specifica gli account utilizzando il auto-enable-organization-members parametro. I valori validi sono:

- ALL(impostazione predefinita): abilitalo per tutti gli account dell'organizzazione. Ciò include l'account amministratore, gli account dei membri esistenti e gli account che successivamente entrano a far parte dell'organizzazione.
- NEW— Abilitalo per il tuo account amministratore. Inoltre, abilitalo automaticamente per gli account che successivamente entrano a far parte della tua organizzazione. Se in precedenza hai abilitato l'individuazione automatica per la tua organizzazione e specifichi questo valore,

l'individuazione automatica continuerà a essere abilitata per gli account dei membri esistenti per i quali è attualmente abilitata.

- **NONE**— Abilitalo solo per il tuo account amministratore. Non abilitarlo automaticamente per gli account che successivamente entrano a far parte della tua organizzazione. Se in precedenza hai abilitato l'individuazione automatica per la tua organizzazione e specifichi questo valore, l'individuazione automatica continuerà a essere abilitata per gli account dei membri esistenti per i quali è attualmente abilitata.

Se desideri abilitare in modo selettivo il rilevamento automatico dei dati sensibili solo per determinati account membro, specifica **NEW** o **NONE**. È quindi possibile utilizzare l'`BatchUpdateAutomatedDiscoveryAccounts` operazione o eseguire il `batch-update-automated-discovery-accounts` comando per abilitare l'individuazione automatica degli account.

Se disponi di un account Macie autonomo, utilizza l'`UpdateAutomatedDiscoveryConfiguration` operazione o esegui il `update-automated-discovery-configuration` comando per abilitare il rilevamento automatico dei dati sensibili per il tuo account. Nella richiesta, specifica **ENABLED** il `status` parametro. Per il `autoEnableOrganizationMembers` parametro, valuta se intendi diventare l'amministratore di Macie per altri account e specifica il valore appropriato. Se lo specifichi **NONE**, il rilevamento automatico non viene abilitato automaticamente per un account quando diventi l'amministratore Macie dell'account. Se specifichi **ALL** o **NEW**, il rilevamento automatico viene abilitato automaticamente per l'account. Se utilizzi il AWS CLI, utilizza il `auto-enable-organization-members` parametro per specificare il valore appropriato per questa impostazione.

Gli esempi seguenti mostrano come utilizzare per AWS CLI abilitare l'individuazione automatica dei dati sensibili per uno o più account in un'organizzazione. Questo primo esempio consente per la prima volta l'individuazione automatica di tutti gli account di un'organizzazione. Consente l'individuazione automatica dell'account amministratore di Macie, di tutti gli account membro esistenti e di tutti gli account che successivamente entrano a far parte dell'organizzazione.

```
$ aws macie2 update-automated-discovery-configuration --status ENABLED --auto-  
enable-organization-members ALL --region us-east-1
```

us-east-1 Dov'è la regione in cui abilitare il rilevamento automatico dei dati sensibili per gli account, la regione Stati Uniti orientali (Virginia settentrionale). Se la richiesta ha esito positivo, Macie abilita il rilevamento automatico degli account e restituisce una risposta vuota.

L'esempio successivo modifica l'impostazione di abilitazione dei membri per un'organizzazione in. NONE Con questa modifica, l'individuazione automatica dei dati sensibili non viene abilitata automaticamente per gli account che successivamente entrano a far parte dell'organizzazione. È invece abilitato solo per l'account amministratore di Macie e per tutti gli account membro esistenti per cui è attualmente abilitato.

```
$ aws macie2 update-automated-discovery-configuration --status ENABLED --auto-  
enable-organization-members NONE --region us-east-1
```

us-east-1 Dov'è la regione in cui modificare l'impostazione, la regione Stati Uniti orientali (Virginia settentrionale). Se la richiesta ha esito positivo, Macie aggiorna l'impostazione e restituisce una risposta vuota.

Gli esempi seguenti consentono l'individuazione automatica di dati sensibili per due account membri di un'organizzazione. L'amministratore Macie ha già abilitato il rilevamento automatico per l'organizzazione. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws macie2 batch-update-automated-discovery-accounts \  
--region us-east-1 \  
--accounts ' [{"accountId": "123456789012", "status": "ENABLED"},  
{ "accountId": "111122223333", "status": "ENABLED"} ] '
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 batch-update-automated-discovery-accounts ^  
--region us-east-1 ^  
--accounts=[{"accountId\":"123456789012",\"status\":"ENABLED\"},{\"accountId\":"  
\"111122223333\",\"status\":"ENABLED\"}]
```

Dove:

- **us-east-1** è la regione in cui abilitare l'individuazione automatica dei dati sensibili per gli account specificati, la regione Stati Uniti orientali (Virginia settentrionale).
- **123456789012** e **111122223333** sono gli account IDs per i quali consentire l'individuazione automatica dei dati sensibili.

Se la richiesta ha esito positivo per tutti gli account specificati, Macie restituisce un array vuoto `errors`. Se la richiesta fallisce per alcuni account, l'array specifica l'errore che si è verificato per ogni account interessato. Per esempio:

```
"errors": [  
  {  
    "accountId": "123456789012",  
    "errorCode": "ACCOUNT_PAUSED"  
  }  
]
```

Nella risposta precedente, la richiesta non è riuscita per l'account specificato (123456789012) perché Macie è attualmente sospeso per l'account. Per risolvere questo errore, l'amministratore di Macie deve prima abilitare Macie per l'account.

Se la richiesta non riesce per tutti gli account, riceverai un messaggio che descrive l'errore che si è verificato.

Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili

Se abiliti il rilevamento automatico dei dati sensibili per il tuo account o la tua organizzazione, puoi modificare le impostazioni di rilevamento automatico per perfezionare le analisi eseguite da Amazon Macie. Le impostazioni specificano i bucket Amazon Simple Storage Service (Amazon S3) da escludere dalle analisi. Specificano inoltre i tipi e le occorrenze di dati sensibili da rilevare e segnalare: identificatori di dati gestiti, identificatori di dati personalizzati ed elenchi di dati consentiti da utilizzare per l'analisi degli oggetti S3.

Per impostazione predefinita, Macie esegue il rilevamento automatico dei dati sensibili per tutti i bucket S3 generici del tuo account. Se sei l'amministratore Macie di un'organizzazione, questo include i bucket di proprietà dei tuoi account membro. Puoi escludere bucket specifici dalle analisi. Ad esempio, è possibile escludere i bucket che in genere memorizzano dati di AWS registrazione, come i registri degli eventi. AWS CloudTrail Se escludi un bucket, puoi includerlo di nuovo in un secondo momento.

Inoltre, Macie analizza gli oggetti S3 utilizzando solo il set di identificatori di dati gestiti che consigliamo per il rilevamento automatico di dati sensibili. Macie non utilizza identificatori di dati personalizzati né consente elenchi definiti dall'utente. Per personalizzare le analisi, puoi aggiungere o rimuovere identificatori di dati gestiti specifici, identificatori di dati personalizzati ed elenchi di dati consentiti.

Se si modifica un'impostazione, Macie applica la modifica all'avvio del ciclo di valutazione e analisi successivo, in genere entro 24 ore. Inoltre, la modifica si applica solo alla versione corrente Regione AWS. Per apportare la stessa modifica in altre regioni, ripeti i passaggi applicabili in ciascuna regione aggiuntiva.

Argomenti

- [Opzioni di configurazione per le organizzazioni](#)
- [Esclusione o inclusione dei bucket S3 nel rilevamento automatico dei dati sensibili](#)
- [Aggiungere o rimuovere identificatori di dati gestiti dal rilevamento automatico di dati sensibili](#)
- [Aggiungere o rimuovere identificatori di dati personalizzati dal rilevamento automatico di dati sensibili](#)
- [Aggiungere o rimuovere elenchi di dati consentiti dal rilevamento automatico di dati sensibili](#)

Note

Per configurare le impostazioni per l'individuazione automatica dei dati sensibili, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo. Se il tuo account fa parte di un'organizzazione, solo l'amministratore Macie dell'organizzazione può configurare e gestire le impostazioni per gli account dell'organizzazione. Se hai un account membro, contatta l'amministratore di Macie per conoscere le impostazioni del tuo account e della tua organizzazione.

Opzioni di configurazione per le organizzazioni

Se un account fa parte di un'organizzazione che gestisce centralmente più account Amazon Macie, l'amministratore Macie dell'organizzazione configura e gestisce l'individuazione automatica dei dati sensibili per gli account dell'organizzazione. Ciò include impostazioni che definiscono l'ambito e la natura delle analisi eseguite da Macie per gli account. I membri non possono accedere a queste impostazioni per i propri account.

Se sei l'amministratore Macie di un'organizzazione, puoi definire l'ambito delle analisi in diversi modi:

- Abilita automaticamente l'individuazione automatica dei dati sensibili per gli account: quando abiliti l'individuazione automatica dei dati sensibili, specifichi se abilitarla per tutti gli account esistenti e i nuovi account membro, solo per i nuovi account membro o per nessun account membro. Se lo abiliti per gli account dei nuovi membri, viene abilitato automaticamente per tutti gli account che

successivamente entrano a far parte dell'organizzazione, quando l'account entra a far parte della tua organizzazione in Macie. Se è abilitato per un account, Macie include i bucket S3 di proprietà dell'account. Se è disabilitato per un account, Macie esclude i bucket di proprietà dell'account.

- Abilita selettivamente l'individuazione automatica dei dati sensibili per gli account: con questa opzione, abiliti o disabiliti l'individuazione automatica dei dati sensibili per i singoli account su base individuale. case-by-case Se lo abiliti per un account, Macie include i bucket S3 di proprietà dell'account. Se non lo abiliti o lo disabiliti per un account, Macie esclude i bucket di proprietà dell'account.
- Escludi bucket S3 specifici dal rilevamento automatico dei dati sensibili: se abiliti il rilevamento automatico di dati sensibili per un account, puoi escludere determinati bucket S3 di proprietà dell'account. Macie quindi salta i bucket quando esegue il rilevamento automatico. Per escludere determinati bucket, aggiungili all'elenco di esclusione nelle impostazioni di configurazione del tuo account amministratore. Puoi escludere fino a 1.000 bucket per la tua organizzazione.

Per impostazione predefinita, il rilevamento automatico dei dati sensibili è abilitato automaticamente per tutti gli account nuovi ed esistenti in un'organizzazione. Inoltre, Macie include tutti i bucket S3 di proprietà degli account. Se mantieni le impostazioni predefinite, significa che Macie esegue il rilevamento automatico di tutti i bucket del tuo account amministratore, che include tutti i bucket di proprietà degli account membro.

In qualità di amministratore di Macie, definisci anche la natura delle analisi che Macie esegue per la tua organizzazione. Puoi farlo configurando impostazioni aggiuntive per il tuo account amministratore: gli identificatori di dati gestiti, gli identificatori di dati personalizzati e gli elenchi di autorizzazioni che desideri che Macie utilizzi quando analizza gli oggetti S3. Macie utilizza le impostazioni del tuo account amministratore quando analizza gli oggetti S3 per altri account dell'organizzazione.

Esclusione o inclusione dei bucket S3 nel rilevamento automatico dei dati sensibili

Per impostazione predefinita, Amazon Macie esegue il rilevamento automatico dei dati sensibili per tutti i bucket S3 generici del tuo account. Se sei l'amministratore Macie di un'organizzazione, questo include i bucket di proprietà dei tuoi account membro.

Per affinare l'ambito, puoi escludere fino a 1.000 bucket S3 dalle analisi. Se escludi un bucket, Macie interrompe la selezione e l'analisi degli oggetti nel bucket quando esegue il rilevamento automatico dei dati sensibili. Le statistiche e i dettagli esistenti sul rilevamento dei dati sensibili relativi al bucket persistono. Ad esempio, l'attuale punteggio di sensibilità del bucket rimane invariato. Dopo aver escluso un bucket, puoi includerlo nuovamente in un secondo momento.

Per escludere o includere un bucket S3 nel rilevamento automatico dei dati sensibili

Puoi escludere o includere successivamente un bucket S3 utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per escludere o includere successivamente un bucket S3 utilizzando la console Amazon Macie.

Per escludere o includere un bucket S3

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri escludere o includere bucket S3 specifici nelle analisi.
3. Nel pannello di navigazione, in Impostazioni, scegli Rilevamento automatico dei dati sensibili.

Viene visualizzata la pagina di individuazione automatica dei dati sensibili che mostra le impostazioni correnti. In quella pagina, la sezione bucket S3 elenca i bucket S3 attualmente esclusi o indica che tutti i bucket sono attualmente inclusi.

4. Nella sezione bucket S3, scegli Modifica.
5. Esegui una di queste operazioni:
 - Per escludere uno o più bucket S3, scegli Aggiungi bucket all'elenco delle esclusioni. Quindi, nella tabella dei bucket S3, seleziona la casella di controllo per ogni bucket da escludere. La tabella elenca tutti i bucket generici per il tuo account o la tua organizzazione nella regione corrente.
 - Per includere uno o più bucket S3 precedentemente esclusi, scegli Rimuovi bucket dall'elenco di esclusione. Quindi, nella tabella dei bucket S3, seleziona la casella di controllo per ogni bucket da includere. La tabella elenca tutti i bucket attualmente esclusi dalle analisi.

Per trovare più facilmente bucket specifici, inserisci i criteri di ricerca nella casella di ricerca sopra la tabella. Puoi anche ordinare la tabella scegliendo un'intestazione di colonna.

6. Al termine della selezione dei bucket, scegliete Aggiungi o Rimuovi, a seconda dell'opzione scelta nel passaggio precedente.

 Tip

Puoi anche escludere o includere singoli bucket S3 su case-by-case base individuale mentre rivedi i dettagli dei bucket sulla console. Per fare ciò, scegli il bucket nella pagina dei bucket S3. Quindi, nel pannello dei dettagli, modifica l'impostazione Escludi dal rilevamento automatico per il bucket.

API

Per escludere o includere successivamente un bucket S3 a livello di codice, utilizza l'API Amazon Macie per aggiornare l'ambito di classificazione del tuo account. L'ambito di classificazione specifica i bucket che non vuoi che Macie analizzi quando esegue il rilevamento automatico di dati sensibili. Definisce un elenco di esclusione dei bucket per il rilevamento automatico.

Quando si aggiorna l'ambito di classificazione, si specifica se aggiungere o rimuovere singoli bucket dall'elenco di esclusione o sovrascrivere l'elenco corrente con un nuovo elenco. Pertanto, è una buona idea iniziare recuperando e rivedendo l'elenco corrente. Per recuperare l'elenco, usa l'operazione. [GetClassificationScope](#) Se stai usando il AWS Command Line Interface (AWS CLI), esegui il [get-classification-scope](#) comando per recuperare l'elenco.

Per recuperare o aggiornare l'ambito di classificazione, devi specificare il relativo identificatore univoco (). È possibile ottenere questo identificatore utilizzando l'operazione. [GetAutomatedDiscoveryConfiguration](#) Questa operazione recupera le impostazioni di configurazione correnti per l'individuazione automatica dei dati sensibili, incluso l'identificatore univoco per l'ambito di classificazione dell'account nell'attuale. Regione AWS Se utilizzi il AWS CLI, esegui il [get-automated-discovery-configuration](#) comando per recuperare queste informazioni.

Quando sei pronto per aggiornare l'ambito di classificazione, utilizza l'[UpdateClassificationScope](#) operazione o, se stai utilizzando il AWS CLI, esegui il [update-classification-scope](#) comando. Nella tua richiesta, utilizza i parametri supportati per escludere o includere un bucket S3 nelle analisi successive:

- Per escludere uno o più bucket, specifica il nome di ogni bucket per il parametro. `bucketNames` Per il parametro `operation`, specifica `ADD`.
- Per includere uno o più bucket precedentemente esclusi, specificate il nome di ogni bucket per il parametro. `bucketNames` Per il parametro `operation`, specifica `REMOVE`.

- Per sovrascrivere l'elenco corrente con un nuovo elenco di bucket da escludere, REPLACE specificate il parametro. operation Per il bucketNames parametro, specificate il nome di ogni bucket da escludere.

Ogni valore del bucketNames parametro deve essere il nome completo di un bucket generico esistente nella regione corrente. I valori sono sensibili alle maiuscole. Se la richiesta ha esito positivo, Macie aggiorna l'ambito di classificazione e restituisce una risposta vuota.

Gli esempi seguenti mostrano come utilizzare per AWS CLI aggiornare l'ambito di classificazione di un account. La prima serie di esempi esclude due bucket S3 (*amzn-s3-demo-bucket1* e *amzn-s3-demo-bucket2*) dalle analisi successive. Aggiunge i bucket all'elenco dei bucket da escludere.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws macie2 update-classification-scope \
--id 117aff7ed76b59a59c3224ebdexample \
--s3 '{"excludes":{"bucketNames":["amzn-s3-demo-bucket1","amzn-s3-demo-bucket2"],"operation": "ADD"}}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 update-classification-scope ^
--id 117aff7ed76b59a59c3224ebdexample ^
--s3={"excludes":{"bucketNames":["amzn-s3-demo-bucket1","\ "amzn-s3-demo-bucket2"],"operation":"ADD"}}
```

La serie di esempi successiva include più avanti i bucket (e) nelle analisi successive. *amzn-s3-demo-bucket1* *amzn-s3-demo-bucket2* Rimuove i bucket dall'elenco dei bucket da escludere. Per Linux, macOS o Unix:

```
$ aws macie2 update-classification-scope \
--id 117aff7ed76b59a59c3224ebdexample \
--s3 '{"excludes":{"bucketNames":["amzn-s3-demo-bucket1","amzn-s3-demo-bucket2"],"operation": "REMOVE"}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 update-classification-scope ^  
--id 117aff7ed76b59a59c3224ebdexample ^  
--s3={"excludes":{"bucketNames":["amzn-s3-demo-bucket1","amzn-s3-demo-  
bucket2"],"operation":"REMOVE"}}
```

Gli esempi seguenti sovrascrivono e sostituiscono l'elenco corrente con un nuovo elenco di bucket S3 da escludere. Il nuovo elenco specifica tre bucket da escludere:, e. *amzn-s3-demo-bucket amzn-s3-demo-bucket2 amzn-s3-demo-bucket3* Per Linux, macOS o Unix:

```
$ aws macie2 update-classification-scope \  
--id 117aff7ed76b59a59c3224ebdexample \  
--s3 '{"excludes":{"bucketNames":["amzn-s3-demo-bucket","amzn-s3-demo-  
bucket2","amzn-s3-demo-bucket3"],"operation": "REPLACE"}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 update-classification-scope ^  
--id 117aff7ed76b59a59c3224ebdexample ^  
--s3={"excludes":{"bucketNames":["amzn-s3-demo-bucket","amzn-s3-demo-  
bucket2","amzn-s3-demo-bucket3"],"operation":"REPLACE"}}
```

Aggiungere o rimuovere identificatori di dati gestiti dal rilevamento automatico di dati sensibili

Un identificatore di dati gestiti è un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili, ad esempio numeri di carte di credito, chiavi di accesso AWS segrete o numeri di passaporto per un determinato paese o area geografica. Per impostazione predefinita, Amazon Macie analizza gli oggetti S3 utilizzando il set di identificatori di dati gestiti che consigliamo per il rilevamento automatico di dati sensibili. Per esaminare un elenco di questi identificatori, consulta. [Impostazioni predefinite per l'individuazione automatica dei dati sensibili](#)

Puoi personalizzare le analisi per concentrarti su tipi specifici di dati sensibili:

- Aggiungi identificatori di dati gestiti per i tipi di dati sensibili che desideri che Macie rilevi e riporti e
- Rimuovi gli identificatori di dati gestiti per i tipi di dati sensibili che non vuoi che Macie rilevi e segnali.

Per un elenco completo di tutti gli identificatori di dati gestiti attualmente forniti da Macie e i dettagli relativi a ciascuno di essi, consulta. [Utilizzo di identificatori di dati gestiti](#)

Se rimuovi un identificatore di dati gestito, la modifica non influirà sulle statistiche e sui dettagli esistenti sull'individuazione dei dati sensibili per i bucket S3. Ad esempio, se rimuovi l'identificatore di dati gestito per le chiavi di accesso AWS segrete e Macie aveva precedentemente rilevato quei dati in un bucket, Macie continua a segnalare tali rilevamenti. Tuttavia, invece di rimuovere l'identificatore, che influisce sulle analisi successive di tutti i bucket, valuta la possibilità di escluderne i rilevamenti dai punteggi di sensibilità solo per determinati bucket. Per ulteriori informazioni, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Per aggiungere o rimuovere identificatori di dati gestiti dal rilevamento automatico di dati sensibili

Puoi aggiungere o rimuovere identificatori di dati gestiti utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per aggiungere o rimuovere un identificatore di dati gestito utilizzando la console Amazon Macie.

Per aggiungere o rimuovere un identificatore di dati gestito

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri aggiungere o rimuovere un identificatore di dati gestito dalle analisi.
3. Nel riquadro di navigazione, in Impostazioni, scegli Rilevamento automatico dei dati sensibili.

Viene visualizzata la pagina di individuazione automatica dei dati sensibili che mostra le impostazioni correnti. In quella pagina, la sezione Identificatori di dati gestiti mostra le impostazioni correnti, organizzate in due schede:

- Aggiunto all'impostazione predefinita: questa scheda elenca gli identificatori di dati gestiti che hai aggiunto. Macie utilizza questi identificatori in aggiunta a quelli presenti nel set predefinito e che non hai rimosso.
 - Rimosso dall'impostazione predefinita: questa scheda elenca gli identificatori di dati gestiti che hai rimosso. Macie non utilizza questi identificatori.
4. Nella sezione Identificatori di dati gestiti, scegli Modifica.
 5. Effettua una delle seguenti operazioni:
 - Per aggiungere uno o più identificatori di dati gestiti, scegli la scheda Aggiunto ai valori predefiniti. Quindi, nella tabella, seleziona la casella di controllo per ogni identificatore di

dati gestiti da aggiungere. Se è già selezionata una casella di controllo, l'identificatore è già stato aggiunto.

- Per rimuovere uno o più identificatori di dati gestiti, scegli la scheda Rimosso da predefinito. Quindi, nella tabella, seleziona la casella di controllo per ogni identificatore di dati gestiti da rimuovere. Se è già selezionata una casella di controllo, l'identificatore è già stato rimosso.

In ogni scheda, la tabella mostra un elenco di tutti gli identificatori di dati gestiti attualmente forniti da Macie. Nella tabella, la prima colonna specifica l'ID di ogni identificatore di dati gestito. L'ID descrive il tipo di dati sensibili che un identificatore è progettato per rilevare, ad esempio USA_PASSPORT_NUMBER per i numeri di passaporto statunitensi. Per trovare più facilmente identificatori di dati gestiti specifici, inserisci i criteri di ricerca nella casella di ricerca sopra la tabella. Puoi anche ordinare la tabella scegliendo un'intestazione di colonna.

6. Al termine, scegli Salva.

API

Per aggiungere o rimuovere un identificatore di dati gestito a livello di codice, utilizza l'API Amazon Macie per aggiornare il modello di ispezione della sensibilità per il tuo account. Il modello memorizza le impostazioni che specificano quali identificatori di dati gestiti utilizzare (includere) oltre a quelli del set predefinito. Specificano inoltre gli identificatori di dati gestiti da non utilizzare (escludere). Le impostazioni specificano anche eventuali identificatori di dati personalizzati e consentono gli elenchi che desideri che Macie utilizzi.

Quando aggiorni il modello, sovrascrivi le impostazioni correnti. Pertanto, è una buona idea iniziare recuperando le impostazioni correnti e determinando quali conservare. Per recuperare le impostazioni correnti, utilizza l'operazione. [GetSensitivityInspectionTemplate](#) Se stai usando AWS Command Line Interface (AWS CLI), esegui il [get-sensitivity-inspection-template](#) comando per recuperare le impostazioni.

Per recuperare o aggiornare il modello, devi specificare il suo identificatore univoco (`id`). È possibile ottenere questo identificatore utilizzando l'operazione. [GetAutomatedDiscoveryConfiguration](#) Questa operazione recupera le impostazioni di configurazione correnti per l'individuazione automatica dei dati sensibili, incluso l'identificatore univoco per il modello di controllo della sensibilità per l'account nell'attuale versione. Regione AWS Se utilizzi il AWS CLI, esegui il [get-automated-discovery-configuration](#) comando per recuperare queste informazioni.

Quando sei pronto per aggiornare il modello, usa

l'[UpdateSensitivityInspectionTemplate](#) operazione o, se stai usando il AWS CLI, esegui il [update-sensitivity-inspection-template](#) comando. Nella tua richiesta, utilizza i parametri appropriati per aggiungere o rimuovere uno o più identificatori di dati gestiti dalle analisi successive:

- Per iniziare a utilizzare un identificatore di dati gestito, specifica il relativo ID per il `managedDataIdentifierIds` parametro del parametro. `includes`
- Per interrompere l'utilizzo di un identificatore di dati gestito, specificate il relativo ID per il `managedDataIdentifierIds` parametro del `excludes` parametro.
- Per ripristinare le impostazioni predefinite, non specificarne nessuna IDs per i `excludes` parametri `includes` and. Macie inizia quindi a utilizzare solo gli identificatori di dati gestiti inclusi nel set predefinito.

Oltre ai parametri per gli identificatori di dati gestiti, utilizza i `includes` parametri appropriati per specificare eventuali identificatori di dati personalizzati (`customDataIdentifierIds`) e consentire gli elenchi (`allowListIds`) che desideri vengano utilizzati da Macie. Specificate anche la regione a cui si riferisce la richiesta. Se la richiesta ha esito positivo, Macie aggiorna il modello e restituisce una risposta vuota.

Gli esempi seguenti mostrano come utilizzare il per AWS CLI aggiornare il modello di ispezione di sensibilità per un account. Gli esempi aggiungono un identificatore di dati gestito e ne rimuovono un altro dalle analisi successive. Inoltre mantengono le impostazioni correnti che specificano due identificatori di dati personalizzati da utilizzare.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 update-sensitivity-inspection-template \  
--id fd7b6d71c8006fcd6391e6eedexample \  
--excludes '{"managedDataIdentifierIds":["UK_ELECTORAL_ROLL_NUMBER"]}' \  
--includes '{"managedDataIdentifierIds":  
["STRIPE_CREDENTIALS"],"customDataIdentifierIds":  
["3293a69d-4a1e-4a07-8715-208ddexample","6fad0fb5-3e82-4270-bede-469f2example"]}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws macie2 update-sensitivity-inspection-template ^
```

```
--id fd7b6d71c8006fcd6391e6eedexample ^  
--excludes={"managedDataIdentifierIds":["UK_ELECTORAL_ROLL_NUMBER"]} ^  
--includes={"managedDataIdentifierIds":["STRIPE_CREDENTIALS"],  
"customDataIdentifierIds":["3293a69d-4a1e-4a07-8715-208ddexample",  
"6fad0fb5-3e82-4270-bede-469f2example"]}
```

Dove:

- *fd7b6d71c8006fcd6391e6eedexample* è l'identificatore univoco per il modello di controllo della sensibilità da aggiornare.
- *UK_ELECTORAL_ROLL_NUMBER* è l'ID dell'identificatore di dati gestito da smettere di usare (escludere).
- *STRIPE_CREDENTIALS* è l'ID dell'identificatore di dati gestito da iniziare a utilizzare (include).
- *3293a69d-4a1e-4a07-8715-208ddexample* e *6fad0fb5-3e82-4270-bede-469f2example* sono gli identificatori univoci da utilizzare per gli identificatori di dati personalizzati.

Aggiungere o rimuovere identificatori di dati personalizzati dal rilevamento automatico di dati sensibili

Un identificatore di dati personalizzato è un insieme di criteri definiti per rilevare dati sensibili. I criteri sono costituiti da un'espressione regolare (regex) che definisce uno schema di testo da abbinare e, facoltativamente, sequenze di caratteri e una regola di prossimità che perfeziona i risultati. Per ulteriori informazioni, consulta [Creazione di identificatori di dati personalizzati](#).

Per impostazione predefinita, Amazon Macie non utilizza identificatori di dati personalizzati quando esegue il rilevamento automatico di dati sensibili. Se desideri che Macie utilizzi identificatori di dati personalizzati specifici, puoi aggiungerli alle analisi successive. Macie utilizza quindi gli identificatori di dati personalizzati in aggiunta a tutti gli identificatori di dati gestiti per cui Macie configuri.

Se aggiungi un identificatore di dati personalizzato, puoi rimuoverlo in un secondo momento. La modifica non influisce sulle statistiche e sui dettagli esistenti relativi all'individuazione dei dati sensibili per i bucket S3. Vale a dire, se rimuovi un identificatore di dati personalizzato che in precedenza produceva rilevamenti per un bucket, Macie continua a segnalare tali rilevamenti. Tuttavia, invece di rimuovere l'identificatore, che influisce sulle analisi successive di tutti i bucket, valuta la possibilità di escluderne i rilevamenti dai punteggi di sensibilità solo per determinati bucket. Per ulteriori informazioni, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Per aggiungere o rimuovere identificatori di dati personalizzati dal rilevamento automatico di dati sensibili

Puoi aggiungere o rimuovere identificatori di dati personalizzati utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per aggiungere o rimuovere un identificatore di dati personalizzato utilizzando la console Amazon Macie.

Per aggiungere o rimuovere un identificatore di dati personalizzato

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri aggiungere o rimuovere un identificatore di dati personalizzato dalle analisi.
3. Nel riquadro di navigazione, in Impostazioni, scegli Rilevamento automatico dei dati sensibili.

Viene visualizzata la pagina di individuazione automatica dei dati sensibili che mostra le impostazioni correnti. In quella pagina, la sezione Identificatori di dati personalizzati elenca gli identificatori di dati personalizzati che hai già aggiunto oppure indica che non hai aggiunto alcun identificatore di dati personalizzato.

4. Nella sezione Identificatori di dati personalizzati, scegli Modifica.
5. Effettua una delle seguenti operazioni:
 - Per aggiungere uno o più identificatori di dati personalizzati, seleziona la casella di controllo per ogni identificatore di dati personalizzato da aggiungere. Se è già selezionata una casella di controllo, l'identificatore è già stato aggiunto.
 - Per rimuovere uno o più identificatori di dati personalizzati, deseleziona la casella di controllo relativa a ciascun identificatore di dati personalizzato da rimuovere. Se una casella di controllo è già deselezionata, Macie attualmente non utilizza quell'identificatore.

Tip

Per rivedere o testare le impostazioni per un identificatore di dati personalizzato prima di aggiungerlo o rimuoverlo, scegli l'icona del link



) accanto al nome dell'identificatore. Macie apre una pagina che mostra le impostazioni dell'identificatore. Per testare l'identificatore anche con dati di esempio, inserisci fino

a 1.000 caratteri di testo nella casella Dati di esempio di quella pagina. Quindi scegli Test. Macie valuta i dati del campione e riporta il numero di corrispondenze.

6. Al termine, scegli Salva.

API

Per aggiungere o rimuovere un identificatore di dati personalizzato a livello di codice, utilizza l'API Amazon Macie per aggiornare il modello di ispezione della sensibilità per il tuo account. Il modello memorizza le impostazioni che specificano gli identificatori di dati personalizzati che desideri che Macie utilizzi per l'individuazione automatica di dati sensibili. Le impostazioni specificano anche quali identificatori di dati gestiti e consentono l'utilizzo degli elenchi.

Quando si aggiorna il modello, si sovrascrivono le impostazioni correnti. Pertanto, è una buona idea iniziare recuperando le impostazioni correnti e determinando quali conservare. Per recuperare le impostazioni correnti, utilizzate l'operazione. [GetSensitivityInspectionTemplate](#) Se stai usando AWS Command Line Interface (AWS CLI), esegui il [get-sensitivity-inspection-template](#) comando per recuperare le impostazioni.

Per recuperare o aggiornare il modello, devi specificare il suo identificatore univoco (). id È possibile ottenere questo identificatore utilizzando l'operazione. [GetAutomatedDiscoveryConfiguration](#) Questa operazione recupera le impostazioni di configurazione correnti per l'individuazione automatica dei dati sensibili, incluso l'identificatore univoco per il modello di controllo della sensibilità per l'account nell'attuale versione. Regione AWS Se utilizzi il AWS CLI, esegui il [get-automated-discovery-configuration](#) comando per recuperare queste informazioni.

Quando sei pronto per aggiornare il modello, usa l'[UpdateSensitivityInspectionTemplate](#) operazione o, se stai usando il AWS CLI, esegui il [update-sensitivity-inspection-template](#) comando. Nella tua richiesta, utilizza il `customDataIdentifierIds` parametro per aggiungere o rimuovere uno o più identificatori di dati personalizzati dalle analisi successive:

- Per iniziare a utilizzare un identificatore di dati personalizzato, specifica il relativo identificatore univoco per il parametro.
- Per smettere di utilizzare un identificatore di dati personalizzato, omettete il relativo identificatore univoco dal parametro.

Usa parametri aggiuntivi per specificare quali identificatori di dati gestiti e quali elenchi di dati consentiti vuoi che Macie utilizzi. Specificate anche la regione a cui si riferisce la richiesta. Se la richiesta ha esito positivo, Macie aggiorna il modello e restituisce una risposta vuota.

Gli esempi seguenti mostrano come utilizzare il per AWS CLI aggiornare il modello di ispezione di sensibilità per un account. Gli esempi aggiungono due identificatori di dati personalizzati alle analisi successive. Inoltre mantengono le impostazioni correnti che specificano gli identificatori di dati gestiti e gli elenchi consentiti da utilizzare: utilizzano il set predefinito di identificatori di dati gestiti e un elenco consentito.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws macie2 update-sensitivity-inspection-template \
--id fd7b6d71c8006fcd6391e6eedexample \
--includes '{"allowListIds":["nkr81bmtu2542yyexample"],"customDataIdentifierIds":
["3293a69d-4a1e-4a07-8715-208ddexample","6fad0fb5-3e82-4270-bede-469f2example"]}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 update-sensitivity-inspection-template ^
--id fd7b6d71c8006fcd6391e6eedexample ^
--includes={"allowListIds":["nkr81bmtu2542yyexample"],"customDataIdentifierIds
":["3293a69d-4a1e-4a07-8715-208ddexample","6fad0fb5-3e82-4270-
bede-469f2example"]}
```

Dove:

- *fd7b6d71c8006fcd6391e6eedexample* è l'identificatore univoco per il modello di controllo della sensibilità da aggiornare.
- *nkr81bmtu2542yyexample* è l'identificatore univoco dell'elenco consentito da utilizzare.
- *3293a69d-4a1e-4a07-8715-208ddexample* e *6fad0fb5-3e82-4270-bede-469f2example* sono gli identificatori univoci da utilizzare per gli identificatori di dati personalizzati.

Aggiungere o rimuovere elenchi di dati consentiti dal rilevamento automatico di dati sensibili

In Amazon Macie, un elenco consentito definisce un testo specifico o un pattern di testo che vuoi che Macie ignori quando ispeziona gli oggetti S3 alla ricerca di dati sensibili. Se il testo corrisponde a una voce o a uno schema in un elenco consentito, Macie non riporta il testo. Questo è il caso anche se il testo corrisponde ai criteri di un identificatore di dati gestito o personalizzato. Per ulteriori informazioni, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).

Per impostazione predefinita, Macie non utilizza gli elenchi consentiti quando esegue il rilevamento automatico dei dati sensibili. Se desideri che Macie utilizzi elenchi di autorizzazioni specifici, puoi aggiungerli alle analisi successive. Se aggiungi un elenco consentito, puoi rimuoverlo in un secondo momento.

Per aggiungere o rimuovere elenchi consentiti dal rilevamento automatico dei dati sensibili

Puoi aggiungere o rimuovere elenchi consentiti utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per aggiungere o rimuovere un elenco di prodotti consentiti utilizzando la console Amazon Macie.

Per aggiungere o rimuovere un elenco di elementi consentiti

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Region AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri aggiungere o rimuovere un elenco consentito dalle analisi.
3. Nel riquadro di navigazione, in Impostazioni, scegli Rilevamento automatico dei dati sensibili.

Viene visualizzata la pagina di individuazione automatica dei dati sensibili che mostra le impostazioni correnti. In quella pagina, la sezione Consenti elenchi consentiti specifica gli elenchi consentiti che hai già aggiunto oppure indica che non hai aggiunto alcun elenco consentito.

4. Nella sezione Consenti elenchi, scegli Modifica.
5. Effettua una delle seguenti operazioni:
 - Per aggiungere uno o più elenchi consentiti, seleziona la casella di controllo per ogni elenco consentito da aggiungere. Se è già selezionata una casella di controllo, l'elenco è già stato aggiunto.

- Per rimuovere uno o più elenchi consentiti, deseleziona la casella di controllo relativa a ciascun elenco consentito da rimuovere. Se una casella di controllo è già deselezionata, Macie attualmente non utilizza quell'elenco.

Tip

Per rivedere le impostazioni di un elenco consentito prima di aggiungerlo o rimuoverlo, scegli l'icona del link



) accanto al nome dell'elenco. Macie apre una pagina che mostra le impostazioni dell'elenco. Se l'elenco specifica un'espressione regolare (regex), puoi anche usare questa pagina per testare l'espressione regolare con dati di esempio. A tale scopo, inserisci fino a 1.000 caratteri di testo nella casella Dati di esempio, quindi scegli Test. Macie valuta i dati di esempio e riporta il numero di corrispondenze.

6. Al termine, scegli Salva.

API

Per aggiungere o rimuovere un elenco di dati consentiti a livello di programmazione, utilizza l'API Amazon Macie per aggiornare il modello di ispezione della sensibilità per il tuo account. Il modello memorizza le impostazioni che specificano quali elenchi di autorizzazioni desideri che Macie utilizzi per l'individuazione automatica di dati sensibili. Le impostazioni specificano anche quali identificatori di dati gestiti e identificatori di dati personalizzati utilizzare.

Quando si aggiorna il modello, si sovrascrivono le impostazioni correnti. Pertanto, è una buona idea iniziare recuperando le impostazioni correnti e determinando quali conservare. Per recuperare le impostazioni correnti, utilizzate l'operazione. [GetSensitivityInspectionTemplate](#) Se stai usando AWS Command Line Interface (AWS CLI), esegui il [get-sensitivity-inspection-template](#) comando per recuperare le impostazioni.

Per recuperare o aggiornare il modello, devi specificare il suo identificatore univoco (). id È possibile ottenere questo identificatore utilizzando l'operazione. [GetAutomatedDiscoveryConfiguration](#) Questa operazione recupera le impostazioni di configurazione correnti per l'individuazione automatica dei dati sensibili, incluso l'identificatore univoco per il modello di controllo della sensibilità per l'account nell'attuale versione. Regione

AWS Se utilizzi il AWS CLI, esegui il [get-automated-discovery-configuration](#) comando per recuperare queste informazioni.

Quando sei pronto per aggiornare il modello, usa l'[UpdateSensitivityInspectionTemplate](#) operazione o, se stai usando il AWS CLI, esegui il [update-sensitivity-inspection-template](#) comando. Nella tua richiesta, usa il `allowListIds` parametro per aggiungere o rimuovere uno o più elenchi di autorizzazioni dalle analisi successive:

- Per iniziare a utilizzare un elenco di opzioni consentite, specifica il relativo identificatore univoco per il parametro.
- Per interrompere l'utilizzo di un elenco consentito, omettete il relativo identificatore univoco dal parametro.

Usa parametri aggiuntivi per specificare quali identificatori di dati gestiti e identificatori di dati personalizzati vuoi che Macie utilizzi. Specifica anche la regione a cui si riferisce la richiesta. Se la richiesta ha esito positivo, Macie aggiorna il modello e restituisce una risposta vuota.

Gli esempi seguenti mostrano come utilizzare il per AWS CLI aggiornare il modello di ispezione di sensibilità per un account. Gli esempi aggiungono un elenco di autorizzazioni alle analisi successive. Mantengono inoltre le impostazioni correnti che specificano quali identificatori di dati gestiti e identificatori di dati personalizzati utilizzare: utilizzano il set predefinito di identificatori di dati gestiti e due identificatori di dati personalizzati.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 update-sensitivity-inspection-template \
--id fd7b6d71c8006fcd6391e6eedexample \
--includes '{"allowListIds":["nkr81bmtu2542yyexample"],"customDataIdentifierIds":
["3293a69d-4a1e-4a07-8715-208ddexample","6fad0fb5-3e82-4270-bede-469f2example"]}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws macie2 update-sensitivity-inspection-template ^
--id fd7b6d71c8006fcd6391e6eedexample ^
--includes={"allowListIds":["nkr81bmtu2542yyexample"],"customDataIdentifierIds
":["3293a69d-4a1e-4a07-8715-208ddexample"],"6fad0fb5-3e82-4270-
bede-469f2example"}
```

Dove:

- *fd7b6d71c8006fcd6391e6eedexample* è l'identificatore univoco per il modello di controllo della sensibilità da aggiornare.
- *nkr81bmtu2542yyexample* è l'identificatore univoco dell'elenco consentito da utilizzare.
- *3293a69d-4a1e-4a07-8715-208ddexample* e *6fad0fb5-3e82-4270-bede-469f2example* sono gli identificatori univoci da utilizzare per gli identificatori di dati personalizzati.

Disabilitazione del rilevamento automatico di dati sensibili

Puoi disabilitare il rilevamento automatico dei dati sensibili per un account o un'organizzazione in qualsiasi momento. In tal caso, Amazon Macie interrompe l'esecuzione di tutte le attività di rilevamento automatizzato per l'account o l'organizzazione prima dell'inizio di un successivo ciclo di valutazione e analisi, in genere entro 48 ore. Gli effetti aggiuntivi variano:

- Se sei un amministratore di Macie e lo disattivi per un singolo account della tua organizzazione, tu e l'account potete continuare ad accedere a tutti i dati statistici, i dati di inventario e altre informazioni che Macie ha prodotto e fornito direttamente durante il rilevamento automatico dell'account. Puoi abilitare nuovamente l'individuazione automatica per l'account. Macie riprende quindi tutte le attività di rilevamento automatico dell'account.
- Se sei un amministratore di Macie e lo disattivi per la tua organizzazione, tu e gli account dell'organizzazione perderete l'accesso a tutti i dati statistici, ai dati di inventario e ad altre informazioni che Macie ha prodotto e fornito direttamente durante l'esecuzione del rilevamento automatico per la tua organizzazione. Ad esempio, l'inventario dei bucket S3 non include più visualizzazioni di sensibilità o analisi statistiche. Successivamente puoi abilitare nuovamente il rilevamento automatico per la tua organizzazione. Macie riprende quindi tutte le attività di individuazione automatica degli account dell'organizzazione. Se lo riattivi entro 30 giorni, tu e gli account riavrete accesso ai dati e alle informazioni che Macie aveva precedentemente prodotto e fornito direttamente durante l'esecuzione del rilevamento automatico. Se non lo riattivi entro 30 giorni, Macie elimina definitivamente questi dati e informazioni.
- Se lo disabiliti per il tuo account Macie autonomo, perdi l'accesso a tutti i dati statistici, ai dati di inventario e ad altre informazioni che Macie ha prodotto e fornito direttamente durante il rilevamento automatico del tuo account. Se non lo riattivi entro 30 giorni, Macie elimina definitivamente questi dati e informazioni.

Puoi continuare ad accedere ai dati sensibili raccolti da Macie durante l'individuazione automatica dei dati sensibili per l'account o l'organizzazione. Macie archivia i risultati per 90 giorni. Macie conserva anche le impostazioni di configurazione per il rilevamento automatico. Inoltre, i dati che hai archiviato o pubblicato su altri Servizi AWS rimangono intatti e non sono interessati, come i risultati del rilevamento di dati sensibili in Amazon S3 e la ricerca di eventi in Amazon EventBridge.

Per disabilitare il rilevamento automatico di dati sensibili

Se sei l'amministratore Macie di un'organizzazione o disponi di un account Macie autonomo, puoi disabilitare il rilevamento automatico dei dati sensibili utilizzando la console Amazon Macie o l'API Amazon Macie. Se disponi di un account membro in un'organizzazione, collabora con l'amministratore di Macie per disabilitare il rilevamento automatico del tuo account. Solo l'amministratore di Macie può disabilitare il rilevamento automatico per il tuo account.

Console

Segui questi passaggi per disabilitare il rilevamento automatico dei dati sensibili utilizzando la console Amazon Macie.

Per disabilitare il rilevamento automatico di dati sensibili

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri disabilitare il rilevamento automatico dei dati sensibili.
3. Nel riquadro di navigazione, in Impostazioni, scegli Rilevamento automatico dei dati sensibili.
4. Se sei l'amministratore Macie di un'organizzazione, scegli un'opzione nella sezione Stato per specificare gli account per cui disabilitare il rilevamento automatico dei dati sensibili per:
 - Per disabilitarlo solo per determinati account membro, scegli Gestisci account. Quindi, nella tabella della pagina Account, seleziona la casella di controllo relativa a ciascun account per cui disabilitarlo. Al termine, scegli Disattiva l'individuazione automatica dei dati sensibili nel menu Azioni.
 - Per disabilitarlo solo per il tuo account amministratore Macie, scegli Disabilita. Nella finestra di dialogo che appare, scegli Il mio account, quindi scegli Disabilita.
 - Per disabilitarlo per tutti gli account della tua organizzazione e dell'organizzazione in generale, scegli Disabilita. Nella finestra di dialogo visualizzata, scegli La mia organizzazione, quindi scegli Disabilita.
5. Se hai un account Macie indipendente, scegli Disabilita nella sezione Stato.

Se usi Macie in più regioni e desideri disabilitare il rilevamento automatico dei dati sensibili in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Con l'API Amazon Macie, puoi disabilitare il rilevamento automatico di dati sensibili in due modi. La modalità di disattivazione dipende in parte dal tipo di account di cui disponi. Se sei l'amministratore Macie di un'organizzazione, dipende anche dal fatto che desideri disabilitare il rilevamento automatico solo per determinati account membri o per l'intera organizzazione. Se lo disabiliti per la tua organizzazione, lo disattivi per tutti gli account che attualmente fanno parte della tua organizzazione. Se successivamente si aggiungono altri account all'organizzazione, il rilevamento automatico viene disabilitato anche per tali account.

Per disabilitare l'individuazione automatica dei dati sensibili per un'organizzazione o un account Macie autonomo, usa l'[UpdateAutomatedDiscoveryConfiguration](#) operazione. Oppure, se stai usando il AWS Command Line Interface (AWS CLI), esegui il [update-automated-discovery-configuration](#) comando. Nella richiesta, DISABLED specificate il status parametro.

Per disabilitare l'individuazione automatica dei dati sensibili solo per determinati account membri di un'organizzazione, utilizza l'[BatchUpdateAutomatedDiscoveryAccounts](#) operazione. In alternativa, se utilizzi il AWS CLI, esegui il comando [batch-update-automated-discovery-accounts](#). Nella richiesta, utilizza il `accountId` parametro per specificare l'ID dell'account per il quale desideri disabilitare il rilevamento automatico. Per il parametro `status`, specifica DISABLED. Per disabilitare l'individuazione automatica di un account, Macie deve essere attualmente abilitato per l'account.

Gli esempi seguenti mostrano come utilizzare l'opzione per AWS CLI disabilitare l'individuazione automatica dei dati sensibili per uno o più account di un'organizzazione. Questo primo esempio disabilita l'individuazione automatica per un'organizzazione. Disattiva il rilevamento automatico per l'account amministratore Macie e per tutti gli account dei membri dell'organizzazione.

```
$ aws macie2 update-automated-discovery-configuration --status DISABLED --region us-east-1
```

us-east-1 Dov'è la regione in cui disabilitare il rilevamento automatico dei dati sensibili per l'organizzazione, la regione Stati Uniti orientali (Virginia settentrionale). Se la richiesta ha esito positivo, Macie disabilita il rilevamento automatico per l'organizzazione e restituisce una risposta vuota.

Questi esempi successivi disabilitano l'individuazione automatica dei dati sensibili per due account membri di un'organizzazione. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws macie2 batch-update-automated-discovery-accounts \  
--region us-east-1 \  
--accounts '[{"accountId":"123456789012", "status":"DISABLED"},  
{ "accountId":"111122223333", "status":"DISABLED"}]'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 batch-update-automated-discovery-accounts ^  
--region us-east-1 ^  
--accounts=[{"accountId\" : \"123456789012\", \"status\" : \"DISABLED\"}, { \"accountId\" :  
\"111122223333\", \"status\" : \"DISABLED\"}]
```

Dove:

- **us-east-1** è la regione in cui disattivare l'individuazione automatica dei dati sensibili per gli account specificati, la regione Stati Uniti orientali (Virginia settentrionale).
- **123456789012** e **111122223333** sono gli account IDs per i quali disabilitare l'individuazione automatica dei dati sensibili.

Se la richiesta ha esito positivo per tutti gli account specificati, Macie restituisce un array vuoto `errors`. Se la richiesta fallisce per alcuni account, l'array specifica l'errore che si è verificato per ogni account interessato. Per esempio:

```
"errors": [  
  {  
    "accountId": "123456789012",  
    "errorCode": "ACCOUNT_PAUSED"  
  }  
]
```

Nella risposta precedente, la richiesta non è riuscita per l'account specificato (123456789012) perché Macie è attualmente sospeso per l'account.

Se la richiesta non riesce per tutti gli account, riceverai un messaggio che descrive l'errore che si è verificato. Per esempio:

```
An error occurred (ConflictException) when calling the
BatchUpdateAutomatedDiscoveryAccounts operation: Cannot modify account states
while auto-enable is set to ALL.
```

Nella risposta precedente, la richiesta non è riuscita perché l'impostazione di abilitazione dei membri per l'organizzazione è attualmente configurata per consentire l'individuazione automatica dei dati sensibili per tutti gli account (). ALL Per risolvere l'errore, l'amministratore di Macie deve prima modificare questa impostazione in o. NONE NEW Per ulteriori informazioni su questa impostazione, consulta [Abilitare l'individuazione automatica dei dati sensibili](#).

Revisione dei risultati automatizzati del rilevamento di dati sensibili

Se il rilevamento automatico dei dati sensibili è abilitato, Amazon Macie genera e mantiene automaticamente dati di inventario aggiuntivi, statistiche e altre informazioni sui bucket generici Amazon Simple Storage Service (Amazon S3) per uso generico per il tuo account. Se sei l'amministratore Macie di un'organizzazione, per impostazione predefinita sono inclusi i bucket S3 di proprietà dei tuoi account membro.

Le informazioni aggiuntive acquisiscono i risultati delle attività automatizzate di rilevamento di dati sensibili che Macie ha svolto finora. Inoltre, integra altre informazioni fornite da Macie sui tuoi dati Amazon S3, come l'accesso pubblico e le impostazioni di crittografia per i singoli bucket S3. Oltre ai metadati e alle statistiche, Macie registra i dati sensibili che trova e le analisi che esegue: rilevamenti di dati sensibili e risultati della scoperta di dati sensibili.

Man mano che l'individuazione automatica dei dati sensibili progredisce ogni giorno, le seguenti funzionalità e dati possono aiutarti a rivedere e valutare i risultati:

- [Dashboard di riepilogo](#): fornisce statistiche aggregate per il tuo patrimonio di dati Amazon S3. Le statistiche includono dati per metriche chiave come il numero totale di bucket in cui Macie ha trovato dati sensibili e quanti di questi bucket sono accessibili al pubblico. Segnalano inoltre problemi che influiscono sulla copertura dei dati di Amazon S3.
- [Mappa termica dei bucket S3](#): fornisce una rappresentazione visiva e interattiva della sensibilità dei dati nell'insieme dei dati, raggruppati per. Account AWS Per ogni account, la mappa include statistiche di sensibilità aggregate e utilizza colori per indicare il punteggio di sensibilità corrente

per ogni bucket di proprietà dell'account. La mappa utilizza anche simboli per aiutarti a identificare i bucket accessibili pubblicamente, che non possono essere analizzati da Macie e altro ancora.

- [Tabella dei bucket S3](#): fornisce informazioni di riepilogo per ogni bucket S3 dell'inventario. Per ogni bucket, la tabella include dati come il punteggio di sensibilità corrente del bucket, il numero di oggetti che Macie può analizzare nel bucket e se sono stati configurati processi di rilevamento di dati sensibili per analizzare periodicamente gli oggetti nel bucket. È possibile esportare i dati dalla tabella in un file con valori separati da virgole (CSV).
- [Dettagli del bucket S3](#): fornisce statistiche e informazioni dettagliate su un bucket S3. I dettagli includono un elenco di oggetti che Macie ha analizzato nel bucket e un'analisi dettagliata dei tipi e del numero di occorrenze di dati sensibili che Macie ha trovato nel bucket. Questi si aggiungono ai dettagli sulle impostazioni che influiscono sulla sicurezza e sulla privacy dei dati del bucket.
- Rilevamento di [dati sensibili](#): fornisci report dettagliati sui dati sensibili che Macie ha trovato nei singoli oggetti S3. I dettagli includono quando Macie ha trovato i dati sensibili e il tipo e il numero di occorrenze dei dati sensibili trovati da Macie. I dettagli includono anche informazioni sul bucket S3 e sull'oggetto interessati, comprese le impostazioni di accesso pubblico del bucket e la data dell'ultima modifica dell'oggetto.
- [Risultati del rilevamento di dati sensibili](#): fornisci le registrazioni delle analisi eseguite da Macie per i singoli oggetti S3. Ciò include oggetti in cui Macie non trova dati sensibili e oggetti che Macie non può analizzare a causa di problemi o errori. Se Macie trova dati sensibili in un oggetto, il risultato della scoperta dei dati sensibili fornisce informazioni sui dati sensibili trovati da Macie.

Con questi dati, puoi valutare la sensibilità dei dati in tutto il tuo patrimonio di dati Amazon S3 e approfondire per valutare e analizzare singoli bucket e oggetti S3. Oltre alle informazioni fornite da Macie sulla sicurezza e la privacy dei tuoi dati Amazon S3, puoi anche identificare i casi in cui potrebbe essere necessaria una correzione immediata, ad esempio un bucket accessibile al pubblico in cui Macie ha trovato dati sensibili.

Dati aggiuntivi possono aiutarti a valutare e monitorare la copertura dei tuoi dati Amazon S3. Con i dati di copertura, puoi controllare lo stato delle analisi relative al tuo insieme di dati e ai singoli bucket S3 al suo interno. Puoi anche identificare i problemi che impedivano a Macie di analizzare gli oggetti in bucket specifici. Se risolvi i problemi, puoi aumentare la copertura dei dati di Amazon S3 durante i cicli di analisi successivi. Per ulteriori informazioni, consulta [Valutazione della copertura automatizzata del rilevamento di dati sensibili](#).

Argomenti

- [Revisione delle statistiche sulla sensibilità dei dati nella dashboard di riepilogo](#)

- [Visualizzazione della sensibilità dei dati con la mappa dei bucket S3](#)
- [Valutazione della sensibilità dei dati con la tabella dei bucket S3](#)
- [Revisione dei dettagli sulla sensibilità dei dati per i bucket S3](#)
- [Analisi dei risultati derivanti dal rilevamento automatico di dati sensibili](#)
- [Accesso ai risultati del rilevamento mediante il rilevamento automatico di dati sensibili](#)

Revisione delle statistiche sulla sensibilità dei dati nella dashboard di riepilogo

Sulla console Amazon Macie, la dashboard Summary fornisce un'istantanea dei dati aggregati di statistiche e risultati per i dati correnti di Amazon Simple Storage Service (Amazon S3). Regione AWSÈ progettato per aiutarti a valutare il livello di sicurezza generale dei tuoi dati Amazon S3.

Le statistiche del dashboard includono dati relativi a parametri di sicurezza chiave, come il numero di bucket S3 per uso generico accessibili pubblicamente o condivisi con altri. Account AWS La dashboard mostra anche gruppi di dati aggregati relativi ai risultati del tuo account, ad esempio i bucket che hanno generato il maggior numero di risultati nei sette giorni precedenti. Se sei l'amministratore Macie di un'organizzazione, la dashboard fornisce statistiche e dati aggregati per tutti gli account dell'organizzazione. Puoi facoltativamente filtrare i dati per account.

Se l'individuazione automatica dei dati sensibili è abilitata, la dashboard di riepilogo include statistiche aggiuntive. Le statistiche registrano lo stato e i risultati delle attività di rilevamento automatizzato che Macie ha svolto finora per i tuoi dati Amazon S3. L'immagine seguente mostra un esempio di queste statistiche.



Le statistiche sono organizzate principalmente in due sezioni, Individuazione automatica e Problemi di copertura. Le statistiche nella sezione Rilevamento automatico forniscono un'istantanea dello stato e dei risultati correnti delle attività automatizzate di rilevamento di dati sensibili. Le statistiche nella sezione Problemi di copertura indicano se i problemi hanno impedito a Macie di analizzare gli

oggetti nei singoli bucket S3. Le statistiche non includono i dati relativi ai processi di rilevamento di dati sensibili che crei ed esegui. Tuttavia, è probabile che la risoluzione dei problemi di copertura per l'individuazione automatica dei dati sensibili aumenti anche la copertura dei lavori eseguiti successivamente.

Argomenti

- [Visualizzazione della dashboard di riepilogo](#)
- [Comprensione delle statistiche sull'individuazione dei dati sensibili nella dashboard di riepilogo](#)

Visualizzazione della dashboard di riepilogo

Segui questi passaggi per visualizzare la dashboard di riepilogo sulla console Amazon Macie. Per interrogare le statistiche a livello di codice, utilizza il [GetBucketStatistics](#) funzionamento dell'API Amazon Macie.

Per visualizzare la dashboard di riepilogo

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, scegli Riepilogo. Macie visualizza la dashboard di riepilogo.
3. Per approfondire ed esaminare i dati di supporto per un elemento sulla dashboard, scegli l'elemento.

Se sei l'amministratore Macie di un'organizzazione, la dashboard mostra statistiche e dati aggregati per il tuo account e gli account dei membri dell'organizzazione. Per visualizzare i dati solo per un determinato account, inserisci l'ID dell'account nella casella Account sopra la dashboard.

Comprensione delle statistiche sull'individuazione dei dati sensibili nella dashboard di riepilogo

La dashboard di riepilogo include statistiche aggregate che possono aiutarti a monitorare il rilevamento automatico di dati sensibili per i tuoi dati Amazon S3. Fornisce un'istantanea dello stato attuale e dei risultati delle analisi dei dati di Amazon S3 nel periodo corrente. Regione AWS Ad esempio, puoi utilizzare le statistiche del dashboard per determinare rapidamente in quanti bucket S3 Amazon Macie ha trovato dati sensibili e quanti di questi bucket sono accessibili pubblicamente. Puoi anche valutare la copertura dei tuoi dati Amazon S3. Le statistiche sulla copertura possono aiutarti a identificare i problemi che impediscono a Macie di analizzare gli oggetti nei singoli bucket S3.

Nella dashboard, le statistiche per l'individuazione automatica dei dati sensibili sono organizzate nelle seguenti sezioni:

- [Archiviazione e individuazione di dati sensibili](#)
- [Discovery automatizzata](#)
- [Problemi di copertura](#)

Le statistiche individuali in ogni sezione sono le seguenti. Per informazioni sulle statistiche in altre sezioni del pannello di controllo, consulta [Comprensione dei componenti della dashboard di riepilogo](#).

Archiviazione e individuazione di dati sensibili

Nella parte superiore della dashboard, le statistiche indicano la quantità di dati archiviata in Amazon S3 e la quantità di dati che Amazon Macie può analizzare per rilevare dati sensibili. L'immagine seguente mostra un esempio di queste statistiche per un'organizzazione con sette account.

Total accounts	Storage (classifiable/total)	Objects (classifiable/total)
7	307.7 GB / 313.4 GB	626.3 k / 633.0 k

Le statistiche individuali in questa sezione sono:

- Account totali: questo campo viene visualizzato se sei l'amministratore Macie di un'organizzazione o hai un account Macie autonomo. Indica il numero totale di Account AWS bucket personali presenti nel tuo inventario di bucket. Se sei un amministratore Macie, questo è il numero totale di account Macie che gestisci per la tua organizzazione. Se hai un account Macie indipendente, questo valore è 1.

Bucket S3 totali: questo campo viene visualizzato se disponi di un account membro in un'organizzazione. Indica il numero totale di bucket generici presenti nel tuo inventario, inclusi i bucket che non contengono oggetti.

- Archiviazione: queste statistiche forniscono informazioni sulla dimensione di archiviazione degli oggetti nel tuo inventario bucket:
 - Classificabile: la dimensione totale di archiviazione di tutti gli oggetti che Macie può analizzare nei bucket.
 - Totale: la dimensione totale di archiviazione di tutti gli oggetti nei bucket, inclusi gli oggetti che Macie non può analizzare.

Se alcuni oggetti sono file compressi, questi valori non riflettono la dimensione effettiva di quei file dopo la decompressione. Se il controllo delle versioni è abilitato per uno qualsiasi dei bucket, questi

valori si basano sulla dimensione di archiviazione della versione più recente di ogni oggetto in quei bucket.

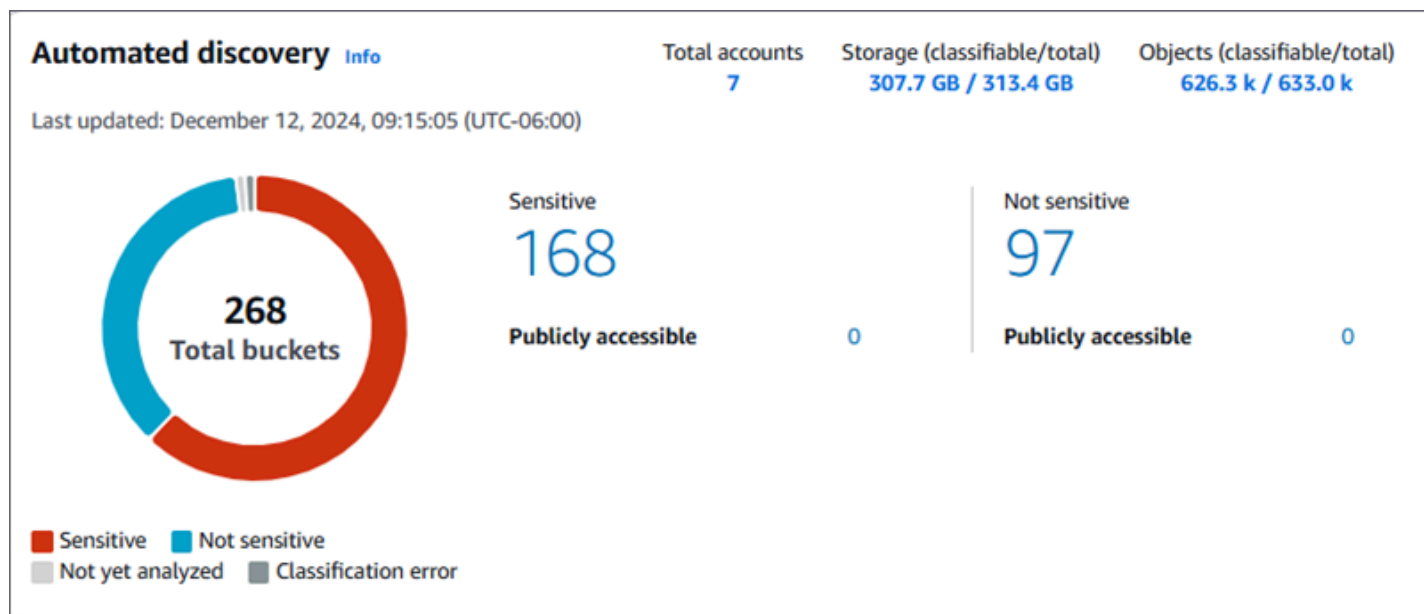
- **Oggetti:** queste statistiche forniscono informazioni sul numero di oggetti presenti nell'inventario dei bucket:
 - **Classificabile:** il numero totale di oggetti che Macie può analizzare nei bucket.
 - **Totale:** il numero totale di oggetti nei bucket, inclusi gli oggetti che Macie non può analizzare.

Nelle statistiche precedenti, i dati e gli oggetti sono classificabili se utilizzano una classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un file o un formato di storage supportato. È possibile rilevare dati sensibili negli oggetti utilizzando Macie. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).

Tieni presente che le statistiche di Storage and Objects non includono dati sugli oggetti nei bucket a cui Macie non può accedere. Per identificare i bucket in cui ciò si verifica, scegli la statistica Accesso negato nella sezione Problemi di copertura del pannello di controllo.

Individuazione automatica

Questa sezione riporta lo stato e i risultati delle attività automatizzate di rilevamento di dati sensibili che Amazon Macie ha svolto finora per i tuoi dati Amazon S3. L'immagine seguente mostra un esempio delle statistiche fornite da questa sezione.



Le statistiche individuali in questa sezione sono le seguenti.

Benne totali

Il grafico ad anello indica il numero totale di bucket presenti nell'inventario dei bucket. Il grafico raggruppa i bucket in categorie in base al punteggio di sensibilità corrente di ogni bucket:

- Sensibile (rosso): il numero totale di bucket il cui punteggio di sensibilità è compreso tra 51 e 100.
- Non sensibile (blu): il numero totale di bucket il cui punteggio di sensibilità è compreso tra 1 e 49.
- Non ancora analizzato (grigio chiaro): il numero totale di bucket il cui punteggio di sensibilità è 50.
- Errore di classificazione (grigio scuro): il numero totale di bucket il cui punteggio di sensibilità è -1.

Per dettagli sulla gamma di punteggi di sensibilità ed etichette definiti da Macie, vedi. [Punteggio di sensibilità per i bucket S3](#)

Per visualizzare le statistiche aggiuntive relative a un gruppo, passa il mouse sul gruppo:

- Secchielli: il numero totale di secchi.
- Accessibile pubblicamente: il numero totale di bucket che consentono al pubblico di accedere in lettura o scrittura al bucket.
- Byte classificabili: la dimensione totale di archiviazione di tutti gli oggetti che Macie può analizzare nei bucket. Questi oggetti utilizzano classi di storage Amazon S3 supportate e hanno estensioni dei nomi di file per i formati di file o di storage supportati. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).
- Byte totali: la dimensione totale di storage di tutti i bucket.

Nelle statistiche precedenti, i valori delle dimensioni di archiviazione si basano sulla dimensione di archiviazione della versione più recente di ciascun oggetto nei bucket. Se alcuni degli oggetti sono file compressi, questi valori non riflettono la dimensione effettiva di tali file dopo la decompressione.

Sensibile

Quest'area indica il numero totale di bucket che attualmente hanno un punteggio di sensibilità compreso tra 51 e 100. All'interno di questo gruppo, Pubblicamente accessibile indica il numero totale di bucket che consentono inoltre al pubblico in generale di avere accesso in lettura o scrittura al bucket.

Non sensibile

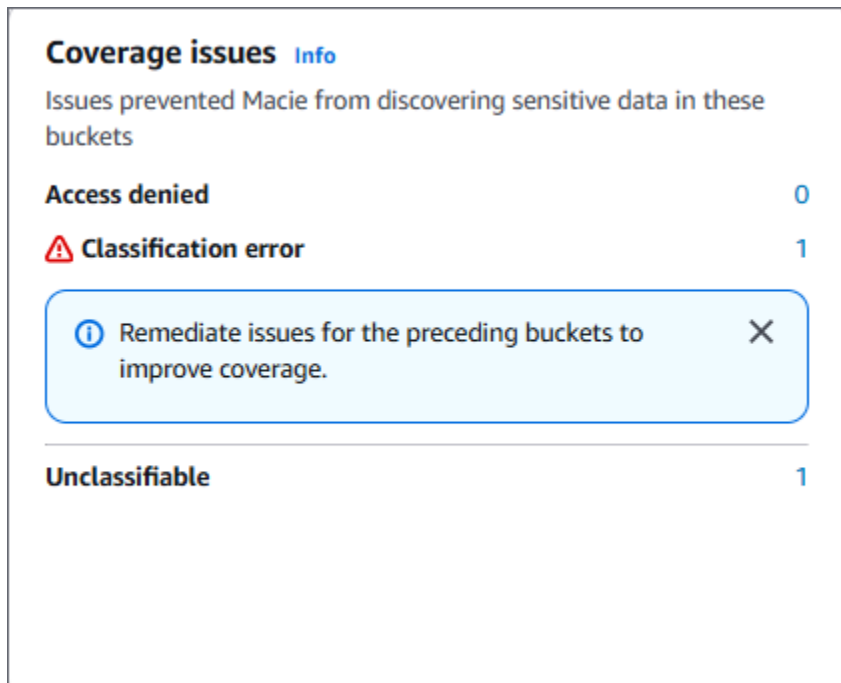
Quest'area indica il numero totale di bucket che attualmente hanno un punteggio di sensibilità compreso tra 1 e 49. All'interno di questo gruppo, Pubblicamente accessibile indica il numero totale di bucket che consentono inoltre al pubblico in generale di avere accesso in lettura o scrittura al bucket.

Per determinare e calcolare i valori per le statistiche accessibili pubblicamente, Macie analizza una combinazione di impostazioni a livello di account e bucket per ogni bucket, come le impostazioni di blocco dell'accesso pubblico per l'account e il bucket e la policy del bucket per il bucket. Macie esegue questa operazione per un massimo di 10.000 bucket per account. Per ulteriori informazioni, consulta [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#).

Tieni presente che le statistiche nella sezione Individuazione automatica non includono i risultati dei processi di rilevamento di dati sensibili che crei ed esegui.

Problemi di copertura

In questa sezione, le statistiche indicano se determinati tipi di problemi hanno impedito ad Amazon Macie di analizzare gli oggetti nei singoli bucket S3. L'immagine seguente mostra un esempio delle statistiche fornite da questa sezione.



Coverage issues Info	
Issues prevented Macie from discovering sensitive data in these buckets	
Access denied	0
 Classification error	1
 Remediate issues for the preceding buckets to improve coverage.	
Unclassifiable	1

Le statistiche individuali in questa sezione sono:

- **Accesso negato:** il numero totale di bucket a cui Macie non può accedere. Macie non può analizzare alcun oggetto in questi bucket. Le impostazioni delle autorizzazioni dei bucket impediscono a Macie di accedere ai bucket e agli oggetti dei bucket.
- **Errore di classificazione:** il numero totale di bucket che Macie non ha ancora analizzato a causa di errori di classificazione a livello di oggetto. Macie ha provato ad analizzare uno o più oggetti in questi bucket. Tuttavia, Macie non è riuscito ad analizzare gli oggetti a causa di problemi relativi alle impostazioni delle autorizzazioni a livello di oggetto, al contenuto degli oggetti o alle quote.
- **Inclassificabile:** il numero totale di bucket che non memorizzano oggetti classificabili. Macie non può analizzare alcun oggetto in questi bucket. Tutti gli oggetti utilizzano classi di storage Amazon S3 che Macie non supporta oppure hanno estensioni di nomi di file per formati di file o di storage che Macie non supporta.

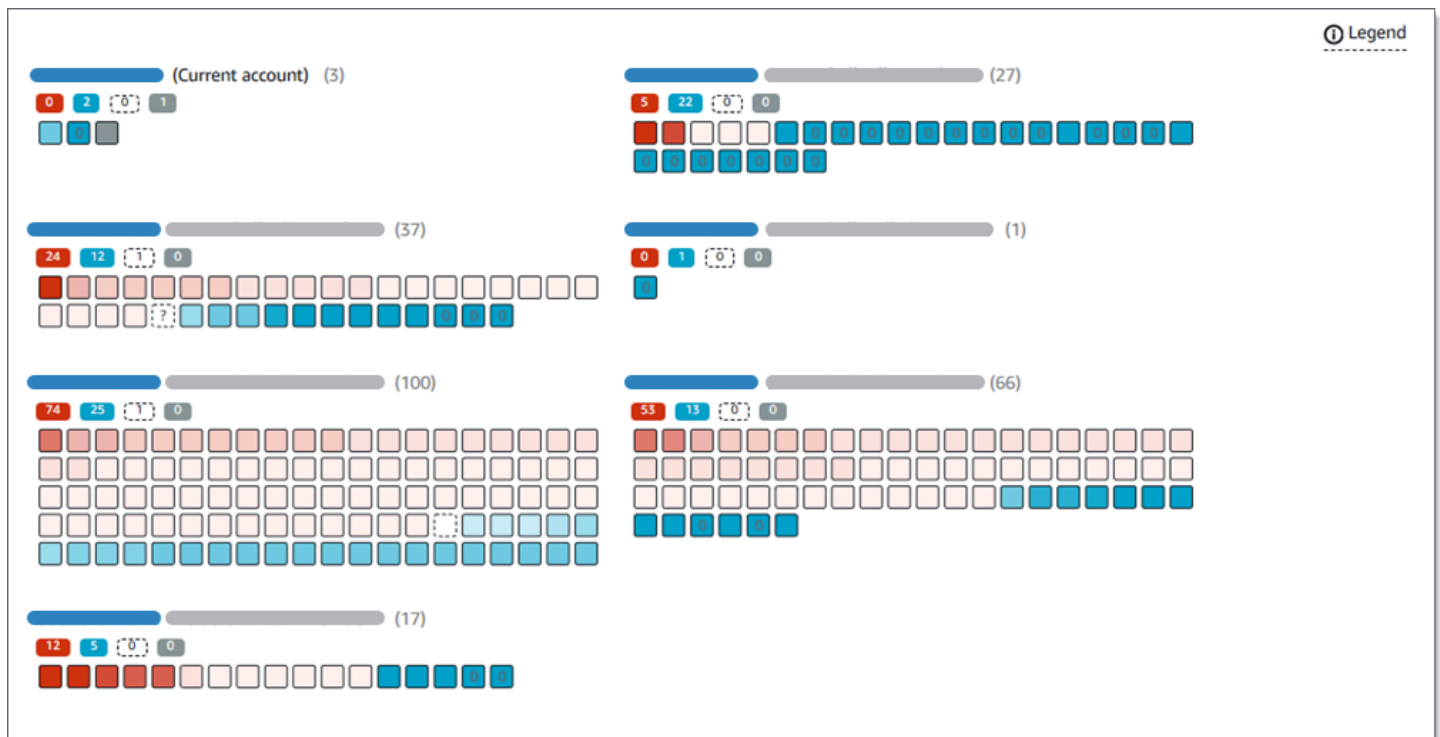
Scegli il valore di una statistica per visualizzare dettagli aggiuntivi e, se applicabile, linee guida per la correzione. Se risolvi i problemi di accesso e gli errori di classificazione, puoi aumentare la copertura dei dati di Amazon S3 durante i cicli di analisi successivi. Per ulteriori informazioni, consulta [Valutazione della copertura automatizzata del rilevamento di dati sensibili](#).

Tieni presente che le statistiche nella sezione Problemi di copertura non includono esplicitamente i dati relativi ai processi di rilevamento di dati sensibili che crei ed esegui. Tuttavia, è probabile che la risoluzione dei problemi di copertura che influiscono sul rilevamento automatico dei dati sensibili aumenti anche la copertura dei lavori eseguiti successivamente.

Visualizzazione della sensibilità dei dati con la mappa dei bucket S3

Sulla console Amazon Macie, la mappa termica dei bucket S3 fornisce una rappresentazione visiva e interattiva della sensibilità dei dati nell'insieme dei dati di Amazon Simple Storage Service (Amazon S3). Acquisisce i risultati delle attività automatizzate di rilevamento di dati sensibili che Macie ha svolto finora per i tuoi dati Amazon S3 attuali. Regione AWS

Se sei l'amministratore Macie di un'organizzazione, la mappa include i risultati per i bucket S3 di proprietà dei tuoi account membro. I dati sono raggruppati Account AWS e ordinati per ID account, come mostrato nell'immagine seguente.



La mappa mostra i dati per un massimo di 100 bucket S3 per ogni account. Per visualizzare i dati per tutti i bucket, puoi [passare alla visualizzazione tabella](#) e rivedere i dati in formato tabulare.

Per visualizzare la mappa, scegli i bucket S3 nel pannello di navigazione sulla console. Quindi scegli map



nella parte superiore della pagina. La mappa è disponibile solo se il rilevamento automatico dei dati sensibili è attualmente abilitato. Non include i risultati dei processi di rilevamento di dati sensibili creati ed eseguiti dall'utente.

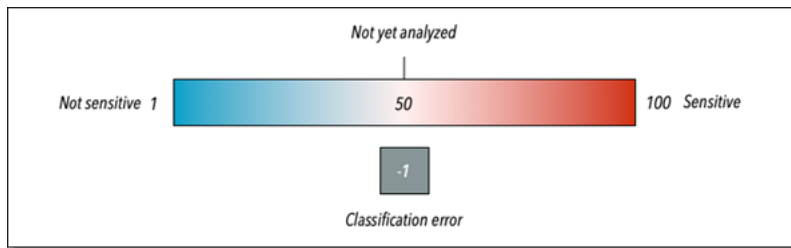
Argomenti

- [Interpretazione dei dati nella mappa dei bucket S3](#)
- [Interazione con la mappa dei bucket S3](#)

Interpretazione dei dati nella mappa dei bucket S3

Nella mappa dei bucket S3, ogni quadrato rappresenta un bucket S3 generico nell'inventario dei bucket. Il colore di un quadrato rappresenta il punteggio di sensibilità corrente di un bucket, che misura l'intersezione di due dimensioni principali: la quantità di dati sensibili che Macie ha trovato nel bucket e la quantità di dati che Macie ha analizzato nel bucket. L'intensità della tonalità del colore

rappresenta il punto in cui rientra un punteggio in un intervallo di valori di sensibilità dei dati, come mostrato nell'immagine seguente.



In generale, è possibile interpretare l'intensità del colore e della tonalità come segue:

- **Blu:** se il punteggio di sensibilità corrente di un bucket è compreso tra 1 e 49, il quadrato del bucket è blu e l'etichetta di sensibilità del bucket è Non sensibile. L'intensità della tonalità blu riflette il numero di oggetti unici che Macie ha analizzato nel bucket rispetto al numero totale di oggetti unici nel bucket. Una tonalità più scura indica un punteggio di sensibilità inferiore.
- **Nessun colore:** se il punteggio di sensibilità corrente di un bucket è 50, il quadrato del bucket non è colorato e l'etichetta di sensibilità del bucket non è ancora analizzata. Inoltre, il quadrato ha un bordo tratteggiato.
- **Rosso:** se il punteggio di sensibilità corrente di un bucket è compreso tra 51 e 100, il quadrato del bucket è rosso e l'etichetta di sensibilità del bucket è Sensibile. L'intensità della tonalità rossa riflette la quantità di dati sensibili che Macie ha trovato nel bucket. Una tonalità più scura indica un punteggio di sensibilità più elevato.
- **Grigio:** se il punteggio di sensibilità corrente di un bucket è -1, il quadrato del bucket è grigio scuro e l'etichetta di sensibilità del bucket è Errore di classificazione. L'intensità della tonalità non varia.

Per dettagli sulla gamma di punteggi di sensibilità ed etichette definiti da Macie, vedi [Punteggio di sensibilità per i bucket S3](#)

Nella mappa, il quadrato di un bucket S3 potrebbe contenere anche un simbolo. Il simbolo indica un errore, un problema o un altro tipo di considerazione che potrebbe influire sulla valutazione della sensibilità di un bucket. Un simbolo può anche indicare un potenziale problema con la sicurezza del bucket, ad esempio se il bucket è accessibile pubblicamente. La tabella seguente elenca i simboli utilizzati da Macie per avvisare l'utente di questi casi.

Symbol	Definizione	Descrizione
	Accesso negato	A Macie non è consentit o accedere al bucket o agli oggetti del bucket. Di conseguenza, Macie non può analizzare alcun oggetto nel bucket. Questo problema si verifica in genere perché un bucket ha una politica restrittiva sui bucket. Per informazioni su come risolvere questo problema, consulta Consentir e a Macie di accedere a bucket e oggetti S3
	Accessibile pubblicamente	Il pubblico in generale ha accesso in lettura o scrittura al bucket. Per effettuare questa determinazione, Macie analizza una combinazione di impostazioni per ogni bucket, ad esempio le impostazioni di blocco dell'accesso pubblico per l'account e il bucket e la politica del bucket per il bucket. Macie può eseguire questa operazione per un massimo di 10.000 bucket per account. Per ulteriori informazioni, consulta In che modo Macie monitora la sicurezza dei dati di Amazon S3.

Symbol	Definizione	Descrizione
	Inclassificabile	Macie non può analizzare nessun oggetto nel secchio. Tutti gli oggetti del bucket utilizzano classi di storage Amazon S3 che Macie non supporta oppure hanno estensioni di nomi di file per formati di file o di archiviazione che Macie non supporta. Affinché Macie possa analizzare un oggetto, l'oggetto deve utilizzare una classe di archiviazione supportata e avere un'estensione del nome di file per un file o un formato di archiviazione supportato. Per ulteriori informazioni, consulta Classi e formati di archiviazione supportati.
	Zero byte	Il bucket non contiene alcun oggetto da analizzare da Macie. Il bucket è vuoto o tutti gli oggetti nel bucket contengono zero (0) byte di dati.

Interazione con la mappa dei bucket S3

Mentre esamiini la mappa dei bucket S3, puoi interagire con essa in diversi modi per rivelare e valutare dati e dettagli aggiuntivi per singoli account e bucket. Segui questi passaggi per visualizzare la mappa e utilizzare le varie funzionalità che offre.

Per interagire con la mappa dei bucket S3

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra una mappa del tuo inventario di bucket. Se invece la pagina mostra il tuo inventario in formato tabellare, scegli map



nella parte superiore della pagina.

Per impostazione predefinita, la mappa non mostra i dati relativi ai bucket attualmente esclusi dal rilevamento automatico dei dati sensibili. Se sei l'amministratore Macie di un'organizzazione, inoltre, non visualizza i dati degli account per i quali l'individuazione automatica dei dati sensibili è attualmente disabilitata. Per visualizzare questi dati, scegli X nel filtro È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Nella parte superiore della pagina, scegli facoltativamente refresh



per recuperare i metadati del bucket più recenti da Amazon S3.

4. Nella mappa dei bucket S3, esegui una delle seguenti operazioni:

- Per determinare quanti bucket hanno un'etichetta di sensibilità specifica, fai riferimento ai badge colorati immediatamente sotto un ID. Account AWS I badge mostrano i conteggi aggregati dei bucket, suddivisi per etichetta di sensibilità.

Ad esempio, il badge rosso riporta il numero totale di bucket di proprietà dell'account e con l'etichetta Sensitive. Il punteggio di sensibilità per questi bucket varia da 51 a 100. Il badge blu riporta il numero totale di bucket di proprietà dell'account e contrassegnati dall'etichetta Non sensibile. Il punteggio di sensibilità per questi bucket varia da 1 a 49.

- Per esaminare un sottoinsieme di informazioni su un bucket, passa il mouse sul quadrato del bucket. Un popover mostra il nome del bucket e il punteggio di sensibilità corrente.

Il popover mostra anche il numero totale di oggetti che Macie può analizzare nel bucket e la dimensione totale di archiviazione della versione più recente di tali oggetti. Questi oggetti sono classificabili. Utilizzano classi di storage Amazon S3 supportate e dispongono di estensioni dei nomi di file per i formati di file o di storage supportati. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).

- Per filtrare la mappa e visualizzare solo i bucket che hanno un valore specifico per un campo, posiziona il cursore nella casella del filtro, quindi aggiungi una condizione di filtro per il campo. Macie applica i criteri della condizione e la visualizza sotto la casella del filtro. Per perfezionare ulteriormente i risultati, aggiungi condizioni di filtro per campi aggiuntivi. Per ulteriori informazioni, consulta [Filtrare l'inventario dei bucket S3](#).
 - Per approfondire e visualizzare solo i bucket di proprietà di un determinato account, scegli l'ID dell'account. Macie apre una nuova scheda che filtra e visualizza i dati solo per quell'account.
5. Per esaminare le statistiche sulla sensibilità dei dati e altre informazioni per un determinato bucket, scegli il quadrato del bucket. Quindi consulta il pannello dei dettagli. Per informazioni su questi dettagli, vedere [Revisione dei dettagli sulla sensibilità dei dati per i bucket S3](#).

 Tip

Nella scheda Bucket details del pannello, puoi eseguire il pivot e approfondire molti campi. Per mostrare i bucket che hanno lo stesso valore per un campo, scegli nel campo.



Per mostrare i bucket che hanno altri valori per un campo, scegli



nel campo.

Valutazione della sensibilità dei dati con la tabella dei bucket S3

Per esaminare le informazioni di riepilogo relative ai bucket Amazon Simple Storage Service (Amazon S3), puoi utilizzare la tabella dei bucket S3 sulla console Amazon Macie. Utilizzando la tabella, puoi rivedere e analizzare un inventario dei tuoi bucket generici nella versione corrente Regione AWS e approfondire le informazioni e le statistiche dettagliate per i singoli bucket. Se sei l'amministratore Macie di un'organizzazione, la tabella include informazioni sui bucket di proprietà dei tuoi account membro. Se preferisci accedere e interrogare i dati a livello di codice, puoi utilizzare il [DescribeBuckets](#) funzionamento dell'API Amazon Macie.

Sulla console, puoi ordinare e filtrare la tabella per personalizzare la visualizzazione. Puoi anche esportare i dati dalla tabella in un file con valori separati da virgole (CSV). Se scegli un bucket S3 nella tabella, il pannello dei dettagli mostra informazioni aggiuntive sul bucket. Ciò include dettagli e statistiche per impostazioni e metriche che forniscono informazioni sulla sicurezza e la privacy dei dati del bucket. Se il rilevamento automatico dei dati sensibili è abilitato, include anche i dati che

acquisiscono i risultati delle attività di rilevamento automatizzato che Macie ha svolto finora per il bucket.

Per valutare la sensibilità dei dati utilizzando la tabella dei bucket S3

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra l'inventario dei bucket.

Per impostazione predefinita, la pagina non mostra i dati relativi ai bucket attualmente esclusi dal rilevamento automatico dei dati sensibili. Se sei l'amministratore Macie di un'organizzazione, inoltre, non vengono visualizzati i dati degli account per i quali l'individuazione automatica dei dati sensibili è attualmente disabilitata. Per visualizzare questi dati, scegli X nel filtro È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Scegli la tabella



)
nella parte superiore della pagina. Macie mostra il numero di secchi nel tuo inventario e una tabella dei secchi.

4. Per recuperare i metadati del bucket più recenti da Amazon S3, scegli refresh



)
nella parte superiore della pagina.

Se l'icona delle informazioni



)
appare accanto ai nomi dei bucket, ti consigliamo di farlo. [Questa icona indica che un bucket è stato creato nelle ultime 24 ore, probabilmente dopo l'ultima volta che Macie ha recuperato i metadati del bucket e dell'oggetto da Amazon S3 come parte del ciclo di aggiornamento giornaliero.](#)

5. Nella tabella dei bucket S3, esamina le informazioni di riepilogo su ogni bucket del tuo inventario:
 - Sensibilità: il punteggio di sensibilità attuale del bucket. Per informazioni sulla gamma di punteggi di sensibilità definiti da Macie, consulta. [Punteggio di sensibilità per i bucket S3](#)
 - Bucket: il nome del bucket.
 - Account: l'ID dell'account Account AWS che possiede il bucket.
 - Oggetti classificabili: il numero totale di oggetti che Macie può analizzare per rilevare i dati sensibili nel bucket.

- Dimensioni classificabili: la dimensione totale di archiviazione di tutti gli oggetti che Macie può analizzare per rilevare i dati sensibili nel bucket.

Questo valore non riflette le dimensioni effettive degli oggetti compressi dopo che sono stati decompressi. Inoltre, se il controllo delle versioni è abilitato per il bucket, questo valore si basa sulla dimensione di archiviazione della versione più recente di ogni oggetto nel bucket.

- Monitoraggio per processo: indipendentemente dal fatto che tu abbia configurato processi di rilevamento di dati sensibili per analizzare periodicamente gli oggetti nel bucket su base giornaliera, settimanale o mensile.

Se il valore di questo campo è Sì, il bucket viene incluso in modo esplicito in un processo periodico oppure il bucket corrisponde ai criteri per un processo periodico nelle ultime 24 ore. Inoltre, lo stato di almeno uno di questi lavori non è Annullato. Macie aggiorna questi dati su base giornaliera.

- Ultimo processo eseguito: se hai configurato un job di rilevamento di dati sensibili una tantum o periodico per analizzare gli oggetti nel bucket, questo campo indica la data e l'ora più recenti in cui uno di questi processi ha iniziato a essere eseguito. Altrimenti, in questo campo viene visualizzato un trattino (—).

Nei dati precedenti, gli oggetti sono classificabili se utilizzano una classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un formato di file o di storage supportato. Puoi rilevare dati sensibili negli oggetti usando Macie. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).

6. Per analizzare l'inventario utilizzando la tabella, esegui una delle seguenti operazioni:

- Per ordinare la tabella in base a un campo specifico, scegli l'intestazione di colonna del campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna.
- Per filtrare la tabella e visualizzare solo i bucket che hanno un valore specifico per un campo, posiziona il cursore nella casella del filtro, quindi aggiungi una condizione di filtro per il campo. Per rifinire ulteriormente i risultati, aggiungi condizioni di filtro per campi aggiuntivi. Per ulteriori informazioni, consulta [Filtrare l'inventario dei bucket S3](#).
- Per esaminare le statistiche sulla sensibilità dei dati e altre informazioni per un determinato bucket, scegli il nome del bucket. Quindi consulta il pannello dei dettagli. Per informazioni su questi dettagli, vedere [Analisi dei dettagli dei bucket S3](#).

 Tip

Nella scheda Bucket details del pannello, puoi eseguire il pivot e approfondire molti campi. Per mostrare i bucket che hanno lo stesso valore per un campo, scegli nel campo.



Per mostrare i bucket che hanno altri valori per un campo, scegli



nel campo.

7. Per esportare i dati dalla tabella in un file CSV, seleziona la casella di controllo per ogni riga da esportare oppure seleziona la casella di controllo nell'intestazione della colonna di selezione per selezionare tutte le righe. Quindi scegli Esporta in CSV nella parte superiore della pagina. Puoi esportare fino a 50.000 righe dalla tabella.
8. Per eseguire un'analisi più approfondita e immediata degli oggetti in uno o più bucket, seleziona la casella di controllo per ogni bucket. Quindi seleziona Crea processo. Per ulteriori informazioni, consulta [Creazione di un processo di rilevamento dei dati sensibili](#).

Revisione dei dettagli sulla sensibilità dei dati per i bucket S3

Man mano che l'individuazione automatica dei dati sensibili progredisce, puoi esaminare i risultati dettagliati nelle statistiche e in altre informazioni fornite da Amazon Macie su ciascuno dei tuoi bucket Amazon Simple Storage Service (Amazon S3). Se sei l'amministratore Macie di un'organizzazione, sono inclusi i bucket di proprietà dei tuoi account membro.

Le statistiche e le informazioni includono dettagli che forniscono informazioni sulla sicurezza e la privacy dei dati di un bucket S3. Raccolgono anche i risultati delle attività automatizzate di scoperta di dati sensibili che Macie ha svolto finora per un sacco di tempo. Ad esempio, puoi trovare un elenco di oggetti che Macie ha analizzato in un bucket. Puoi anche trovare un'analisi dettagliata dei tipi e del numero di occorrenze di dati sensibili che Macie ha trovato in un bucket. Tieni presente che questi dati non includono i risultati dei processi di rilevamento di dati sensibili che crei ed esegui.

Macie ricalcola e aggiorna automaticamente le statistiche e i dettagli per i bucket S3 mentre esegue il rilevamento automatico dei dati sensibili. Per esempio:

- Se Macie non trova dati sensibili in un oggetto S3, Macie riduce il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario. Macie aggiunge inoltre l'oggetto all'elenco degli oggetti selezionati per l'analisi.
- Se Macie trova dati sensibili in un oggetto S3, Macie aggiunge tali occorrenze alla suddivisione dei tipi di dati sensibili che Macie ha trovato nel bucket. Macie aumenta anche il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario. Inoltre, Macie aggiunge l'oggetto all'elenco degli oggetti selezionati per l'analisi. Queste attività si aggiungono alla creazione di una ricerca di dati sensibili per l'oggetto.
- Se Macie trova dati sensibili in un oggetto S3 che viene successivamente modificato o eliminato, Macie rimuove le occorrenze di dati sensibili per l'oggetto dalla suddivisione dei tipi di dati sensibili del bucket. Macie riduce anche il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità del bucket, se necessario. Inoltre, Macie rimuove l'oggetto dall'elenco degli oggetti selezionati per l'analisi.
- Se Macie tenta di analizzare un oggetto S3 ma un problema o un errore impedisce l'analisi, Macie aggiunge l'oggetto all'elenco degli oggetti selezionati per l'analisi e indica che non è stato in grado di analizzare l'oggetto.

Se sei l'amministratore Macie di un'organizzazione o disponi di un account Macie autonomo, puoi opzionalmente utilizzare questi dettagli per valutare e modificare determinate impostazioni di rilevamento automatico per un bucket S3. Ad esempio, puoi includere o escludere tipi specifici di dati sensibili dal punteggio di un bucket. Per ulteriori informazioni, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Per esaminare i dettagli sulla sensibilità dei dati per un bucket S3

Per verificare la sensibilità dei dati e altri dettagli per un bucket S3, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Sulla console, il pannello dei dettagli fornisce l'accesso centralizzato a queste informazioni. Con l'API, puoi recuperare ed elaborare i dati a livello di codice.

Console

Segui questi passaggi per verificare la sensibilità dei dati e altri dettagli per un bucket S3 utilizzando la console Amazon Macie.

Per esaminare i dettagli di un bucket S3

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>

2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra una mappa interattiva del tuo inventario di bucket. Facoltativamente, scegli table



) nella parte superiore della pagina per visualizzare l'inventario in formato tabulare.

Per impostazione predefinita, la pagina non mostra i dati relativi ai bucket attualmente esclusi dal rilevamento automatico dei dati sensibili. Se sei l'amministratore Macie di un'organizzazione, inoltre, non vengono visualizzati i dati degli account per i quali l'individuazione automatica dei dati sensibili è attualmente disabilitata. Per visualizzare questi dati, scegli X nel filtro È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Per recuperare i metadati del bucket più recenti da Amazon S3, scegli refresh



) nella parte superiore della pagina.

4. Scegli il bucket di cui desideri esaminare i dettagli. Il pannello dei dettagli mostra le statistiche sulla sensibilità dei dati e altre informazioni sul bucket.

La parte superiore del pannello mostra informazioni generali sul bucket: il nome del bucket, l'ID dell'account del proprietario del Account AWS bucket e il punteggio di sensibilità corrente del bucket. Se sei un amministratore di Macie o disponi di un account Macie autonomo, offre anche opzioni per modificare alcune impostazioni di rilevamento automatico per il bucket. Le impostazioni e le informazioni aggiuntive sono organizzate nelle seguenti schede:

[Sensibilità](#) | [Dettagli del bucket](#) | [Esempi di oggetti](#) | [Rilevamento](#) di [dati sensibili](#)

Le impostazioni e le informazioni individuali su ciascuna scheda sono le seguenti.

Sensibilità

Questa scheda mostra l'attuale punteggio di sensibilità del bucket, compreso tra -1 e 100. Per informazioni sulla gamma di punteggi di sensibilità definiti da Macie, consulta. [Punteggio di sensibilità per i bucket S3](#)

La scheda fornisce anche un'analisi dettagliata dei tipi di dati sensibili che Macie ha trovato negli oggetti del bucket e il numero di occorrenze di ciascun tipo:

- Tipo di dati sensibili: l'identificatore univoco (ID) dell'identificatore di dati gestito che ha rilevato i dati o il nome dell'identificatore di dati personalizzato che ha rilevato i dati.

L'ID di un identificatore di dati gestito descrive il tipo di dati sensibili che è progettato per rilevare, ad esempio USA_PASSPORT_NUMBER per i numeri di passaporto statunitensi. Per informazioni dettagliate su ciascun identificatore di dati gestito, consulta [Utilizzo di identificatori di dati gestiti](#)

- Conteggio: il numero totale di occorrenze dei dati rilevate dall'identificatore di dati gestito o personalizzato.
- Stato del punteggio: questo campo viene visualizzato se sei un amministratore Macie o hai un account Macie autonomo. Specifica se le occorrenze dei dati sono incluse o escluse dal punteggio di sensibilità del bucket.

Se Macie calcola il punteggio del bucket, puoi modificare il calcolo includendo o escludendo tipi specifici di dati sensibili dal punteggio: seleziona la casella di controllo relativa all'identificatore che ha rilevato i dati sensibili da includere o escludere, quindi scegli un'opzione dal menu Azioni. Per ulteriori informazioni, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Se Macie non ha trovato dati sensibili negli oggetti attualmente archiviati nel bucket, questa sezione mostra il messaggio Nessun rilevamento trovato.

Nota che la scheda Sensibilità non include i dati relativi agli oggetti che sono stati modificati o eliminati dopo che Macie li ha analizzati. Se gli oggetti vengono modificati o eliminati dopo l'analisi, Macie ricalcola e aggiorna automaticamente le statistiche e i dati appropriati per escludere gli oggetti.

Dettagli del bucket

Questa scheda fornisce dettagli sulle impostazioni del bucket, incluse le impostazioni sulla sicurezza dei dati e sulla privacy. Ad esempio, puoi esaminare le suddivisioni delle impostazioni di accesso pubblico del bucket e determinare se il bucket replica oggetti o è condiviso con altri. Account AWS

In particolare, il campo Ultimo aggiornamento indica l'ultima data in cui Macie ha recuperato i metadati da Amazon S3 per il bucket o gli oggetti del bucket. Il campo Ultima esecuzione di rilevamento automatico indica quando Macie ha analizzato l'ultima volta gli oggetti nel bucket durante l'individuazione automatica dei dati sensibili. Se questa analisi non è stata effettuata, in questo campo viene visualizzato un trattino (—).

La scheda fornisce anche statistiche a livello di oggetto che possono aiutarti a valutare la quantità di dati che Macie può analizzare nel bucket. Indica inoltre se sono stati configurati

processi di rilevamento di dati sensibili per analizzare gli oggetti nel bucket. In tal caso, è possibile accedere ai dettagli sul processo eseguito più di recente e quindi, facoltativamente, visualizzare tutti i risultati prodotti dal lavoro.

In alcuni casi, questa scheda potrebbe non includere tutti i dettagli di un bucket. Ciò può verificarsi se si archiviano più di 10.000 bucket in Amazon S3. Macie conserva i dati di inventario completi per soli 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente. Macie può, tuttavia, analizzare gli oggetti in bucket che superano questa quota. Per esaminare ulteriori dettagli sui bucket, usa Amazon S3.

Per ulteriori dettagli sulle informazioni contenute in questa scheda, consulta [Analisi dei dettagli dei bucket S3](#)

Esempi di oggetti

Questa scheda elenca gli oggetti che Macie ha selezionato per l'analisi durante l'individuazione automatica dei dati sensibili per il bucket. Facoltativamente, scegli il nome di un oggetto per aprire la console Amazon S3 e visualizzare le proprietà dell'oggetto.

L'elenco include dati per un massimo di 100 oggetti. L'elenco viene compilato in base al valore del campo di sensibilità dell'oggetto: Sensitivo, seguito da Non sensibile, seguito dagli oggetti che Macie non è stato in grado di analizzare.

Nell'elenco, il campo Sensibilità dell'oggetto indica se Macie ha trovato dati sensibili in un oggetto:

- Sensibile: Macie ha rilevato almeno un'occorrenza di dati sensibili nell'oggetto.
- Non sensibile: Macie non ha trovato dati sensibili nell'oggetto.
- — (trattino) — Macie non è riuscita a completare l'analisi dell'oggetto a causa di un problema o di un errore.

Il campo dei risultati della classificazione indica se Macie è stata in grado di analizzare un oggetto:

- Completa: Macie ha completato l'analisi dell'oggetto.
- Parziale: Macie ha analizzato solo un sottoinsieme di dati nell'oggetto a causa di un problema o di un errore. Ad esempio, l'oggetto è un file di archivio che contiene file in un formato non supportato.
- Ignorato: Macie non è stato in grado di analizzare alcun dato nell'oggetto a causa di un problema o di un errore. Ad esempio, l'oggetto è crittografato con una chiave che Macie non può usare.

Nota che l'elenco non include gli oggetti che sono stati modificati o eliminati dopo che Macie li ha analizzati o ha tentato di analizzarli. Macie rimuove automaticamente un oggetto dall'elenco se l'oggetto viene successivamente modificato o eliminato.

Rilevamento di dati sensibili

Questa scheda fornisce statistiche aggregate e automatizzate sull'individuazione dei dati sensibili per il bucket:

- **Byte analizzati:** la quantità totale di dati, in byte, che Macie ha analizzato nel bucket.
- **Byte classificabili:** la dimensione totale di archiviazione, in byte, di tutti gli oggetti che Macie può analizzare nel bucket. Questi oggetti utilizzano classi di storage Amazon S3 supportate e hanno estensioni dei nomi di file per i formati di file o di storage supportati. Per ulteriori informazioni, consulta [Classi e formati di archiviazione supportati](#).
- **Rilevamenti totali:** il numero totale di occorrenze di dati sensibili che Macie ha trovato nel bucket. Ciò include le occorrenze attualmente soppresse dalle impostazioni del punteggio di sensibilità per il bucket.

Il grafico Oggetti analizzati indica il numero totale di oggetti che Macie ha analizzato nel bucket. Fornisce inoltre una rappresentazione visiva del numero di oggetti in cui Macie ha trovato o non ha trovato dati sensibili. La legenda sotto il grafico mostra una suddivisione di questi risultati:

- **Oggetti sensibili (rosso):** il numero totale di oggetti in cui Macie ha trovato almeno una occorrenza di dati sensibili.
- **Oggetti non sensibili (blu):** il numero totale di oggetti in cui Macie non ha trovato dati sensibili.
- **Oggetti ignorati (grigio scuro):** il numero totale di oggetti che Macie non è stato in grado di analizzare a causa di un problema o di un errore.

L'area sotto la legenda del grafico fornisce un'analisi dettagliata dei casi in cui Macie non è stato in grado di analizzare gli oggetti a causa di determinati tipi di problemi di autorizzazione o errori crittografici:

- **Ignorata: crittografia non valida:** il numero totale di oggetti crittografati con chiavi fornite dal cliente. Macie non può accedere a queste chiavi.
- **Ignorato: KMS non valido:** il numero totale di oggetti crittografati con chiavi AWS Key Management Service (AWS KMS) che non sono più disponibili. Questi oggetti sono crittografati con quelli AWS KMS keys che erano disabilitati, la cui eliminazione è pianificata o sono stati eliminati. Macie non può usare queste chiavi.

- Ignorato: autorizzazione negata: il numero totale di oggetti a cui Macie non può accedere a causa delle impostazioni delle autorizzazioni per l'oggetto o delle impostazioni delle autorizzazioni per la chiave utilizzata per crittografare l'oggetto.

Per informazioni dettagliate su questi e altri tipi di problemi ed errori che possono verificarsi, consulta [Risolvere i problemi di copertura](#). Se risolvi i problemi e gli errori, puoi aumentare la copertura dei dati del bucket durante i cicli di analisi successivi.

Le statistiche nella scheda Rilevamento dei dati sensibili non includono i dati relativi agli oggetti che sono stati modificati o eliminati dopo che Macie li ha analizzati o ha tentato di analizzarli. Se gli oggetti vengono modificati o eliminati dopo che Macie li ha analizzati o ha tentato di analizzarli, Macie ricalcola automaticamente queste statistiche per escludere gli oggetti.

API

Per recuperare la sensibilità dei dati e altri dettagli per un bucket S3 a livello di codice, sono disponibili diverse opzioni. L'opzione appropriata dipende dai dettagli che desideri recuperare:

- Per recuperare il punteggio di sensibilità corrente di un bucket e le statistiche di analisi aggregate, utilizza l'operazione. [GetResourceProfile](#). Oppure, se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando. [get-resource-profile](#). Le statistiche includono dati come il numero di oggetti che Macie ha analizzato e il numero di oggetti in cui Macie ha trovato dati sensibili.
- Per recuperare un'analisi dettagliata dei tipi e della quantità di dati sensibili che Macie ha trovato in un bucket, usa l'operazione. [ListResourceProfileDetections](#). Oppure, se utilizzi il, esegui il comando AWS CLI. [list-resource-profile-detections](#). La suddivisione fornisce anche dettagli sull'identificatore di dati gestito o personalizzato che ha rilevato ogni tipo di dati sensibili.
- Per recuperare un elenco di un massimo di 100 oggetti che Macie ha selezionato da un bucket per l'analisi, usa l'operazione. [ListResourceProfileArtifacts](#). Oppure, se utilizzi il AWS CLI, esegui il comando. [list-resource-profile-artifacts](#). Per ogni oggetto, l'elenco specifica: l'Amazon Resource Name (ARN) dell'oggetto, se Macie ha completato l'analisi dell'oggetto e se Macie ha trovato dati sensibili nell'oggetto.

Nella tua richiesta, usa il `resourceArn` parametro per specificare l'ARN del bucket di cui recuperare i dettagli. Se si utilizza il AWS CLI, utilizzare il `resource-arn` parametro per specificare l'ARN.

Per ulteriori dettagli su un bucket S3, come le impostazioni di accesso pubblico del bucket, usa l'operazione. [DescribeBuckets](#) Se utilizzi il AWS CLI, esegui il comando [describe-buckets](#) per recuperare questi dettagli. Nella richiesta, utilizza facoltativamente i criteri di filtro per specificare il nome del bucket. Per maggiori informazioni ed esempi, consulta [Filtrare l'inventario dei bucket S3](#).

Gli esempi seguenti mostrano come utilizzare il per recuperare i AWS CLI dettagli sulla sensibilità dei dati per un bucket S3. Questo primo esempio recupera il punteggio di sensibilità corrente e le statistiche di analisi aggregate per un bucket.

```
$ aws macie2 get-resource-profile --resource-arn arn:aws:s3:::amzn-s3-demo-bucket
```

arn:aws:s3:::amzn-s3-demo-bucket Dov'è l'ARN del bucket. Se la richiesta ha esito positivo, riceverai un output simile al seguente:

```
{
  "profileUpdatedAt": "2024-11-21T15:44:46+00:00",
  "sensitivityScore": 83,
  "sensitivityScoreOverridden": false,
  "statistics": {
    "totalBytesClassified": 933599,
    "totalDetections": 3641,
    "totalDetectionsSuppressed": 0,
    "totalItemsClassified": 111,
    "totalItemsSensitive": 84,
    "totalItemsSkipped": 1,
    "totalItemsSkippedInvalidEncryption": 0,
    "totalItemsSkippedInvalidKms": 0,
    "totalItemsSkippedPermissionDenied": 0
  }
}
```

L'esempio successivo recupera una suddivisione dei tipi di dati sensibili che Macie ha trovato in un bucket S3 e il numero di occorrenze di ogni tipo. La suddivisione specifica anche quale identificatore di dati gestito o identificatore di dati personalizzato ha rilevato i dati. Indica anche se le occorrenze sono attualmente escluse (suppressed) dal punteggio di sensibilità del bucket, se il punteggio viene calcolato automaticamente da Macie.

```
$ aws macie2 list-resource-profile-detections --resource-arn arn:aws:s3:::amzn-s3-demo-bucket
```

arn:aws:s3:::amzn-s3-demo-bucket Dov'è l'ARN del bucket. Se la richiesta ha esito positivo, riceverai un output simile al seguente:

```
{
  "detections": [
    {
      "count": 8,
      "id": "AWS_CREDENTIALS",
      "name": "AWS_CREDENTIALS",
      "suppressed": false,
      "type": "MANAGED"
    },
    {
      "count": 1194,
      "id": "CREDIT_CARD_NUMBER",
      "name": "CREDIT_CARD_NUMBER",
      "suppressed": false,
      "type": "MANAGED"
    },
    {
      "count": 1194,
      "id": "CREDIT_CARD_SECURITY_CODE",
      "name": "CREDIT_CARD_SECURITY_CODE",
      "suppressed": false,
      "type": "MANAGED"
    },
    {
      "arn": "arn:aws:macie2:us-east-1:123456789012:custom-data-
      identifier/3293a69d-4a1e-4a07-8715-208ddexample",
      "count": 8,
      "id": "3293a69d-4a1e-4a07-8715-208ddexample",
      "name": "Employee IDs with keyword",
      "suppressed": false,
      "type": "CUSTOM"
    },
    {
      "count": 1237,
      "id": "USA_SOCIAL_SECURITY_NUMBER",
      "name": "USA_SOCIAL_SECURITY_NUMBER",
      "suppressed": false,
      "type": "MANAGED"
    }
  ]
}
```



```
}
```

Questo esempio recupera un elenco di oggetti che Macie ha selezionato da un bucket S3 per l'analisi. Per ogni oggetto, l'elenco indica anche se Macie ha completato l'analisi dell'oggetto e se Macie ha trovato dati sensibili nell'oggetto.

```
$ aws macie2 list-resource-profile-artifacts --resource-arn arn:aws:s3:::amzn-s3-demo-bucket
```

arn:aws:s3:::amzn-s3-demo-bucketDov'è l'ARN del bucket. Se la richiesta ha esito positivo, riceverai un output simile al seguente:

```
{
  "artifacts": [
    {
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket/amzn-s3-demo-object1.csv",
      "classificationResultStatus": "COMPLETE",
      "sensitive": true
    },
    {
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket/amzn-s3-demo-object2.xlsx",
      "classificationResultStatus": "COMPLETE",
      "sensitive": true
    },
    {
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket/amzn-s3-demo-object3.json",
      "classificationResultStatus": "COMPLETE",
      "sensitive": true
    },
    {
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket/amzn-s3-demo-object4.pdf",
      "classificationResultStatus": "COMPLETE",
      "sensitive": true
    },
    {
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket/amzn-s3-demo-object5.zip",
      "classificationResultStatus": "PARTIAL",
      "sensitive": true
    },
    {
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket/amzn-s3-demo-object6.vssx",
      "classificationResultStatus": "SKIPPED"
    }
  ]
}
```

```
}  
  ]  
}
```

Analisi dei risultati derivanti dal rilevamento automatico di dati sensibili

Quando Amazon Macie esegue il rilevamento automatico di dati sensibili, crea una ricerca di dati sensibili per ogni oggetto Amazon Simple Storage Service (Amazon S3) in cui trova dati sensibili. Un rilevamento di dati sensibili è un rapporto dettagliato di dati sensibili che Macie ha trovato in un oggetto S3. Un risultato non include i dati sensibili trovati da Macie. Fornisce invece informazioni che è possibile utilizzare per ulteriori indagini e correzioni, se necessario.

Ogni rilevamento di dati sensibili fornisce un indice di gravità e dettagli quali:

- La data e l'ora in cui Macie ha trovato i dati sensibili.
- La categoria e i tipi di dati sensibili trovati da Macie.
- Il numero di occorrenze di ogni tipo di dati sensibili rilevati da Macie.
- Come Macie ha trovato i dati sensibili, l'individuazione automatica dei dati sensibili o un lavoro di scoperta di dati sensibili.
- Il nome, le impostazioni di accesso pubblico, il tipo di crittografia e altre informazioni sul bucket S3 e sull'oggetto interessati.

A seconda del tipo di file o del formato di archiviazione dell'oggetto S3 interessato, i dettagli possono includere anche la posizione di ben 15 occorrenze dei dati sensibili trovati da Macie.

Macie archivia i dati sensibili rilevati per 90 giorni. Puoi accedervi utilizzando la console Amazon Macie o l'API Amazon Macie. Puoi anche monitorare ed elaborare i risultati utilizzando altre applicazioni, servizi e sistemi. Per ulteriori informazioni, consulta [Revisione e analisi dei risultati](#).

Per analizzare i risultati prodotti dal rilevamento automatico di dati sensibili

Per identificare e analizzare i risultati creati da Macie durante l'individuazione automatica di dati sensibili, puoi filtrare i risultati. Con i filtri, puoi utilizzare attributi specifici dei risultati per creare viste e interrogazioni personalizzate sui risultati. Per filtrare i risultati, puoi utilizzare la console Amazon Macie o inviare query a livello di codice utilizzando l'API Amazon Macie. Per ulteriori informazioni, consulta [Filtro dei risultati](#).

 Note

Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, solo l'amministratore Macie dell'organizzazione ha accesso diretto ai risultati prodotti dalla scoperta automatica di dati sensibili per gli account dell'organizzazione. Se hai un account membro e desideri esaminare i risultati relativi al tuo account, contatta l'amministratore di Macie.

Console

Segui questi passaggi per identificare e analizzare i risultati utilizzando la console Amazon Macie.

Per analizzare i risultati prodotti dalla scoperta automatizzata

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Per visualizzare i risultati che sono stati soppressi da una [regola di soppressione](#), modifica l'impostazione dello stato di ricerca. Scegliete Tutto per visualizzare sia i risultati soppressi che quelli non soppressi oppure scegliete Archiviato per visualizzare solo i risultati soppressi. Per nascondere nuovamente i risultati soppressi, scegliete Corrente.
4. Posizionate il cursore nella casella Criteri di filtro. Nell'elenco dei campi che appare, scegli Tipo di origine.

Questo campo specifica in che modo Macie ha trovato i dati sensibili che hanno prodotto un processo di individuazione, individuazione automatica di dati sensibili o un processo di scoperta di dati sensibili. Per trovare questo campo nell'elenco dei campi di filtro, puoi sfogliare l'elenco completo o inserire parte del nome del campo per restringere l'elenco dei campi.

5. Seleziona AUTOMATED_SENSITIVE_DATA_DISCOVERY come valore per il campo, quindi scegli Applica. Macie applica i criteri di filtro e aggiunge la condizione a un token di filtro nella casella Criteri di filtro.
6. Per affinare i risultati, aggiungi condizioni di filtro per campi aggiuntivi, ad esempio, Creato in per l'intervallo di tempo in cui è stato creato un risultato, nome del bucket S3 per il nome di un bucket interessato o Tipo di rilevamento dati sensibili per il tipo di sensibile che è stato rilevato e ha prodotto un risultato.

Se desideri utilizzare nuovamente questo set di condizioni in un secondo momento, puoi salvarlo come regola di filtro. Per fare ciò, scegli Salva regola nella casella Criteri di filtro. Quindi inserisci un nome e, facoltativamente, una descrizione per la regola. Al termine, scegli Salva.

API

Per identificare e analizzare i risultati a livello di codice, specifica i criteri di filtro nelle query inviate utilizzando [ListFindings](#) o il [GetFindingStatistics](#) funzionamento dell'API Amazon Macie. L'ListFindings operazione restituisce una matrice di risultati IDs, un ID per ogni risultato che corrisponde ai criteri di filtro. È quindi possibile utilizzarli IDs per recuperare i dettagli di ogni risultato. L'GetFindingStatistics operazione restituisce dati statistici aggregati su tutti i risultati che corrispondono ai criteri di filtro, raggruppati in base a un campo specificato nella richiesta. Per ulteriori informazioni sul filtraggio programmatico dei risultati, vedere. [Filtro dei risultati](#)

Nei criteri di filtro, includi una condizione per il campo. `originType` Questo campo specifica in che modo Macie ha trovato i dati sensibili che hanno prodotto un processo di individuazione, individuazione automatica di dati sensibili o un processo di scoperta di dati sensibili. Se l'individuazione automatica di dati sensibili ha prodotto un risultato, il valore per questo campo è. `AUTOMATED_SENSITIVE_DATA_DISCOVERY`

Per identificare e analizzare i risultati utilizzando AWS Command Line Interface (AWS CLI), esegui il comando [list-findings](#) o [get-finding-statistics](#). Negli esempi seguenti viene utilizzato il `list-findings` comando per recuperare i risultati relativi a tutti i risultati ad alta gravità generati dall'individuazione automatica di dati sensibili nel periodo corrente. IDs Regione AWS

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws macie2 list-findings ^
--finding-criteria={"criterion":{"classificationDetails.originType":{"eq
\":["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq\
":["High"]}}}
```

Dove:

- `classificationDetails.originType` specifica il nome JSON del campo del tipo di origine e:
 - `eq` specifica l'operatore `equals`.
 - `AUTOMATED_SENSITIVE_DATA_DISCOVERY` è un valore enumerato per il campo.
- `severity.description` specifica il nome JSON del campo Severity e:
 - `eq` specifica l'operatore `equals`.
 - `High` è un valore enumerato per il campo.

Se la richiesta ha esito positivo, Macie restituisce un array. `findingIds` L'array elenca l'identificatore univoco per ogni risultato che corrisponde ai criteri di filtro, come illustrato nell'esempio seguente.

```
{
  "findingIds": [
    "1f1c2d74db5d8caa76859ec52example",
    "6cfa9ac820dd6d55cad30d851example",
    "702a6fd8750e567d1a3a63138example",
    "826e94e2a820312f9f964cf60example",
    "274511c3fdcd87010a19a3a42example"
  ]
}
```

Se nessun risultato corrisponde ai criteri di filtro, Macie restituisce un array vuoto `findingIds`.

```
{
  "findingIds": []
}
```

Accesso ai risultati del rilevamento mediante il rilevamento automatico di dati sensibili

Quando Amazon Macie esegue il rilevamento automatico di dati sensibili, crea un record di analisi per ogni oggetto Amazon Simple Storage Service (Amazon S3) selezionato per l'analisi. Questi record, denominati risultati dell'individuazione di dati sensibili, registrano dettagli sull'analisi eseguita da Macie su singoli oggetti S3. Ciò include oggetti in cui Macie non trova dati sensibili e oggetti che Macie non può analizzare a causa di errori o problemi come le impostazioni delle autorizzazioni o

l'uso di un file o di un formato di archiviazione non supportato. I risultati dell'individuazione di dati sensibili forniscono record di analisi che possono essere utili per controlli o indagini sulla privacy e sulla protezione dei dati.

Se Macie trova dati sensibili in un oggetto S3, il risultato della scoperta dei dati sensibili fornisce informazioni sui dati sensibili trovati da Macie. Le informazioni includono gli stessi tipi di dettagli forniti da una ricerca di dati sensibili. Fornisce anche informazioni aggiuntive, come la posizione di ben 1.000 occorrenze di ogni tipo di dati sensibili trovati da Macie. Per esempio:

- Il numero di colonna e di riga per una cella o un campo in una cartella di lavoro di Microsoft Excel, un file CSV o un file TSV
- Il percorso di un campo o di una matrice in un file JSON o JSON Lines
- Il numero di riga di una riga in un file di testo non binario diverso da un file CSV, JSON, JSON Lines o TSV, ad esempio un file HTML, TXT o XML
- Il numero di pagina di una pagina in un file Adobe Portable Document Format (PDF)
- L'indice dei record e il percorso di un campo in un record in un contenitore di oggetti Apache Avro o in un file Apache Parquet

Se l'oggetto S3 interessato è un file di archivio, ad esempio un file.tar o.zip, il risultato della scoperta dei dati sensibili fornisce anche dati dettagliati sulla posizione delle occorrenze di dati sensibili nei singoli file che Macie ha estratto dall'archivio. Macie non include queste informazioni nelle rilevazioni di dati sensibili per i file di archivio. Per riportare i dati sulla posizione, i risultati del rilevamento dei dati sensibili utilizzano uno schema [JSON standardizzato](#).

Note

Come nel caso delle rilevazioni di dati sensibili, i risultati della scoperta di dati sensibili non includono i dati sensibili che Macie trova negli oggetti S3. Forniscono invece dettagli di analisi che possono essere utili per audit o indagini.

Macie archivia i risultati del rilevamento dei dati sensibili per 90 giorni. Non puoi accedervi direttamente dalla console Amazon Macie o con l'API Amazon Macie. Invece, configuri Macie per crittografarli e archivarli in un bucket S3. Il bucket può fungere da archivio definitivo a lungo termine per tutti i risultati della scoperta di dati sensibili. Per determinare dove si trova questo repository per il tuo account, scegli Risultati Discovery nel riquadro di navigazione

sulla console Amazon Macie. Per eseguire questa operazione a livello di codice, utilizza il [GetClassificationExportConfiguration](#) funzionamento dell'API Amazon Macie. Se non hai configurato questo repository per il tuo account, scopri come [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#) fare.

Dopo aver configurato Macie per archiviare i risultati del rilevamento dei dati sensibili in un bucket S3, Macie scrive i risultati nei file JSON Lines (.jsonl), quindi li crittografa e aggiunge tali file al bucket come file GNU Zip (.gz). Per il rilevamento automatico dei dati sensibili, Macie aggiunge i file a una cartella denominata nel bucket. `automated-sensitive-data-discovery` È quindi possibile, facoltativamente, accedere e interrogare i risultati in quella cartella. Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, Macie aggiunge i file alla `automated-sensitive-data-discovery` cartella nel bucket dell'account dell'amministratore di Macie.

I risultati del rilevamento dei dati sensibili aderiscono a uno schema standardizzato. Questo può aiutarti a interrogarli, monitorarli ed elaborarli utilizzando altre applicazioni, servizi e sistemi. Per un esempio dettagliato e istruttivo su come interrogare e utilizzare questi risultati, consulta il seguente post sul blog sulla AWS sicurezza: [Come interrogare e visualizzare i risultati del rilevamento dei dati sensibili di Macie con Amazon Athena](#) e Amazon. QuickSight Per esempi di query Athena da utilizzare per analizzare i risultati, visita il repository di [Amazon Macie](#) Results Analytics su. GitHub Questo repository fornisce anche istruzioni per configurare Athena per recuperare e decrittografare i risultati e script per creare tabelle per i risultati.

Valutazione della copertura automatizzata del rilevamento di dati sensibili

Man mano che l'individuazione automatica di dati sensibili per il tuo account o la tua organizzazione progredisce, Amazon Macie fornisce statistiche e dettagli per aiutarti a valutare e monitorare la copertura del tuo patrimonio di dati Amazon Simple Storage Service (Amazon S3). Con questi dati, puoi verificare lo stato del rilevamento automatico dei dati sensibili per il tuo patrimonio di dati in generale e per i singoli bucket S3 al suo interno. Puoi anche identificare i problemi che impedivano a Macie di analizzare gli oggetti in bucket specifici. Se risolvi i problemi, puoi aumentare la copertura dei dati di Amazon S3 durante i cicli di analisi successivi.

I dati di copertura forniscono un'istantanea dello stato attuale del rilevamento automatico dei dati sensibili per i bucket generici S3 nella versione attuale. Regione AWS Se sei l'amministratore Macie di un'organizzazione, questo include i bucket di proprietà dei tuoi account membro. Per ogni bucket, i dati indicano se si sono verificati problemi quando Macie ha tentato di analizzare gli oggetti nel bucket. Se si sono verificati problemi, i dati indicano la natura di ciascun problema e, in alcuni casi, il

numero di ricorrenze. I dati vengono aggiornati ogni giorno man mano che l'individuazione automatica dei dati sensibili avanza. Se Macie analizza o tenta di analizzare uno o più oggetti in un bucket durante un ciclo di analisi giornaliero, Macie aggiorna la copertura e altri dati per riflettere i risultati.

Per determinati tipi di problemi, puoi esaminare i dati in forma aggregata per tutti i bucket S3 per uso generico e, facoltativamente, approfondire per ulteriori dettagli su ciascun bucket. Ad esempio, i dati sulla copertura possono aiutarti a identificare rapidamente tutti i bucket a cui Macie non può accedere per il tuo account. I dati di copertura riportano anche i problemi a livello di oggetto che si sono verificati. Questi problemi, denominati errori di classificazione, impedivano a Macie di analizzare oggetti specifici in un bucket. Ad esempio, puoi determinare quanti oggetti Macie non è in grado di analizzare in un bucket perché gli oggetti sono crittografati con una chiave AWS Key Management Service (AWS KMS) che non è più disponibile.

Se utilizzi la console Amazon Macie per esaminare i dati di copertura, la visualizzazione dei dati include indicazioni per risolvere ogni tipo di problema. Gli argomenti successivi di questa sezione forniscono anche linee guida per la risoluzione di ogni tipo.

Argomenti

- [Revisione dei dati di copertura per l'individuazione automatica dei dati sensibili](#)
- [Risolvere i problemi di copertura per l'individuazione automatica dei dati sensibili](#)

Revisione dei dati di copertura per l'individuazione automatica dei dati sensibili

Per esaminare e valutare la copertura mediante il rilevamento automatico dei dati sensibili, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Sia la console che l'API forniscono dati che indicano lo stato attuale delle analisi per i bucket generici Amazon Simple Storage Service (Amazon S3) nell'attuale sistema. Regione AWS I dati includono informazioni sui problemi che creano lacune nelle analisi:

- Bucket a cui Macie non può accedere. Macie non può analizzare alcun oggetto in questi bucket. Le impostazioni delle autorizzazioni dei bucket impediscono a Macie di accedere ai bucket e agli oggetti dei bucket.
- Bucket che non memorizzano oggetti classificabili. Macie non può analizzare alcun oggetto in questi bucket. Tutti gli oggetti utilizzano classi di storage Amazon S3 che Macie non supporta oppure hanno estensioni di nomi di file per formati di file o di storage che Macie non supporta.
- Bucket che Macie non è ancora riuscito ad analizzare a causa di errori di classificazione a livello di oggetto. Macie ha tentato di analizzare uno o più oggetti in questi bucket. Tuttavia, Macie non è

riuscita ad analizzare gli oggetti a causa di problemi relativi alle impostazioni delle autorizzazioni a livello di oggetto, al contenuto degli oggetti o alle quote.

I dati di copertura vengono aggiornati ogni giorno man mano che l'individuazione automatica dei dati sensibili avanza. Se sei l'amministratore Macie di un'organizzazione, i dati includono informazioni per i bucket S3 di proprietà dei tuoi account membro.

Note

I dati di copertura non includono esplicitamente i risultati dei processi di rilevamento di dati sensibili creati ed eseguiti da te. Tuttavia, è probabile che la risoluzione dei problemi di copertura che influiscono sul rilevamento automatico dei dati sensibili aumenti anche la copertura dei lavori eseguiti successivamente. Per valutare la copertura di un lavoro, [esamina i risultati del lavoro](#). Se gli eventi registrati di un lavoro o altri risultati indicano problemi di copertura, le [linee guida sulla risoluzione per l'individuazione automatica dei dati sensibili](#) possono aiutarti a risolvere alcuni di questi problemi.

Per esaminare i dati di copertura per l'individuazione automatica dei dati sensibili

Per esaminare i dati di copertura per il rilevamento automatico dei dati sensibili, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Sulla console, una singola pagina fornisce una visualizzazione unificata dei dati di copertura per tutti i bucket S3 generici nella regione corrente. Ciò include un elenco dei problemi che si sono verificati di recente per ogni bucket. La pagina fornisce anche opzioni per la revisione di gruppi di dati per tipo di problema. Per tenere traccia dell'analisi dei problemi relativi a bucket specifici, puoi esportare i dati dalla pagina in un file con valori separati da virgole (CSV).

Console

Segui questi passaggi per esaminare i dati di copertura utilizzando la console Amazon Macie.

Per esaminare i dati di copertura

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli Copertura delle risorse.
3. Nella pagina Copertura delle risorse, scegli la scheda relativa al tipo di dati di copertura che desideri esaminare:

- **Tutti:** elenca tutti i bucket del tuo account. Per ogni bucket, il campo Problemi indica se i problemi hanno impedito a Macie di analizzare gli oggetti nel bucket. Se il valore di questo campo è Nessuno, Macie ha analizzato almeno uno degli oggetti del bucket o Macie non ha ancora tentato di analizzare nessuno degli oggetti del bucket. Se ci sono problemi, questo campo indica la natura dei problemi e come risolverli. Per gli errori di classificazione a livello di oggetto, potrebbe anche indicare (tra parentesi) il numero di occorrenze dell'errore.
 - **Accesso negato:** elenca i bucket a cui Macie non può accedere. Le impostazioni delle autorizzazioni per questi bucket impediscono a Macie di accedere ai bucket e agli oggetti dei bucket. Di conseguenza, Macie non può analizzare alcun oggetto nei bucket.
 - **Errore di classificazione:** elenca i bucket che Macie non ha ancora analizzato a causa di errori di classificazione a livello di oggetto, ovvero problemi con le impostazioni delle autorizzazioni a livello di oggetto, il contenuto degli oggetti o le quote. Per ogni bucket, il campo Problemi indica la natura di ogni tipo di errore che si è verificato e ha impedito a Macie di analizzare un oggetto nel bucket. Indica inoltre come correggere ogni tipo di errore. A seconda dell'errore, potrebbe anche indicare (tra parentesi) il numero di occorrenze dell'errore.
 - **Inclassificabile:** elenca i bucket che Macie non può analizzare perché non memorizzano oggetti classificabili. Tutti gli oggetti in questi bucket utilizzano classi di storage Amazon S3 non supportate o hanno estensioni di nomi di file per formati di file o di storage non supportati. Di conseguenza, Macie non può analizzare alcun oggetto nei bucket.
4. Per approfondire ed esaminare i dati di supporto per un bucket, scegli il nome del bucket. Quindi consulta il pannello dei dettagli per le statistiche e altre informazioni sul bucket.
 5. Per esportare la tabella in un file CSV, scegli Esporta in CSV nella parte superiore della pagina. Il file CSV risultante contiene un sottoinsieme di metadati per ogni bucket della tabella, per un massimo di 50.000 bucket. Il file include un campo Problemi di copertura. Il valore di questo campo indica se i problemi hanno impedito a Macie di analizzare gli oggetti nel bucket e, in caso affermativo, la natura dei problemi.

API

Per esaminare i dati di copertura in modo programmatico, specifica i criteri di filtro nelle query inviate utilizzando il [DescribeBuckets](#) funzionamento dell'API Amazon Macie. Questa operazione restituisce una serie di oggetti. Ogni oggetto contiene dati statistici e altre informazioni su un bucket S3 generico che corrisponde ai criteri di filtro.

Nei criteri di filtro, includi una condizione per il tipo di dati di copertura che desideri esaminare:

- Per identificare i bucket a cui Macie non può accedere a causa delle impostazioni delle autorizzazioni dei bucket, includi una condizione in cui il valore del campo sia uguale. `errorCode ACCESS_DENIED`
- Per identificare i bucket a cui Macie può accedere e che non ha ancora analizzato, includi le condizioni in cui il valore del campo è uguale e il valore del `sensitivityScore` campo non è uguale 50. `errorCode ACCESS_DENIED`
- Per identificare i bucket che Macie non può analizzare perché tutti gli oggetti dei bucket utilizzano classi o formati di archiviazione non supportati, includi condizioni in cui il valore del campo è uguale 0 e il valore del `classifiableSizeInBytes` campo è maggiore di. `sizeInBytes 0`
- Per identificare i bucket per i quali Macie ha analizzato almeno un oggetto, includi le condizioni in cui il valore del `sensitivityScore` campo rientra nell'intervallo da 1 a 99 ma non è uguale a. 50 Per includere anche i bucket in cui è stato assegnato manualmente il punteggio massimo, l'intervallo deve essere compreso tra 1 e 100.
- Per identificare i bucket che Macie non ha ancora analizzato a causa di errori di classificazione a livello di oggetto, includi una condizione in cui il valore del campo sia uguale. `sensitivityScore -1` Per esaminare quindi un'analisi dettagliata dei tipi e del numero di errori che si sono verificati per un determinato bucket, utilizza l'operazione. [GetResourceProfile](#)

[Se utilizzi AWS Command Line Interface \(AWS CLI\), specifica i criteri di filtro nelle query inviate eseguendo il comando `describe-buckets`.](#) Per esaminare un'analisi dettagliata dei tipi e del numero di errori che si sono verificati per un determinato bucket S3, se presenti, esegui il comando. [get-resource-profile](#)

Ad esempio, i seguenti AWS CLI comandi utilizzano criteri di filtro per recuperare i dettagli di tutti i bucket S3 a cui Macie non può accedere a causa delle impostazioni delle autorizzazioni dei bucket.

Questo esempio è formattato per Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

Questo esempio è formattato per Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"errorCode":{"eq":["ACCESS_DENIED\n"]}}
```

Se la richiesta ha esito positivo, Macie restituisce un array. `buckets` L'array contiene un oggetto per ogni bucket S3 presente nella versione corrente Regione AWS e che corrisponde ai criteri di filtro.

Se nessun bucket S3 soddisfa i criteri di filtro, Macie restituisce un array vuoto. `buckets`

```
{
  "buckets": []
}
```

Per ulteriori informazioni sulla specificazione dei criteri di filtro nelle query, inclusi esempi di criteri comuni, consulta. [Filtrare l'inventario dei bucket S3](#)

Per informazioni dettagliate che possono aiutarti a risolvere i problemi di copertura, consulta.

[Risolvere i problemi di copertura per l'individuazione automatica dei dati sensibili](#)

Risolvere i problemi di copertura per l'individuazione automatica dei dati sensibili

Man mano che la scoperta automatizzata di dati sensibili avanza ogni giorno, Amazon Macie fornisce statistiche e dettagli per aiutarti a valutare e monitorare la copertura del tuo patrimonio di dati Amazon Simple Storage Service (Amazon S3). [Esaminando i dati di copertura](#), puoi verificare lo stato del rilevamento automatico dei dati sensibili per il tuo patrimonio di dati complessivo e per i singoli bucket S3 al suo interno. Puoi anche identificare i problemi che impedivano a Macie di analizzare gli oggetti in bucket specifici. Se risolvi i problemi, puoi aumentare la copertura dei dati di Amazon S3 durante i cicli di analisi successivi.

Macie segnala diversi tipi di problemi che riducono la copertura dei dati di Amazon S3 mediante il rilevamento automatico di dati sensibili. Ciò include problemi a livello di bucket che impediscono a Macie di analizzare qualsiasi oggetto in un bucket S3. Include anche problemi a livello di oggetto. Questi problemi, denominati errori di classificazione, impedivano a Macie di analizzare oggetti specifici in un bucket. Le seguenti informazioni possono aiutarti a esaminare e risolvere i problemi.

Tipi e dettagli dei problemi

- [Accesso negato](#)

- [Errore di classificazione: contenuto non valido](#)
- [Errore di classificazione: crittografia non valida](#)
- [Errore di classificazione: chiave KMS non valida](#)
- [Errore di classificazione: autorizzazione negata](#)
- [Non classificabile](#)

Tip

Per analizzare gli errori di classificazione a livello di oggetto per un bucket S3, inizia esaminando l'elenco degli esempi di oggetti per il bucket. Questo elenco indica quali oggetti Macie ha analizzato o ha tentato di analizzare nel bucket, per un massimo di 100 oggetti. Per esaminare l'elenco sulla console Amazon Macie, scegli il bucket nella pagina dei bucket S3, quindi scegli la scheda Esempi di oggetti nel pannello dei dettagli. Per esaminare l'elenco a livello di codice, utilizza il [ListResourceProfileArtifacts](#) funzionamento dell'API Amazon Macie. Se lo stato dell'analisi di un oggetto è Skipped (SKIPPED), l'oggetto potrebbe aver causato l'errore.

Accesso negato

Questo problema indica che le impostazioni delle autorizzazioni di un bucket S3 impediscono a Macie di accedere al bucket e agli oggetti del bucket. Macie non può recuperare e analizzare alcun oggetto nel bucket.

Dettagli

La causa più comune di questo tipo di problema è una policy restrittiva sui bucket. Una bucket policy è una policy basata sulle risorse AWS Identity and Access Management (IAM) che specifica quali azioni un principale (utente, account, servizio o altra entità) può eseguire su un bucket S3 e le condizioni in base alle quali un principale può eseguire tali azioni. Una policy bucket restrittiva utilizza Deny dichiarazioni Allow o dichiarazioni esplicite che concedono o limitano l'accesso ai dati di un bucket in base a condizioni specifiche. Ad esempio, una policy bucket potrebbe contenere un'Denyistruzione Allow or che nega l'accesso a un bucket a meno che non vengano utilizzati indirizzi IP di origine specifici per accedere al bucket.

Se la policy del bucket per un bucket S3 contiene un'Denyistruzione esplicita con una o più condizioni, a Macie potrebbe non essere consentito di recuperare e analizzare gli oggetti del

bucket per rilevare dati sensibili. Macie può fornire solo un sottoinsieme di informazioni sul bucket, come il nome e la data di creazione del bucket.

Linee guida per la riparazione

Per risolvere questo problema, aggiorna la policy del bucket S3. Assicurati che la policy consenta a Macie di accedere al bucket e agli oggetti del bucket. Per consentire questo accesso, aggiungi una condizione per il ruolo collegato al servizio Macie () alla policy.

`AWSServiceRoleForAmazonMacie` La condizione dovrebbe escludere che il ruolo collegato al servizio Macie corrisponda alla restrizione della policy. Deny Può farlo utilizzando la chiave di contesto della condizione `aws:PrincipalArn` globale e l'Amazon Resource Name (ARN) del ruolo collegato al servizio Macie per il tuo account.

Se aggiorni la policy del bucket e Macie ottiene l'accesso al bucket S3, Macie rileverà la modifica. Quando ciò accade, Macie aggiornerà le statistiche, i dati di inventario e altre informazioni che fornisce sui dati di Amazon S3. Inoltre, gli oggetti del bucket avranno una priorità più elevata per l'analisi durante un ciclo di analisi successivo.

Riferimento aggiuntivo

Per ulteriori informazioni sull'aggiornamento di una policy sui bucket S3 per consentire a Macie di accedere a un bucket, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#). Per informazioni sull'utilizzo delle policy dei bucket per controllare l'accesso ai bucket, consulta le [politiche dei bucket](#) e il modo in cui [Amazon S3 autorizza una richiesta nella Guida per l'utente di Amazon Simple](#) Storage Service.

Errore di classificazione: contenuto non valido

Questo tipo di errore di classificazione si verifica se Macie tenta di analizzare un oggetto in un bucket S3 e l'oggetto presenta un formato errato o l'oggetto contiene contenuti che superano la quota di rilevamento di dati sensibili. Macie non può analizzare l'oggetto.

Dettagli

Questo errore si verifica in genere perché un oggetto S3 è un file malformato o danneggiato. Di conseguenza, Macie non può analizzare e analizzare tutti i dati del file.

Questo errore può verificarsi anche se l'analisi di un oggetto S3 supera la quota di rilevamento di dati sensibili per un singolo file. Ad esempio, la dimensione di archiviazione dell'oggetto supera la quota di dimensione per quel tipo di file.

In entrambi i casi, Macie non può completare l'analisi dell'oggetto S3 e lo stato dell'analisi dell'oggetto è Skipped (). SKIPPED

Linee guida per la riparazione

Per indagare su questo errore, scaricate l'oggetto S3 e controllate la formattazione e il contenuto del file. Valuta anche il contenuto del file rispetto alle quote di Macie per l'individuazione di dati sensibili.

Se non correggi questo errore, Macie proverà ad analizzare altri oggetti nel bucket S3. Se Macie analizza correttamente un altro oggetto, Macie aggiornerà i dati di copertura e le altre informazioni che fornisce sul bucket.

Riferimento aggiuntivo

Per un elenco delle quote di rilevamento dei dati sensibili, incluse le quote per determinati tipi di file, vedere [Quote per Macie](#). Per informazioni su come Macie aggiorna i punteggi di sensibilità e altre informazioni che fornisce sui bucket S3, consulta [Come funziona l'individuazione automatica dei dati sensibili](#).

Errore di classificazione: crittografia non valida

Questo tipo di errore di classificazione si verifica se Macie tenta di analizzare un oggetto in un bucket S3 e l'oggetto viene crittografato con una chiave fornita dal cliente. L'oggetto utilizza la crittografia SSE-C, il che significa che Macie non può recuperare e analizzare l'oggetto.

Dettagli

Amazon S3 supporta diverse opzioni di crittografia per oggetti S3. Per la maggior parte di queste opzioni, Macie può decrittografare un oggetto utilizzando il ruolo collegato al servizio Macie per il tuo account. Tuttavia, ciò dipende dal tipo di crittografia utilizzato.

Affinché Macie possa decrittografare un oggetto S3, l'oggetto deve essere crittografato con una chiave a cui Macie possa accedere e che possa usare. Se un oggetto è crittografato con una chiave fornita dal cliente, Macie non può fornire il materiale chiave necessario per recuperare l'oggetto da Amazon S3. Di conseguenza, Macie non può analizzare l'oggetto e lo stato dell'analisi dell'oggetto è Skipped (). SKIPPED

Guida alla riparazione

Per correggere questo errore, crittografa gli oggetti S3 con chiavi gestite o chiavi () di Amazon S3. AWS Key Management Service AWS KMS Se preferisci utilizzare AWS KMS le chiavi, le chiavi possono essere chiavi KMS AWS gestite o chiavi KMS gestite dal cliente che Macie può utilizzare.

Per crittografare gli oggetti S3 esistenti con chiavi accessibili e utilizzabili da Macie, puoi modificare le impostazioni di crittografia degli oggetti. Per crittografare nuovi oggetti con chiavi accessibili e utilizzabili da Macie, modifica le impostazioni di crittografia predefinite per il bucket S3. Assicurati inoltre che la politica del bucket non richieda la crittografia di nuovi oggetti con una chiave fornita dal cliente.

Se non correggi questo errore, Macie proverà ad analizzare altri oggetti nel bucket S3. Se Macie analizza correttamente un altro oggetto, Macie aggiornerà i dati di copertura e le altre informazioni che fornisce sul bucket.

Riferimento aggiuntivo

Per informazioni sui requisiti e sulle opzioni per l'utilizzo di Macie per analizzare oggetti S3 crittografati, consulta [Analisi di oggetti Amazon S3 crittografati](#) Per informazioni sulle opzioni e le impostazioni di crittografia per i bucket S3, consulta [Protezione dei dati con crittografia e Impostazione del comportamento predefinito di crittografia lato server per i bucket S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

Errore di classificazione: chiave KMS non valida

Questo tipo di errore di classificazione si verifica se Macie tenta di analizzare un oggetto in un bucket S3 e l'oggetto viene crittografato con una chiave AWS Key Management Service (AWS KMS) che non è più disponibile. Macie non può recuperare e analizzare l'oggetto.

Dettagli

AWS KMS offre opzioni per la disabilitazione e l'eliminazione della gestione da parte del cliente. AWS KMS keys Se un oggetto S3 è crittografato con una chiave KMS che è disabilitata, è programmata per l'eliminazione o è stata eliminata, Macie non può recuperare e decrittografare l'oggetto. Di conseguenza, Macie non può analizzare l'oggetto e lo stato dell'analisi dell'oggetto è Skipped (). SKIPPED Affinché Macie analizzi un oggetto crittografato, l'oggetto deve essere crittografato con una chiave a cui Macie possa accedere e che possa usare.

Linee guida per la riparazione

Per correggere questo errore, riattiva la chiave applicabile AWS KMS key o annulla l'eliminazione pianificata della chiave, a seconda dello stato corrente della chiave. Se la chiave applicabile è già stata eliminata, questo errore non può essere corretto.

Per determinare quale oggetto AWS KMS key è stato utilizzato per crittografare un oggetto S3, puoi iniziare utilizzando Macie per rivedere le impostazioni di crittografia lato server per il bucket S3. Se le impostazioni di crittografia predefinite per il bucket sono configurate per utilizzare una chiave KMS, i dettagli del bucket indicano quale chiave viene utilizzata. È quindi possibile controllare lo stato di quella chiave. In alternativa, puoi utilizzare Amazon S3 per rivedere le impostazioni di crittografia per il bucket e i singoli oggetti nel bucket.

Se non correggi questo errore, Macie proverà ad analizzare altri oggetti nel bucket S3. Se Macie analizza correttamente un altro oggetto, Macie aggiornerà i dati di copertura e le altre informazioni che fornisce sul bucket.

Riferimento aggiuntivo

Per informazioni sull'utilizzo di Macie per rivedere le impostazioni di crittografia lato server per un bucket S3, consulta [Analisi dei dettagli dei bucket S3](#) [Per informazioni sulla riattivazione AWS KMS key o sull'annullamento dell'eliminazione pianificata di una chiave, consulta Abilitazione e disabilitazione delle chiavi e Eliminazione delle chiavi nella Guida per gli sviluppatori.](#) [AWS Key Management Service](#)

Errore di classificazione: autorizzazione negata

Questo tipo di errore di classificazione si verifica se Macie tenta di analizzare un oggetto in un bucket S3 e Macie non riesce a recuperare o decrittografare l'oggetto a causa delle impostazioni delle autorizzazioni per l'oggetto o delle impostazioni delle autorizzazioni per la chiave utilizzata per crittografare l'oggetto. Macie non può recuperare e analizzare l'oggetto.

Dettagli

Questo errore si verifica in genere perché un oggetto S3 è crittografato con una chiave gestita dal cliente AWS Key Management Service (AWS KMS) che Macie non può utilizzare. Se un oggetto è crittografato con una soluzione gestita dal cliente AWS KMS key, la policy della chiave deve consentire a Macie di decrittografare i dati utilizzando la chiave.

Questo errore può verificarsi anche se le impostazioni delle autorizzazioni di Amazon S3 impediscono a Macie di recuperare un oggetto S3. La policy del bucket per il bucket S3 potrebbe

limitare l'accesso a oggetti bucket specifici o consentire solo a determinati soggetti (utenti, account, servizi o altre entità) di accedere agli oggetti. Oppure la lista di controllo degli accessi (ACL) di un oggetto potrebbe limitare l'accesso all'oggetto. Di conseguenza, a Macie potrebbe non essere consentito di accedere all'oggetto.

In nessuno dei casi precedenti, Macie non è in grado di recuperare e analizzare l'oggetto e lo stato dell'analisi dell'oggetto è Ignorato (). SKIPPED

Linee guida per la riparazione

Per correggere questo errore, stabilisci se l'oggetto S3 è crittografato con un servizio gestito dal cliente. AWS KMS key In caso affermativo, assicurati che la politica della chiave consenta al ruolo collegato al servizio Macie (`AWSServiceRoleForAmazonMacie`) di decrittografare i dati con la chiave. Il modo in cui consenti questo accesso dipende dal fatto che l'account proprietario possieda AWS KMS key anche il bucket S3 che memorizza l'oggetto. Se lo stesso account possiede la chiave KMS e il bucket, un utente dell'account deve aggiornare la politica della chiave. Se un account possiede la chiave KMS e un altro account possiede il bucket, un utente dell'account proprietario della chiave deve consentire l'accesso alla chiave da più account.

Tip

Puoi generare automaticamente un elenco di tutti i clienti gestiti a AWS KMS keys cui Macie deve accedere per analizzare gli oggetti nei bucket S3 del tuo account. A tale scopo, esegui lo script AWS KMS Permission Analyzer, disponibile nel repository [Amazon Macie Scripts](#) su GitHub. Lo script può anche generare uno script aggiuntivo di comandi (). AWS Command Line Interface AWS CLI Facoltativamente, puoi eseguire questi comandi per aggiornare le impostazioni e le politiche di configurazione richieste per le chiavi KMS che specifichi.

Se a Macie è già consentito utilizzare l'oggetto applicabile AWS KMS key o se l'oggetto S3 non è crittografato con una chiave KMS gestita dal cliente, assicurati che la politica del bucket consenta a Macie di accedere all'oggetto. Verifica inoltre che l'ACL dell'oggetto consenta a Macie di leggere i dati e i metadati dell'oggetto.

Per quanto riguarda la policy bucket, puoi consentire questo accesso aggiungendo una condizione per il ruolo collegato al servizio Macie alla policy. La condizione dovrebbe escludere che il ruolo collegato al servizio Macie corrisponda alla restrizione della policy. Deny Può farlo

utilizzando la chiave di contesto della condizione `aws:PrincipalArn` globale e l'Amazon Resource Name (ARN) del ruolo collegato al servizio Macie per il tuo account.

Per quanto riguarda l'ACL dell'oggetto, puoi consentire questo accesso collaborando con il proprietario dell'oggetto per aggiungere il tuo nome Account AWS come beneficiario con le autorizzazioni per l'oggetto. READ Macie può quindi utilizzare il ruolo collegato al servizio per il tuo account per recuperare e analizzare l'oggetto. Valuta anche la possibilità di modificare le impostazioni di proprietà dell'oggetto per il bucket. È possibile utilizzare queste impostazioni ACLs per disabilitare tutti gli oggetti nel bucket e concedere le autorizzazioni di proprietà all'account proprietario del bucket.

Se non correggi questo errore, Macie proverà ad analizzare altri oggetti nel bucket S3. Se Macie analizza correttamente un altro oggetto, Macie aggiornerà i dati di copertura e le altre informazioni che fornisce sul bucket.

Riferimento aggiuntivo

Per ulteriori informazioni su come consentire a Macie di decrittografare i dati con un servizio gestito AWS KMS key dal cliente, consulta [Consentire a Macie di utilizzare un servizio gestito dal cliente AWS KMS key](#). Per informazioni sull'aggiornamento di una policy relativa ai bucket S3 per consentire a Macie di accedere a un bucket, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Per informazioni sull'aggiornamento di una politica chiave, consulta [Modifica di una politica chiave](#) nella Guida per gli sviluppatori AWS Key Management Service. Per informazioni sull'utilizzo della crittografia gestita dal cliente AWS KMS keys per gli oggetti S3, consulta [Using server-side encryption with keys AWS KMS nella Amazon Simple Storage Service User Guide](#).

Per informazioni sull'utilizzo delle policy dei bucket per controllare l'accesso ai bucket S3, consulta [Controllo degli accessi](#) e Come [Amazon S3 autorizza una richiesta nella Guida per l'utente di Amazon Simple Storage Service](#). Per informazioni sull'utilizzo ACLs delle impostazioni di proprietà degli oggetti per controllare l'accesso agli oggetti S3, consulta [Gestione dell'accesso ACLs e controllo della proprietà degli oggetti e disattivazione del bucket nella ACLs Guida per l'utente di Amazon Simple Storage Service](#).

Non classificabile

Questo problema indica che tutti gli oggetti in un bucket S3 vengono archiviati utilizzando classi di storage Amazon S3 non supportate o formati di file o storage non supportati. Macie non è in grado di analizzare alcun oggetto nel bucket.

Dettagli

Per essere idoneo alla selezione e all'analisi, un oggetto S3 deve utilizzare una classe di storage Amazon S3 supportata da Macie. L'oggetto deve inoltre avere un'estensione del nome di file per un formato di file o di archiviazione supportato da Macie. Se un oggetto non soddisfa questi criteri, viene trattato come un oggetto inclassificabile. Macie non tenta di recuperare o analizzare dati in oggetti inclassificabili.

Se tutti gli oggetti in un bucket S3 sono oggetti inclassificabili, l'intero bucket è un bucket inclassificabile. Macie non può eseguire il rilevamento automatico dei dati sensibili per il bucket.

Linee guida per la riparazione

Per risolvere questo problema, esamina le regole di configurazione del ciclo di vita e altre impostazioni che determinano quali classi di storage vengono utilizzate per archiviare gli oggetti nel bucket S3. Valuta la possibilità di modificare queste impostazioni per utilizzare le classi di archiviazione supportate da Macie. Puoi anche modificare la classe di archiviazione degli oggetti esistenti nel bucket.

Valuta anche i formati di file e di archiviazione degli oggetti esistenti nel bucket S3. Per analizzare gli oggetti, prendi in considerazione la possibilità di trasferire i dati, temporaneamente o permanentemente, su nuovi oggetti che utilizzano un formato supportato.

Se gli oggetti vengono aggiunti al bucket S3 e utilizzano una classe e un formato di archiviazione supportati, Macie rileverà gli oggetti la prossima volta che valuterà l'inventario del bucket. Quando ciò accade, Macie smetterà di segnalare che il bucket non è classificabile nelle statistiche, nei dati di copertura e in altre informazioni che fornisce sui dati di Amazon S3. Inoltre, i nuovi oggetti avranno una priorità più elevata per l'analisi durante un ciclo di analisi successivo.

Riferimento aggiuntivo

Per informazioni sulle classi di storage di Amazon S3 e sui formati di file e storage supportati da Macie, consulta [Classi e formati di storage supportati](#). Per informazioni sulle regole di configurazione del ciclo di vita e sulle opzioni delle classi di storage offerte da Amazon S3, consulta [Managing your storage lifecycle](#) e [Using Amazon S3 Storage Classes nella Amazon Simple Storage Service User Guide](#).

Regolazione dei punteggi di sensibilità per i bucket S3

Mentre esami e valuti statistiche, dati e altri risultati del rilevamento automatico di dati sensibili, in alcuni casi potresti voler perfezionare le valutazioni di sensibilità dei tuoi bucket Amazon Simple

Storage Service (Amazon S3). Potresti anche voler acquisire i risultati delle indagini eseguite da te o dalla tua organizzazione per bucket specifici. Se sei l'amministratore di Amazon Macie di un'organizzazione o disponi di un account Macie autonomo, puoi apportare queste modifiche regolando il punteggio di sensibilità e altre impostazioni per i singoli bucket. Se disponi di un account membro in un'organizzazione, collabora con il tuo amministratore Macie per modificare le impostazioni dei bucket di tua proprietà. Solo l'amministratore Macie della tua organizzazione può modificare queste impostazioni per i tuoi bucket.

Se sei un amministratore Macie o disponi di un account Macie indipendente, puoi regolare il punteggio di sensibilità per un bucket S3 nei seguenti modi:

- **Assegna un punteggio di sensibilità:** per impostazione predefinita, Macie calcola automaticamente il punteggio di sensibilità di un bucket. Il punteggio si basa principalmente sulla quantità di dati sensibili che Macie ha trovato in un bucket e sulla quantità di dati che Macie ha analizzato in un bucket. Per ulteriori informazioni, consulta [Punteggio di sensibilità per i bucket S3](#).

Puoi sovrascrivere il punteggio calcolato di un bucket e assegnare manualmente il punteggio massimo (100), che applica anche l'etichetta Sensitive al bucket. Se lo fai, Macie continua a eseguire il rilevamento automatico dei dati sensibili per il bucket. Tuttavia, le analisi successive non influiscono sul punteggio del bucket. Per calcolare nuovamente il punteggio automaticamente, modifica nuovamente l'impostazione.

- **Escludi o includi i tipi di dati sensibili nel punteggio di sensibilità:** se viene calcolato automaticamente, il punteggio di sensibilità di un bucket si basa in parte sulla quantità di dati sensibili che Macie ha trovato nel bucket. Ciò deriva principalmente dalla natura e dal numero di tipi di dati sensibili rilevati da Macie e dal numero di occorrenze di ciascun tipo. Per impostazione predefinita, Macie include le occorrenze di tutti i tipi di dati sensibili quando calcola il punteggio di un bucket.

Puoi modificare il calcolo escludendo o includendo tipi specifici di dati sensibili nel punteggio di un bucket. Ad esempio, se Macie ha rilevato indirizzi postali in un bucket e tu stabilisci che ciò è accettabile, puoi escludere tutte le occorrenze degli indirizzi postali dal punteggio del bucket. Se escludi un tipo di dati sensibile, Macie continua a ispezionare il bucket per quel tipo di dati e a segnalare le occorrenze che rileva. Tuttavia, tali ricorrenze non influiscono sul punteggio del bucket. Per includere nuovamente un tipo di dati sensibili nella partitura, modifica nuovamente l'impostazione.

Puoi anche escludere un bucket S3 dalle analisi successive. Se escludi un bucket, le statistiche e i dettagli esistenti sul rilevamento dei dati sensibili relativi al bucket persistono. Ad esempio, l'attuale punteggio di sensibilità del bucket rimane invariato. Tuttavia, Macie interrompe l'analisi degli oggetti nel bucket quando esegue il rilevamento automatico dei dati sensibili. Dopo aver escluso un bucket, puoi includerlo nuovamente in un secondo momento.

Se modifichi un'impostazione che influisce sul punteggio di sensibilità di un bucket S3, Macie inizia immediatamente a ricalcolare il punteggio. Macie aggiorna anche le statistiche pertinenti e altre informazioni che fornisce sul bucket e sui dati complessivi di Amazon S3. Ad esempio, se assegni il punteggio massimo a un bucket, Macie incrementa il numero di bucket sensibili nelle statistiche aggregate.

Per regolare il punteggio di sensibilità o altre impostazioni per un bucket S3

Per regolare il punteggio di sensibilità o altre impostazioni per un bucket S3, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per regolare il punteggio di sensibilità o un'impostazione per un bucket S3 utilizzando la console Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione, scegli bucket S3. La pagina dei bucket S3 mostra l'inventario dei bucket.

Per impostazione predefinita, la pagina non mostra i dati relativi ai bucket attualmente esclusi dalle analisi. Se sei l'amministratore Macie di un'organizzazione, inoltre, non vengono visualizzati i dati degli account per i quali l'individuazione automatica di dati sensibili è attualmente disabilitata. Per visualizzare questi dati, scegli X nel filtro È monitorato dal token del filtro di rilevamento automatico sotto la casella del filtro.

3. Scegli il bucket S3 con un'impostazione da regolare. Puoi scegliere il bucket utilizzando la visualizzazione tabellare



o la mappa interattiva ().



4. Nel pannello dei dettagli, effettuate una delle seguenti operazioni:

- Per ignorare il punteggio di sensibilità calcolato e assegnare manualmente un punteggio, attiva Assegna punteggio massimo ().



Questo modifica il punteggio del bucket a 100 e applica l'etichetta Sensitive al bucket.

- Per assegnare un punteggio di sensibilità che Macie calcola automaticamente, disattiva Assegna punteggio massimo ().



- Per escludere o includere tipi specifici di dati sensibili nel punteggio di sensibilità, scegli la scheda Sensibilità. Nella tabella Rilevamenti, seleziona la casella di controllo relativa al tipo di dati sensibili da escludere o includere. Quindi, nel menu Azioni, scegli Escludi dalla partitura per escludere il tipo o scegli Includi nel punteggio per includere il tipo.

Nella tabella, il campo Tipo di dati sensibili specifica l'identificatore di dati gestito o l'identificatore di dati personalizzato che ha rilevato i dati. Per un identificatore di dati gestito, si tratta di un identificatore univoco (ID) che descrive il tipo di dati sensibili che l'identificatore è progettato per rilevare, ad esempio USA_PASSPORT_NUMBER per i numeri di passaporto statunitensi. Per informazioni dettagliate su ciascun identificatore di dati gestito, vedere. [Utilizzo di identificatori di dati gestiti](#)

- Per escludere il bucket dalle analisi successive, attiva Escludi dal rilevamento automatico ().



- Per includere il bucket nelle analisi successive, se lo hai escluso in precedenza, disattiva Escludi dal rilevamento automatico ().



API

Per regolare il punteggio di sensibilità o un'impostazione per un bucket S3 a livello di codice, hai diverse opzioni. L'opzione appropriata dipende da cosa vuoi regolare.

Assegna un punteggio di sensibilità

Per assegnare un punteggio di sensibilità a un bucket S3, usa l'operazione.

[UpdateResourceProfile](#) Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) del bucket. Per il `sensitivityScoreOverride` parametro, esegui una delle seguenti operazioni:

- Per sostituire il punteggio calcolato e assegnare manualmente il punteggio massimo, specificare. 100
- Per assegnare un punteggio che Macie calcola automaticamente, ometti il parametro. Se questo parametro è nullo, Macie calcola e assegna il punteggio.

Se stai usando il AWS Command Line Interface (AWS CLI), esegui il [update-resource-profile](#) comando per assegnare un punteggio di sensibilità a un bucket S3. Nella tua richiesta, usa il `resource-arn` parametro per specificare l'ARN del bucket. Omettete o utilizzate il `sensitivity-score-override` parametro per specificare il punteggio da assegnare.

Se la richiesta ha esito positivo, Macie assegna il punteggio specificato e restituisce una risposta vuota.

Escludi o includi i tipi di dati sensibili nel punteggio di sensibilità

Per escludere o includere i tipi di dati sensibili nel punteggio di sensibilità di un bucket S3, usa l'[UpdateResourceProfileDetections](#) operazione. Quando usi questa operazione, sovrascrivi le impostazioni correnti di inclusione ed esclusione per il punteggio di un bucket. Pertanto, è una buona idea recuperare prima le impostazioni correnti e determinare quali conservare. Per recuperare le impostazioni correnti, utilizzate l'[ListResourceProfileDetections](#) operazione.

Quando sei pronto per aggiornare le impostazioni, usa il `resourceArn` parametro per specificare l'ARN del bucket S3. Per il `suppressDataIdentifiers` parametro, esegui una delle seguenti operazioni:

- Per escludere un tipo di dati sensibile dal punteggio del bucket, utilizzate il `type` parametro per specificare il tipo di identificatore di dati che ha rilevato i dati, un identificatore di dati gestito (MANAGED) o un identificatore di dati personalizzato (). `CUSTOM` Utilizzate il `id` parametro per specificare l'identificatore univoco per l'identificatore di dati gestito o personalizzato che ha rilevato i dati.
- Per includere un tipo di dati sensibile nel punteggio del bucket, non specificare alcun dettaglio per l'identificatore di dati gestito o personalizzato che ha rilevato i dati.
- Per includere tutti i tipi di dati sensibili nel punteggio del bucket, non specificare alcun valore. Se il valore del `suppressDataIdentifiers` parametro è nullo (vuoto), Macie include tutti i tipi di rilevamenti quando calcola il punteggio.

Se utilizzi il AWS CLI, esegui il [update-resource-profile-detections](#) comando per escludere o includere i tipi di dati sensibili nel punteggio di sensibilità per un bucket S3. Utilizzate il `resource-arn` parametro per specificare l'ARN del bucket. Utilizzate il `suppress-data-identifiers` parametro per specificare quali tipi di dati sensibili escludere o includere nel

punteggio del bucket. Per recuperare e rivedere prima le impostazioni correnti per il bucket, esegui il comando. [list-resource-profile-detections](#)

Se la tua richiesta ha esito positivo, Macie aggiorna le impostazioni e restituisce una risposta vuota.

Escludi o includi un bucket S3 nelle analisi

Per escludere o includere successivamente un bucket S3 nelle analisi, utilizza l'operazione. [UpdateClassificationScope](#) Oppure, se utilizzi il AWS CLI, esegui il comando. [update-classification-scope](#) Per ulteriori dettagli ed esempi, vedere [Esclusione o inclusione dei bucket S3 nel rilevamento automatico dei dati sensibili](#).

Gli esempi seguenti mostrano come utilizzare per regolare le impostazioni individuali per un bucket S3. AWS CLI Questo primo esempio assegna manualmente il punteggio di sensibilità massimo (100) a un bucket. Sostituisce il punteggio calcolato dal bucket.

```
$ aws macie2 update-resource-profile --resource-arn arn:aws:s3:::amzn-s3-demo-bucket
--sensitivity-score-override 100
```

arn:aws:s3:::amzn-s3-demo-bucketDov'è l'ARN del bucket S3.

L'esempio successivo modifica il punteggio di sensibilità di un bucket S3 in un punteggio che Macie calcola automaticamente. Attualmente il bucket ha un punteggio assegnato manualmente che sostituisce il punteggio calcolato. Questo esempio rimuove tale override omettendo il `sensitivity-score-override` parametro dalla richiesta.

```
$ aws macie2 update-resource-profile --resource-arn arn:aws:s3:::amzn-s3-demo-bucket2
```

arn:aws:s3:::amzn-s3-demo-bucket2Dov'è l'ARN del bucket S3.

Gli esempi seguenti escludono particolari tipi di dati sensibili dal punteggio di sensibilità di un bucket S3. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws macie2 update-resource-profile-detections \
--resource-arn arn:aws:s3:::amzn-s3-demo-bucket3 \
--suppress-data-identifiers '["type":"MANAGED","id":"ADDRESS"],
{"type":"CUSTOM","id":"3293a69d-4a1e-4a07-8715-208ddexample"]'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 update-resource-profile-detections ^  
--resource-arn arn:aws:s3:::amzn-s3-demo-bucket3 ^  
--suppress-data-identifiers=[{"type\":"MANAGED\","id\":"ADDRESS\"}, {"type\":"  
"CUSTOM\","id\":"3293a69d-4a1e-4a07-8715-208ddexample\"}]
```

Dove:

- *arn:aws:s3:::amzn-s3-demo-bucket3* è l'ARN del bucket S3.
- *ADDRESS* è l'identificatore univoco dell'identificatore di dati gestito che ha rilevato un tipo di dati sensibili da escludere (indirizzi postali).
- *3293a69d-4a1e-4a07-8715-208ddexample* è l'identificatore univoco dell'identificatore di dati personalizzato che ha rilevato un tipo di dati sensibili da escludere.

La prossima serie di esempi include in seguito tutti i tipi di dati sensibili nel punteggio di sensibilità per il bucket S3. Sovrascrive le impostazioni di esclusione correnti per il bucket specificando un valore vuoto (nullo) per il parametro. `suppress-data-identifiers` Per Linux, macOS o Unix:

```
$ aws macie2 update-resource-profile-detections --resource-arn arn:aws:s3:::amzn-s3-  
demo-bucket3 --suppress-data-identifiers '[]'
```

Per Microsoft Windows:

```
C:\> aws macie2 update-resource-profile-detections --resource-arn arn:aws:s3:::amzn-  
s3-demo-bucket3 --suppress-data-identifiers=[]
```

arn:aws:s3:::amzn-s3-demo-bucket3 Dov'è l'ARN del bucket S3.

Punteggio di sensibilità per i bucket S3

Se il rilevamento automatico dei dati sensibili è abilitato, Amazon Macie calcola e assegna automaticamente un punteggio di sensibilità a ogni bucket generico di Amazon Simple Storage Service (Amazon S3) che monitora e analizza per un account o un'organizzazione. Un punteggio di sensibilità è una rappresentazione quantitativa della quantità di dati sensibili che un bucket S3

potrebbe contenere. In base a quel punteggio, Macie assegna anche un'etichetta di sensibilità a ciascun bucket. Un'etichetta di sensibilità è una rappresentazione qualitativa del punteggio di sensibilità di un bucket. Questi valori possono fungere da punti di riferimento per determinare dove potrebbero risiedere i dati sensibili nel tuo patrimonio di dati Amazon S3 e identificare e monitorare i potenziali rischi per la sicurezza di tali dati.

Per impostazione predefinita, il punteggio di sensibilità e l'etichetta di un bucket S3 riflettono i risultati delle attività automatizzate di rilevamento di dati sensibili che Macie ha svolto finora per quel bucket. Non riflettono i risultati dei processi di rilevamento di dati sensibili che crei ed esegui. Inoltre, né il punteggio né l'etichetta implicano o indicano in altro modo la criticità o l'importanza che un bucket o gli oggetti in esso contenuti potrebbero avere per te o la tua organizzazione. Tuttavia, puoi sovrascrivere il punteggio calcolato di un bucket assegnando manualmente il punteggio massimo (100) al bucket. Questo assegna anche l'etichetta *Sensitive* al bucket. Per sostituire un punteggio calcolato, devi essere l'amministratore Macie dell'account proprietario del bucket o avere un account Macie indipendente.

Argomenti

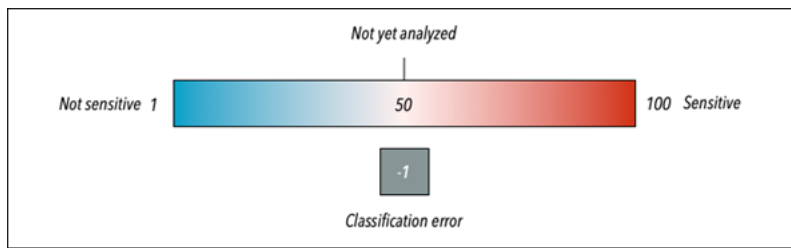
- [Dimensioni e intervalli del punteggio di sensibilità](#)
- [Controllo dei punteggi di sensibilità](#)

Dimensioni e intervalli del punteggio di sensibilità

Se calcolato da Amazon Macie, il punteggio di sensibilità di un bucket S3 è una misura quantitativa dell'intersezione di due dimensioni principali:

- La quantità di dati sensibili che Macie ha trovato nel bucket. Ciò deriva principalmente dalla natura e dal numero di tipi di dati sensibili che Macie ha trovato nel bucket e dal numero di occorrenze di ciascun tipo.
- La quantità di dati che Macie ha analizzato nel bucket. Ciò deriva principalmente dal numero di oggetti unici che Macie ha analizzato nel bucket rispetto al numero totale di oggetti unici nel bucket.

Il punteggio di sensibilità di un bucket S3 determina anche quale etichetta di sensibilità Macie assegna al bucket. L'etichetta di sensibilità è una rappresentazione qualitativa del punteggio, ad esempio *Sensibile* o *Non sensibile*. Sulla console Amazon Macie, il punteggio di sensibilità di un bucket determina anche il colore utilizzato da Macie per rappresentare il bucket nelle visualizzazioni dei dati, come mostrato nell'immagine seguente.



I punteggi di sensibilità vanno da -1 a 100, come descritto nella tabella seguente. Per valutare gli input relativi al punteggio di un bucket S3, puoi fare riferimento alle statistiche sulla scoperta di dati sensibili e ad altri dettagli forniti da Macie sul bucket.

Punteggio di sensibilità	Etichetta di sensibilità	Informazioni aggiuntive
-1	Errore di classificazione	Macie non ha ancora analizzato o con successo nessuno degli oggetti del bucket a causa di errori di classificazione a livello di oggetto, ovvero problemi relativi alle impostazioni delle autorizzazioni a livello di oggetto, al contenuto degli oggetti o alle quote. Quando Macie ha provato ad analizzare uno o più oggetti nel bucket, si sono verificati degli errori. Ad esempio, un oggetto è un file non valido oppure un oggetto è crittografato con una chiave a cui Macie non può accedere o non può usare. I dati di copertura del bucket possono aiutarti a indagare e correggere gli errori. Per ulteriori informazioni, consulta Valutazione della copertura

Punteggio di sensibilità	Etichetta di sensibilità	Informazioni aggiuntive
		<u>automatizzata del rilevamento di dati sensibili.</u> Macie continuerà a provare ad analizzare gli oggetti nel bucket. Se Macie analizza un oggetto con successo, Macie aggiornerà il punteggio di sensibilità e l'etichetta del bucket in modo che riflettano i risultati dell'analisi.

Punteggio di sensibilità	Etichetta di sensibilità	Informazioni aggiuntive
1-49	Non sensibile	In questo intervallo, un punteggio più alto, ad esempio 49, indica che Macie ha analizzato relativamente pochi oggetti nel secchio. Un punteggio più basso, ad esempio 1, indica che Macie ha analizzato molti oggetti nel bucket (rispetto al numero totale di oggetti nel bucket) e ha rilevato relativamente pochi tipi e occorrenze di dati sensibili in tali oggetti. Un punteggio pari a 1 può anche indicare che il bucket non memorizza alcun oggetto o che tutti gli oggetti nel bucket contengono zero (0) byte di dati. Le statistiche sugli oggetti nei dettagli del bucket possono aiutarti a determinare se questo è il caso. Per ulteriori informazioni, consulta Analisi dei dettagli dei bucket S3.

Punteggio di sensibilità	Etichetta di sensibilità	Informazioni aggiuntive
50	Non ancora analizzato	Macie non ha ancora provato ad analizzare o analizzar e nessuno degli oggetti del bucket. Macie assegna automaticamente questo punteggio quando il rilevamento automatico è inizialmente abilitato o viene aggiunto un bucket all'inventario dei bucket di un account. In un'organizzazione, un bucket può avere questo punteggio anche se il rilevamento automatico non è mai stato abilitato per l'account proprietario del bucket. Un punteggio di 50 può anche indicare che le impostazioni delle autorizzazioni del bucket impediscono a Macie di accedere al bucket o agli oggetti del bucket. Ciò è in genere dovuto a una politica restrittiva del bucket. I dettagli del bucket possono aiutarti a determinare se questo è il caso, perché Macie può fornire solo un sottoinsieme di informazioni sul bucket. Per informazioni su come risolvere questo problema, consulta Consentire a Macie

Punteggio di sensibilità	Etichetta di sensibilità	Informazioni aggiuntive
		di accedere a bucket e oggetti S3
51-99	Sensibile	In questo intervallo, un punteggio più alto, ad esempio 99, indica che Macie ha analizzato molti oggetti nel bucket (rispetto al numero totale di oggetti nel bucket) e ha rilevato molti tipi e occorrenze di dati sensibili in tali oggetti. Un punteggio più basso, ad esempio 51, indica che Macie ha analizzato un numero moderato di oggetti nel bucket (rispetto al numero totale di oggetti nel bucket) e ha rilevato almeno alcuni tipi e occorrenze di dati sensibili in tali oggetti.
100	Sensibile	Il punteggio è stato assegnato manualmente al bucket, sostituendo il punteggio calcolato. Macie non assegna questo punteggio ai bucket.

Controllo dei punteggi di sensibilità

Quando il rilevamento automatico dei dati sensibili è inizialmente abilitato per un account, Amazon Macie assegna automaticamente un punteggio di sensibilità di 50 a ciascun bucket S3 di proprietà dell'account. Macie assegna questo punteggio anche a un bucket quando il bucket viene aggiunto all'inventario dei bucket di un account. In base a quel punteggio, l'etichetta di sensibilità di ogni bucket non viene ancora analizzata. L'eccezione è un bucket vuoto, ovvero un bucket che non memorizza alcun oggetto o che tutti gli oggetti nel bucket contengono zero (0) byte di dati. Se questo è il caso di

un bucket, Macie assegna un punteggio pari a 1 al bucket e l'etichetta di sensibilità del bucket è Non sensibile.

Man mano che la scoperta automatica dei dati sensibili avanza ogni giorno, Macie aggiorna i punteggi di sensibilità e le etichette per i bucket S3 in modo che riflettano i risultati della sua analisi. Per esempio:

- Se Macie non trova dati sensibili in un oggetto, Macie riduce il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità se necessario.
- Se Macie trova dati sensibili in un oggetto, Macie aumenta il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità se necessario.
- Se Macie trova dati sensibili in un oggetto che viene successivamente modificato, Macie rimuove i rilevamenti di dati sensibili relativi all'oggetto dal punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità se necessario.
- Se Macie trova dati sensibili in un oggetto che viene successivamente eliminato, Macie rimuove i rilevamenti di dati sensibili per l'oggetto dal punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità, se necessario.
- Se un oggetto viene aggiunto a un bucket precedentemente vuoto e Macie trova dati sensibili nell'oggetto, Macie aumenta il punteggio di sensibilità del bucket e aggiorna l'etichetta di sensibilità se necessario.
- Se le impostazioni delle autorizzazioni di un bucket impediscono a Macie di accedere o recuperare informazioni sul bucket o sugli oggetti del bucket, Macie modifica il punteggio di sensibilità del bucket su 50 e modifica l'etichetta di sensibilità del bucket su Non ancora analizzato.

I risultati dell'analisi possono iniziare a comparire entro 48 ore dall'attivazione del rilevamento automatico dei dati sensibili per un account.

Se sei l'amministratore Macie di un'organizzazione o disponi di un account Macie autonomo, puoi modificare le impostazioni del punteggio di sensibilità per la tua organizzazione o il tuo account:

- Per modificare le impostazioni per le analisi successive di tutti i bucket S3, modifica le impostazioni del tuo account. Puoi iniziare a includere o escludere identificatori di dati gestiti specifici, identificatori di dati personalizzati o elenchi di dati consentiti. Puoi anche escludere bucket specifici. Per ulteriori informazioni, consulta [Configurazione delle impostazioni di rilevamento automatico](#).
- Per regolare le impostazioni per i singoli bucket S3, modifica le impostazioni per ogni bucket. Puoi includere o escludere tipi specifici di dati sensibili dal punteggio di un bucket. Puoi anche

specificare se assegnare un punteggio calcolato automaticamente a un bucket. Per ulteriori informazioni, consulta [Regolazione dei punteggi di sensibilità per i bucket S3](#).

Se disabiliti il rilevamento automatico dei dati sensibili, l'effetto varia a seconda dei punteggi e delle etichette di sensibilità esistenti. Se lo disabiliti per un account membro di un'organizzazione, i punteggi e le etichette esistenti persistono per i bucket S3 di proprietà dell'account. Se lo disabiliti per un'intera organizzazione o per un account Macie indipendente, i punteggi e le etichette esistenti persistono solo per 30 giorni. Dopo 30 giorni, Macie reimposta i punteggi e le etichette per tutti i bucket di proprietà dell'organizzazione o dell'account. Se un bucket memorizza oggetti, Macie modifica il punteggio a 50 e assegna l'etichetta Non ancora analizzato al bucket. Se un bucket è vuoto, Macie porta il punteggio a 1 e assegna l'etichetta Non sensibile al bucket. Dopo questo ripristino, Macie interrompe l'aggiornamento dei punteggi di sensibilità e delle etichette per i bucket, a meno che non abiliti nuovamente l'individuazione automatica dei dati sensibili per l'organizzazione o l'account.

Impostazioni predefinite per l'individuazione automatica dei dati sensibili

Se il rilevamento automatico dei dati sensibili è abilitato, Amazon Macie seleziona e analizza automaticamente gli oggetti campione da tutti i bucket generici Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) del tuo account. Se sei l'amministratore Macie di un'organizzazione, per impostazione predefinita sono inclusi i bucket S3 di proprietà dei tuoi account membro.

Se sei un amministratore Macie o disponi di un account Macie autonomo, puoi affinare l'ambito delle analisi escludendo specifici bucket S3 dal rilevamento automatico dei dati sensibili. Puoi farlo in due modi: modificando le impostazioni del tuo account e modificando le impostazioni per i singoli bucket. In qualità di amministratore di Macie, puoi anche abilitare o disabilitare il rilevamento automatico dei dati sensibili per i singoli account della tua organizzazione.

Per impostazione predefinita, Macie analizza gli oggetti S3 utilizzando solo il set di identificatori di dati gestiti che consigliamo per l'individuazione automatica dei dati sensibili. Macie non utilizza identificatori di dati personalizzati né elenchi di dati consentiti dall'utente. Se sei un amministratore Macie o disponi di un account Macie autonomo, puoi personalizzare le analisi configurando Macie per utilizzare identificatori di dati gestiti specifici, identificatori di dati personalizzati ed elenchi di dati consentiti. Puoi farlo modificando le impostazioni del tuo account.

Per informazioni sulla modifica delle impostazioni, consulta [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#).

Argomenti

- [Identificatori di dati gestiti predefiniti per l'individuazione automatica di dati sensibili](#)
- [Aggiornamenti alle impostazioni predefinite per l'individuazione automatica dei dati sensibili](#)

Identificatori di dati gestiti predefiniti per l'individuazione automatica di dati sensibili

Per impostazione predefinita, Amazon Macie analizza gli oggetti S3 utilizzando solo il set di identificatori di dati gestiti che consigliamo per il rilevamento automatico di dati sensibili. Questo set predefinito di identificatori di dati gestiti è progettato per rilevare categorie e tipi comuni di dati sensibili. Sulla base della nostra ricerca, è in grado di rilevare categorie e tipi generali di dati sensibili, ottimizzando al contempo i risultati riducendo il rumore.

L'impostazione predefinita è dinamica. Man mano che rilasciamo nuovi identificatori di dati gestiti, li aggiungiamo al set predefinito se è probabile che ottimizzino ulteriormente i risultati del rilevamento automatico dei dati sensibili. Nel tempo, potremmo anche aggiungere o rimuovere gli identificatori di dati gestiti esistenti dal set. La rimozione di un identificatore di dati gestito non influisce sulle statistiche e sui dettagli di rilevamento dei dati sensibili esistenti per i bucket S3. Ad esempio, se rimuoviamo l'identificatore di dati gestiti per un tipo di dati sensibili che Macie aveva precedentemente rilevato in un bucket, Macie continua a segnalare tali rilevamenti. Se aggiungiamo o rimuoviamo un identificatore di dati gestito dal set predefinito, aggiorniamo questa pagina per indicare la natura e la tempistica della modifica. Per ricevere avvisi automatici su queste modifiche, puoi iscriverti al feed RSS nella pagina della cronologia dei documenti di [Macie](#).

I seguenti argomenti elencano gli identificatori di dati gestiti attualmente inclusi nel set predefinito, organizzati per categoria e tipo di dati sensibili. Specificano l'identificatore univoco (ID) per ogni identificatore di dati gestiti del set. Questo ID descrive il tipo di dati sensibili che un identificatore di dati gestito è progettato per rilevare, ad esempio: per le chiavi private PGP e PGP_PRIVATE_KEY USA_PASSPORT_NUMBER per i numeri di passaporto degli Stati Uniti. Se modifichi le impostazioni per l'individuazione automatica dei dati sensibili, puoi utilizzare questo ID per escludere esplicitamente un identificatore di dati gestito dalle analisi successive.

Argomenti

- [Credenziali](#)
- [Informazioni finanziarie](#)
- [Informazioni personali di identificazione \(PII\)](#)

Per dettagli sugli identificatori di dati gestiti specifici o per un elenco completo di tutti gli identificatori di dati gestiti attualmente forniti da Macie, consulta [Utilizzo di identificatori di dati gestiti](#)

Credenziali

Per rilevare le occorrenze dei dati relativi alle credenziali negli oggetti S3, Macie utilizza i seguenti identificatori di dati gestiti per impostazione predefinita.

Tipo di dati sensibili	ID identificatore dei dati gestiti
AWS chiave di accesso segreta	AWS_CREDENTIALS
Intestazione HTTP Basic Authorization	HTTP_BASIC_AUTH_HEADER
Chiave privata OpenSSH	OPENSSH_PRIVATE_KEY
Chiave privata PGP	PGP_PRIVATE_KEY
Chiave privata Public Key Cryptography Standard (PKCS)	PKCS
Chiave privata PuTTY	PUTTY_PRIVATE_KEY

Informazioni finanziarie

Per rilevare le occorrenze di informazioni finanziarie negli oggetti S3, Macie utilizza i seguenti identificatori di dati gestiti per impostazione predefinita.

Tipo di dati sensibili	ID identificatore dei dati gestiti
Dati a banda magnetica della carta di credito	CREDIT_CARD_MAGNETIC_STRIPE
Numero di carta di credito	CREDIT_CARD_NUMBER (per i numeri di carte di credito in prossimità di una parola chiave)

Informazioni personali di identificazione (PII)

Per rilevare le occorrenze di informazioni di identificazione personale (PII) negli oggetti S3, Macie utilizza i seguenti identificatori di dati gestiti per impostazione predefinita.

Tipo di dati sensibili	ID identificatore dei dati gestiti
Numero identificativo della patente di guida	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (per gli Stati Uniti), UK_DRIVERS_LICENSE
Numero di lista elettorale	UK_ELECTORAL_ROLL_NUMBER
Numeri di carta d'identità	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Numero NINO (National Insurance Number)	UK_NATIONAL_INSURANCE_NUMBER
Numero di passaporto	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Social Insurance Number (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Social Security number (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
Numero identificativo del contribuente o codice fiscale	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Aggiornamenti alle impostazioni predefinite per l'individuazione automatica dei dati sensibili

La tabella seguente descrive le modifiche alle impostazioni che Amazon Macie utilizza di default per il rilevamento automatico di dati sensibili. Per ricevere avvisi automatici su queste modifiche, iscriviti al feed RSS nella pagina della cronologia dei documenti di [Macie](#).

Modifica	Descrizione	Data
Implementato un nuovo set dinamico di identificatori di dati gestiti predefiniti	Le nuove configurazioni automatizzate di rilevamento dei dati sensibili si basano ora su un set dinamico predefinito di identificatori di dati gestiti. Se abiliti il rilevamento automatico dei dati sensibili per la prima volta in o dopo questa data, la configurazione si basa sul set dinamico. Se hai abilitato il rilevamento automatico dei dati sensibili per la prima volta prima di questa data, la configurazione si basa su un diverso set di identificatori di dati gestiti. Per ulteriori informazioni, consulta le note dopo questa tabella.	2 agosto 2023
Disponibilità generale	Versione iniziale del rilevamento automatico dei dati sensibili.	28 novembre 2022

Se inizialmente hai abilitato il rilevamento automatico dei dati sensibili prima del 2 agosto 2023, la configurazione non si basa sul set dinamico di identificatori di dati gestiti predefiniti. Si basa invece su un set statico di identificatori di dati gestiti che abbiamo definito per la versione iniziale del rilevamento automatico dei dati sensibili, come elencato nella tabella seguente.

Per determinare quando hai inizialmente abilitato il rilevamento automatico dei dati sensibili, puoi utilizzare la console Amazon Macie: scegli l'individuazione automatica dei dati sensibili nel riquadro di navigazione, quindi fai riferimento alla data di attivazione nella sezione Stato. Puoi farlo anche a livello di codice: utilizza il [GetAutomatedDiscoveryConfiguration](#) funzionamento dell'API Amazon Macie e fai riferimento al valore del campo. `firstEnabledAt` Se la data è precedente al 2 agosto 2023 e desideri iniziare a utilizzare il set dinamico di identificatori di dati gestiti predefiniti, contatta per ricevere assistenza. Supporto AWS

La tabella seguente elenca tutti gli identificatori di dati gestiti presenti nel set statico. La tabella viene ordinata prima per categoria di dati sensibili e poi per tipo di dati sensibili. Per informazioni dettagliate sugli identificatori di dati gestiti specifici, vedere. [Utilizzo di identificatori di dati gestiti](#)

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
Credenziali	AWS chiave di accesso segreta	AWS_CREDENTIALS
Credenziali	intestazione HTTP Basic Authorization	HTTP_BASIC_AUTH_HEADER
Credenziali	Chiave privata OpenSSH	OPENSSH_PRIVATE_KEY
Credenziali	Chiave privata PGP	PGP_PRIVATE_KEY
Credenziali	Chiave privata Public Key Cryptography Standard (PKCS)	PKCS
Credenziali	Chiave privata PuTTY	PUTTY_PRIVATE_KEY
Informazioni finanziarie	Numero del conto bancario	BANK_ACCOUNT_NUMBER (per numeri di conto bancari canadesi e statunitensi), FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER,

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
		UK_BANK_ACCOUNT_NUMBER
Informazioni finanziarie	Data di scadenza della carta di credito	CREDIT_CARD_EXPIRATION
Informazioni finanziarie	dati a banda magnetica della carta di credito	CREDIT_CARD_MAGNETIC_STRIPE
Informazioni finanziarie	Numero di carta di credito	CREDIT_CARD_NUMBER (per i numeri di carte di credito in prossimità di una parola chiave)
Informazioni finanziarie	Codice di verifica della carta di credito	CREDIT_CARD_SECURITY_CODE
Informazioni personali : informazioni sanitarie personali (PHI)	Numero di registrazione DEA (Drug Enforcement Agency)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Informazioni personali: PHI	Health Insurance Claim Number (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
Informazioni personali: PHI	Numero di identificazione medica e assistenza sanitaria	CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
Informazioni personali: PHI	Codice HCPCS (Healthcare Common Procedure Coding System)	USA_HEALTHCARE_PROCEDURE_CODE
Informazioni personali: PHI	National Drug Code (NDC)	USA_NATIONAL_DRUG_CODE
Informazioni personali: PHI	National Provider Identifier (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
Informazioni personali: PHI	Identificatore univoco del dispositivo (UDI)	MEDICAL_DEVICE_UDI
Informazioni personali: informazioni di identificazione personale (PII)	Data di nascita	DATE_OF_BIRTH

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
Informazioni personali: PII	Numero identificativo della patente di guida	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (per gli Stati Uniti), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVER

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
		S_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Informazioni personali: PII	Numero di lista elettorale	UK_ELECTORAL_ROLL_NUMBER
Informazioni personali: PII	Nome completo	NAME
Informazioni personali: PII	Coordinate del sistema di posizionamento globale (GPS)	LATITUDE_LONGITUDE
Informazioni personali: PII	Indirizzo postale	ADDRESS, BRAZIL_CEP_CODE
Informazioni personali: PII	Numeri di carta d'identità	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Informazioni personali: PII	Numero NINO (National Insurance Number)	UK_NATIONAL_INSURANCE_NUMBER

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
Informazioni personali: PII	Numero di passaporto	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Informazioni personali: PII	Numero di residenza permanente (Green Card)	CANADA_NATIONAL_IDENTIFICATION_NUMBER
Informazioni personali: PII	Numero di telefono	BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (per Canada e Stati Uniti), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
Informazioni personali: PII	Social Insurance Number (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Informazioni personali: PII	Social Security number (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Categoria di dati sensibili	Tipo di dati sensibili	ID identificatore dei dati gestiti
Informazioni personali: PII	Numero identificativo del contribuente o codice fiscale	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CN PJ_NUMBER, BRAZIL_CP F_NUMBER, FRANCE_TA X_IDENTIFICATION_N UMBER, GERMANY_T AX_IDENTIFICATION_ NUMBER, SPAIN_NIE _NUMBER, SPAIN_NIF _NUMBER, SPAIN_TAX _IDENTIFICATION_NU MBER, UK_TAX_ID ENTIFICATION_NUMBE R, USA_INDIV IDUAL_TAX_IDENTIFI CATION_NUMBER
Informazioni personali: PII	Numeri di matricola del veicolo (VIN)	VEHICLE_IDENTIFICA TION_NUMBER

Esecuzione di processi di rilevamento dei dati sensibili

Con Amazon Macie, puoi creare ed eseguire processi di rilevamento di dati sensibili per automatizzare il rilevamento, la registrazione e il reporting di dati sensibili nei bucket generici di Amazon Simple Storage Service (Amazon S3). Un processo di rilevamento di dati sensibili è una serie di attività di elaborazione e analisi automatizzate che Macie esegue per rilevare e segnalare dati sensibili negli oggetti Amazon S3. Ogni lavoro fornisce report dettagliati sui dati sensibili trovati da Macie e sulle analisi eseguite da Macie. Creando ed eseguendo processi, puoi creare e mantenere una visione completa dei dati archiviati dalla tua organizzazione in Amazon S3 e di eventuali rischi di sicurezza o conformità per tali dati.

Per aiutarti a soddisfare e mantenere la conformità ai requisiti di sicurezza e privacy dei dati, Macie offre diverse opzioni per la pianificazione e la definizione dell'ambito di un lavoro. È possibile configurare un processo in modo che venga eseguito una sola volta per l'analisi e la valutazione su

richiesta o su base ricorrente per analisi, valutazione e monitoraggio periodici. Puoi anche definire l'ampiezza e la profondità dell'analisi di un job: bucket S3 specifici che selezioni o bucket che soddisfano criteri specifici. Facoltativamente, puoi affinare l'ambito di tale analisi scegliendo opzioni aggiuntive. Le opzioni includono criteri personalizzati che derivano dalle proprietà degli oggetti S3, come tag, prefissi e data dell'ultima modifica di un oggetto.

Per ogni lavoro, specifichi anche i tipi di dati sensibili che vuoi che Macie rilevi e segnali. Puoi configurare un lavoro per utilizzare [identificatori di dati gestiti forniti](#) da Macie, [identificatori di dati personalizzati](#) definiti da te o una combinazione dei due. Selezionando identificatori di dati gestiti e personalizzati specifici per un lavoro, puoi personalizzare l'analisi in modo che si concentri su tipi specifici di dati sensibili. Per ottimizzare l'analisi, puoi anche configurare un processo per utilizzare gli elenchi di dati [consentiti](#). Gli elenchi consentiti specificano il testo e gli schemi di testo che vuoi che Macie ignori, in genere eccezioni relative ai dati sensibili per scenari o ambienti particolari dell'organizzazione.

Ogni lavoro produce registrazioni dei dati sensibili trovati da Macie e delle analisi eseguite da Macie: rilevamenti di dati sensibili e risultati della scoperta di dati sensibili. Un rilevamento di dati sensibili è un rapporto dettagliato dei dati sensibili che Macie ha trovato in un oggetto S3. Un risultato di scoperta di dati sensibili è un record che registra i dettagli sull'analisi di un oggetto S3. Macie crea un risultato di scoperta di dati sensibili per ogni oggetto per il quale configuri un processo per analizzare. Ciò include oggetti in cui Macie non trova dati sensibili e quindi non produce risultati su dati sensibili e oggetti che Macie non può analizzare a causa di errori o problemi. Ogni tipo di record aderisce a uno schema standardizzato, che può aiutarti a interrogare, monitorare ed elaborare i record per soddisfare i requisiti di sicurezza e conformità.

Argomenti

- [Opzioni di ambito per i lavori di rilevamento di dati sensibili](#)
- [Creazione di un processo di rilevamento dei dati sensibili](#)
- [Analisi dei risultati di un processo di rilevamento di dati sensibili](#)
- [Gestione dei processi di rilevamento di dati sensibili](#)
- [Monitoraggio dei processi di rilevamento di dati sensibili con CloudWatch Logs](#)
- [Previsione e monitoraggio dei costi per i lavori di scoperta di dati sensibili](#)
- [Identificatori di dati gestiti consigliati per i lavori di rilevamento di dati sensibili](#)

Opzioni di ambito per i lavori di rilevamento di dati sensibili

Con i processi di rilevamento di dati sensibili, definisci l'ambito dell'analisi che Amazon Macie esegue per rilevare e segnalare dati sensibili nei bucket generici di Amazon Simple Storage Service (Amazon S3). Per aiutarti a farlo, Macie offre diverse opzioni specifiche per il lavoro che puoi scegliere quando crei e configuri un lavoro.

Opzioni di ambito

- [Bucket S3 o criteri relativi ai bucket](#)
- [Profondità di campionamento](#)
- [Esecuzione iniziale: include gli oggetti S3 esistenti](#)
- [Criteri relativi agli oggetti S3](#)

Bucket S3 o criteri relativi ai bucket

Quando crei un processo di rilevamento di dati sensibili, specifichi in quali bucket S3 vengono archiviati gli oggetti che desideri che Macie analizzi durante l'esecuzione del lavoro. Puoi farlo in due modi: selezionando bucket S3 specifici dall'inventario dei bucket o specificando criteri personalizzati che derivano dalle proprietà dei bucket S3.

Seleziona bucket S3 specifici

Con questa opzione, selezioni esplicitamente ogni bucket S3 da analizzare. Quindi, quando il processo viene eseguito, Macie analizza gli oggetti solo nei bucket selezionati. Se configuri un lavoro per essere eseguito periodicamente su base giornaliera, settimanale o mensile, Macie analizza gli oggetti negli stessi bucket ogni volta che il lavoro viene eseguito.

Questa configurazione è utile nei casi in cui si desidera eseguire un'analisi mirata di un set specifico di dati. Ti offre un controllo preciso e prevedibile sui bucket analizzati da un job.

Specificate i criteri del bucket S3

Con questa opzione, definisci i criteri di runtime che determinano quali bucket S3 analizzare. I criteri consistono in una o più condizioni che derivano dalle proprietà del bucket, come le impostazioni e i tag di accesso pubblico. Quando il processo viene eseguito, Macie identifica i bucket che corrispondono ai criteri specificati e quindi analizza gli oggetti in tali bucket. Se configuri un lavoro in modo che venga eseguito periodicamente, Macie esegue questa operazione ogni volta che il lavoro viene eseguito. Di conseguenza, Macie potrebbe analizzare gli oggetti

in diversi bucket ogni volta che viene eseguito il job, a seconda delle modifiche all'inventario dei bucket e dei criteri definiti.

Questa configurazione è utile nei casi in cui desideri che l'ambito dell'analisi si adatti dinamicamente alle modifiche all'inventario dei bucket. Se configuri un processo per utilizzare i criteri dei bucket e lo esegui periodicamente, Macie identifica automaticamente i nuovi bucket che corrispondono ai criteri e ispeziona tali bucket per verificare la presenza di dati sensibili.

Gli argomenti di questa sezione forniscono dettagli aggiuntivi su ciascuna opzione.

Argomenti

- [Selezione di bucket S3 specifici](#)
- [Specificazione dei criteri del bucket S3](#)

Selezione di bucket S3 specifici

Se scegli di selezionare esplicitamente ogni bucket S3 che desideri venga analizzato da un job, Macie ti fornisce un inventario dei bucket generici attualmente in uso. Regione AWS Puoi quindi rivedere il tuo inventario e selezionare i bucket che desideri. Se sei l'amministratore Macie di un'organizzazione, il tuo inventario include i bucket di proprietà dei tuoi account membro. Puoi selezionare fino a 1.000 di questi bucket, che coprono fino a 1.000 account.

Per aiutarti a selezionare i bucket, l'inventario fornisce dettagli e statistiche per ogni bucket. Ciò include la quantità di dati che un job può analizzare in ogni bucket: gli oggetti classificabili sono oggetti che utilizzano una [classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un file o un formato di storage supportato](#). L'inventario indica anche se sono stati configurati lavori esistenti per analizzare gli oggetti in un bucket. Questi dettagli possono aiutarti a stimare l'ampiezza di un lavoro e a perfezionare le tue selezioni.

Nella tabella dell'inventario:

- Sensibilità: specifica il punteggio di sensibilità corrente del bucket, se il [rilevamento automatico dei dati sensibili](#) è abilitato.
- Oggetti classificabili: specifica il numero totale di oggetti che il job può analizzare nel bucket.
- Dimensione classificabile: specifica la dimensione di archiviazione totale di tutti gli oggetti che il job può analizzare nel bucket.

Se il bucket memorizza oggetti compressi, questo valore non riflette la dimensione effettiva di tali oggetti dopo la loro decompressione. Se il controllo delle versioni è abilitato per il bucket, questo valore si basa sulla dimensione di archiviazione della versione più recente di ogni oggetto nel bucket.

- **Monitorato per processo:** specifica se sono stati configurati lavori esistenti per analizzare periodicamente gli oggetti nel bucket su base giornaliera, settimanale o mensile.

Se il valore di questo campo è Sì, il bucket viene incluso in modo esplicito in un processo periodico oppure il bucket corrisponde ai criteri per un processo periodico nelle ultime 24 ore. Inoltre, lo stato di almeno uno di questi lavori non è Annullato. Macie aggiorna questi dati su base giornaliera.

- **Ultimo processo eseguito:** se hai configurato un processo periodico o occasionale per analizzare gli oggetti nel bucket, questo campo specifica la data e l'ora più recenti in cui uno di questi lavori ha iniziato a essere eseguito. Altrimenti, in questo campo viene visualizzato un trattino (—).

Se l'icona delle informazioni



appare accanto ai nomi dei bucket, ti consigliamo di recuperare i metadati dei bucket più recenti da Amazon S3. Per fare ciò, scegli refresh (↻) sopra la tabella.



L'icona delle informazioni indica che un bucket è stato creato nelle ultime 24 ore, probabilmente dopo l'ultima volta che Macie ha recuperato i metadati del bucket e dell'oggetto da Amazon S3 come parte del ciclo di aggiornamento giornaliero. Per ulteriori informazioni, consulta [Aggiornamenti dei dati](#).

Se l'icona di avviso



appare accanto al nome di un bucket, a Macie non è consentito accedere al bucket o agli oggetti del bucket. Ciò significa che il job non sarà in grado di analizzare gli oggetti nel bucket. Per esaminare il problema, consulta la policy e le impostazioni delle autorizzazioni del bucket in Amazon S3. Ad esempio, il bucket potrebbe avere una politica restrittiva. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Per personalizzare la visualizzazione e trovare bucket specifici più facilmente, puoi filtrare la tabella inserendo i criteri di filtro nella casella del filtro. La tabella seguente mostra alcuni esempi.

Per mostrare tutti i bucket che...	Applica questo filtro...
Sono di proprietà di un account specifico	ID account = <i>the 12-digit ID for the account</i>
Sono accessibili al pubblico	Autorizzazione effettiva = Pubblica
Non sono inclusi in nessun lavoro periodico	Monitorato attivamente dal lavoro = False
Non sono inclusi in nessun lavoro periodico o occasionale	Definito in job = False
Hai una chiave di tag specifica*	Chiave tag = <i>the tag key</i>
Hanno un valore di tag specifico*	Valore del tag = <i>the tag value</i>
Archivia oggetti non crittografati (o oggetti che utilizzano la crittografia lato client)	Il numero di oggetti mediante crittografia è Nessuna crittografia e Da = 1

* Le chiavi e i valori dei tag distinguono tra maiuscole e minuscole. Inoltre, è necessario specificare un valore completo e valido. Non è possibile specificare valori parziali o utilizzare caratteri jolly.

Per visualizzare dettagli aggiuntivi per un bucket, scegli il nome del bucket e consulta il pannello dei dettagli. Nel pannello puoi anche:

- Orientati e approfondisci determinati campi scegliendo una lente d'ingrandimento per il campo. Scegli



di mostrare i bucket con lo stesso valore. Scegli



di mostrare i bucket con altri valori.

- Recupera i metadati più recenti per gli oggetti nel bucket. Questo può essere utile se hai creato di recente un bucket o hai apportato modifiche significative agli oggetti del bucket nelle ultime 24 ore. Per recuperare i dati, scegliete refresh



nella sezione Statistiche degli oggetti del pannello. Questa opzione è disponibile per i bucket che memorizzano 30.000 o meno oggetti.

In alcuni casi, il pannello potrebbe non includere tutti i dettagli di un bucket. Ciò può verificarsi se si archiviano più di 10.000 bucket in Amazon S3. Macie conserva i dati di inventario completi per soli 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente. Tuttavia, è possibile configurare un processo per analizzare gli oggetti nei bucket che superano questa quota. Per esaminare ulteriori dettagli su questi bucket, usa Amazon S3.

Specificazione dei criteri del bucket S3

Se scegli di specificare i criteri del bucket per un lavoro, Macie offre opzioni per definire e testare i criteri. Questi sono criteri di runtime che determinano quali bucket S3 memorizzano gli oggetti da analizzare. Ogni volta che il processo viene eseguito, Macie identifica i bucket generici che corrispondono ai criteri specificati, quindi analizza gli oggetti nei bucket appropriati. Se sei l'amministratore Macie di un'organizzazione, questo include i bucket di proprietà dei tuoi account membro.

Definizione dei criteri del bucket

I criteri del bucket sono costituiti da una o più condizioni che derivano dalle proprietà dei bucket S3. Ogni condizione, nota anche come criterio, è composta dalle seguenti parti:

- Un campo basato su proprietà, ad esempio ID account o Autorizzazione effettiva.
- Un operatore, uguale a (*eq*) o non uguale a (*neq*).
- Uno o più valori.
- Un'istruzione di inclusione o esclusione che indica se analizzare (includere) o ignorare (escludere) i bucket che corrispondono alla condizione.

Se specifichi più di un valore per un campo, Macie usa la logica OR per unire i valori. Se specifichi più di una condizione per i criteri, Macie utilizza la logica AND per unire le condizioni. Inoltre, le condizioni di esclusione hanno la precedenza sulle condizioni di inclusione. Ad esempio, se includi bucket accessibili pubblicamente ed escludi bucket con tag specifici, il job analizza gli oggetti in qualsiasi bucket accessibile pubblicamente a meno che il bucket non abbia uno dei tag specificati.

Puoi definire condizioni che derivano da uno qualsiasi dei seguenti campi basati sulle proprietà per i bucket S3.

ID account

L'identificatore univoco (ID) di chi possiede un bucket. Account AWS Per specificare più valori per questo campo, inserisci l'ID di ogni account e separa ogni voce con una virgola.

Nota che Macie non supporta l'uso di caratteri jolly o valori parziali per questo campo.

Nome bucket

Il nome di un bucket. Questo campo è correlato al campo Name, non al campo Amazon Resource Name (ARN), in Amazon S3. Per specificare più valori per questo campo, inserisci il nome di ogni bucket e separa ogni voce con una virgola.

Nota che i valori distinguono tra maiuscole e minuscole. Inoltre, Macie non supporta l'uso di caratteri jolly o valori parziali per questo campo.

Autorizzazione effettiva

Specifica se un bucket è accessibile pubblicamente. È possibile scegliere uno o più dei seguenti valori per questo campo:

- Non pubblico: il pubblico in generale non ha accesso in lettura o scrittura al bucket.
- Pubblico: il pubblico in generale ha accesso in lettura o scrittura al bucket.
- Sconosciuto: Macie non è stata in grado di valutare le impostazioni di accesso pubblico per il bucket. Un problema o una quota impedivano a Macie di recuperare e valutare i dati richiesti.

Per determinare se un bucket è accessibile pubblicamente, Macie analizza una combinazione di impostazioni a livello di account e bucket per il bucket: le impostazioni di blocco dell'accesso pubblico per l'account, le impostazioni di blocco dell'accesso pubblico per il bucket, la politica del bucket per il bucket e l'elenco di controllo degli accessi (ACL) per il bucket. Per informazioni su queste impostazioni, consulta [Controllo degli accessi](#) e [Blocco dell'accesso pubblico allo storage Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

Accesso condiviso

Specifica se un bucket è condiviso con un altro Account AWS, un'identità di accesso di CloudFront origine Amazon (OAI) o un controllo di accesso all' CloudFront origine (OAC). Puoi scegliere uno o più dei seguenti valori per questo campo:

- Esterno: il bucket è condiviso con uno o più dei seguenti elementi o con una combinazione dei seguenti elementi: un CloudFront OAI, un CloudFront OAC o un account esterno all'organizzazione (che non fa parte della).
 - Interno: il bucket è condiviso con uno o più account interni (che fanno parte della) tua organizzazione. Non è condiviso con un CloudFront OAI o un OAC.
 - Non condiviso: il bucket non è condiviso con un altro account, un CloudFront OAI o un OAC.
- CloudFront

- Sconosciuto: Macie non è stata in grado di valutare le impostazioni di accesso condiviso per il bucket. Un problema o una quota impedivano a Macie di recuperare e valutare i dati richiesti.

Per determinare se un bucket è condiviso con un altro Account AWS, Macie analizza la policy del bucket e l'ACL del bucket. Inoltre, un'organizzazione è definita come un insieme di account Macie gestiti centralmente come gruppo di account correlati tramite o su invito di Macie. AWS Organizations Per informazioni sulle opzioni di Amazon S3 per la condivisione dei bucket, consulta il [controllo degli accessi](#) nella Guida per l'utente di Amazon Simple Storage Service.

Per determinare se un bucket è condiviso con un CloudFront OAI o un OAC, Macie analizza la policy relativa al bucket. Un CloudFront OAI o OAC consente agli utenti di accedere agli oggetti di un bucket tramite una o più distribuzioni specificate. CloudFront Per informazioni su CloudFront OAI e OACs, consulta la sezione [Restrizione dell'accesso a un'origine Amazon S3](#) nella CloudFront Amazon Developer Guide.

Tag

I tag associati a un bucket. I tag sono etichette che è possibile definire e assegnare a determinati tipi di AWS risorse, inclusi i bucket S3. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Per informazioni sull'etichettatura dei bucket S3, consulta [Using cost allocation S3 bucket tag nella Amazon Simple Storage Service User Guide](#).

Per un processo di rilevamento di dati sensibili, puoi utilizzare questo tipo di condizione per includere o escludere bucket che hanno una chiave di tag specifica, un valore di tag specifico o una chiave di tag e un valore di tag specifici (in coppia). Per esempio:

- Se si specifica **Project** come chiave di tag e non si specifica alcun valore di tag per una condizione, qualsiasi bucket con la chiave di tag Project soddisfa i criteri della condizione, indipendentemente dai valori di tag associati a quella chiave di tag.
- Se specificate **Development** e **Test** come valori di tag e non specificate alcuna chiave di tag per una condizione, qualsiasi bucket con il valore del **Test** tag **Development** o corrisponde ai criteri della condizione, indipendentemente dalle chiavi di tag associate a tali valori di tag.

I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Inoltre, Macie non supporta l'uso di caratteri jolly o valori parziali nelle condizioni dei tag.

Per specificare più chiavi di tag in una condizione, inserisci ogni chiave di tag nel campo Chiave e separa ogni voce con una virgola. Per specificare più valori di tag in una condizione, inserisci ogni valore di tag nel campo Valore e separa ogni voce con una virgola.

Se memorizzi più di 10.000 bucket in Amazon S3, tieni presente che Macie non conserva i dati dei tag per tutti i bucket. Macie conserva i dati di inventario completi per soli 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente. Per tutti gli altri bucket, le chiavi e i valori dei tag associati non sono inclusi nei dati di inventario. Ciò significa che i bucket non corrisponderanno a chiavi o valori di tag specifici in una condizione che utilizza l'operatore equals (=). Se specifichi un operatore not equals (neq) per una condizione basata su tag, significa che i bucket corrisponderanno alla condizione.

Test dei criteri del bucket

Mentre definisci i criteri del bucket, puoi testare e perfezionare i criteri visualizzando in anteprima i risultati. A tale scopo, espandi la sezione Visualizza l'anteprima dei risultati dei criteri che appare sotto i criteri sulla console. Questa sezione mostra una tabella con un massimo di 25 bucket generici che attualmente soddisfano i criteri.

La tabella fornisce anche informazioni sulla quantità di dati che il job può analizzare in ogni bucket: gli oggetti classificabili sono oggetti che utilizzano una [classe di storage Amazon S3 supportata e hanno un'estensione del nome di file per un file o un formato di storage supportato](#). La tabella indica anche se sono stati configurati lavori esistenti per analizzare periodicamente gli oggetti in un bucket.

Nella tabella:

- **Sensibilità:** specifica il punteggio di sensibilità corrente del bucket, se il [rilevamento automatico dei dati sensibili](#) è abilitato.
- **Oggetti classificabili:** specifica il numero totale di oggetti che il job può analizzare nel bucket.
- **Dimensione classificabile:** specifica la dimensione di archiviazione totale di tutti gli oggetti che il job può analizzare nel bucket.

Se il bucket memorizza oggetti compressi, questo valore non riflette la dimensione effettiva di tali oggetti dopo la loro decompressione. Se il controllo delle versioni è abilitato per il bucket, questo valore si basa sulla dimensione di archiviazione della versione più recente di ogni oggetto nel bucket.

- **Monitorato per processo:** specifica se sono stati configurati lavori esistenti per analizzare periodicamente gli oggetti nel bucket su base giornaliera, settimanale o mensile.

Se il valore di questo campo è Sì, il bucket viene incluso in modo esplicito in un processo periodico oppure il bucket corrisponde ai criteri per un processo periodico nelle ultime 24 ore. Inoltre, lo stato di almeno uno di questi lavori non è Annullato. Macie aggiorna questi dati su base giornaliera.

Se l'icona di avviso



)
appare accanto al nome di un bucket, a Macie non è consentito accedere al bucket o agli oggetti del bucket. Ciò significa che il job non sarà in grado di analizzare gli oggetti nel bucket. Per esaminare il problema, consulta la policy e le impostazioni delle autorizzazioni del bucket in Amazon S3. Ad esempio, il bucket potrebbe avere una politica restrittiva. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Per rifinire i criteri del bucket per il job, utilizza le opzioni di filtro per aggiungere, modificare o rimuovere condizioni dai criteri. Macie aggiorna quindi la tabella in base alle modifiche apportate.

Profondità di campionamento

Con questa opzione, specifichi la percentuale di oggetti S3 idonei che desideri che venga analizzato da un processo di rilevamento di dati sensibili. Gli oggetti idonei sono oggetti che: utilizzano una [classe di storage Amazon S3 supportata](#), hanno un'estensione del nome di file per un [file o un formato di storage supportato](#) e soddisfano altri criteri specificati per il processo.

Se questo valore è inferiore al 100%, Macie seleziona gli oggetti idonei da analizzare a caso, fino alla percentuale specificata, e analizza tutti i dati in tali oggetti. Ad esempio, se si configura un lavoro per analizzare 10.000 oggetti e si specifica una profondità di campionamento del 20%, Macie analizza circa 2.000 oggetti idonei selezionati casualmente durante l'esecuzione del lavoro.

La riduzione della profondità di campionamento di un lavoro può ridurre i costi e ridurre la durata di un lavoro. È utile nei casi in cui i dati negli oggetti sono estremamente coerenti e si desidera determinare se un bucket S3, anziché ogni oggetto, memorizza dati sensibili.

Nota che questa opzione controlla la percentuale di oggetti che vengono analizzati, non la percentuale di byte che vengono analizzati. Se inserisci una profondità di campionamento inferiore al 100%, Macie analizza tutti i dati in ogni oggetto selezionato, non la percentuale dei dati in ogni oggetto selezionato.

Esecuzione iniziale: include gli oggetti S3 esistenti

È possibile utilizzare processi di rilevamento di dati sensibili per eseguire analisi continue e incrementali degli oggetti nei bucket S3. Se configuri un processo per l'esecuzione periodica, Macie esegue questa operazione automaticamente: ogni esecuzione analizza solo gli oggetti che sono stati creati o modificati dopo l'esecuzione precedente. Con l'opzione **Includi oggetti esistenti**, scegli il punto di partenza per il primo incremento:

- Per analizzare tutti gli oggetti esistenti subito dopo aver terminato la creazione del lavoro, selezionate la casella di controllo relativa a questa opzione.
- Per attendere e analizzare solo gli oggetti che vengono creati o modificati dopo la creazione del lavoro e prima della prima esecuzione, deselectionate la casella di controllo relativa a questa opzione.

La deselection di questa casella di controllo è utile nei casi in cui i dati sono già stati analizzati e si desidera continuare ad analizzarli periodicamente. Ad esempio, se in precedenza hai utilizzato un altro servizio o un'applicazione per classificare i dati e hai recentemente iniziato a utilizzare Macie, potresti utilizzare questa opzione per garantire la continua scoperta e classificazione dei dati senza incorrere in costi inutili o duplicare i dati di classificazione.

Ogni esecuzione successiva di un processo periodico analizza automaticamente solo gli oggetti che vengono creati o modificati dopo l'esecuzione precedente.

Sia per i lavori periodici che per quelli occasionali, è inoltre possibile configurare un lavoro per analizzare solo gli oggetti che vengono creati o modificati prima o dopo un determinato periodo o durante un determinato intervallo di tempo. A tale scopo, aggiungete criteri relativi agli oggetti che utilizzano la data dell'ultima modifica per gli oggetti.

Criteri relativi agli oggetti S3

Per ottimizzare l'ambito di un processo di rilevamento di dati sensibili, puoi definire criteri personalizzati per gli oggetti S3. Macie utilizza questi criteri per determinare quali oggetti analizzare (includere) o ignorare (escludere) durante l'esecuzione del lavoro. I criteri consistono in una o più condizioni che derivano dalle proprietà degli oggetti S3. Le condizioni si applicano agli oggetti in tutti i bucket S3 inclusi nell'analisi. Se un bucket memorizza più versioni di un oggetto, le condizioni si applicano alla versione più recente dell'oggetto.

Se definisci più condizioni come criteri dell'oggetto, Macie utilizza la logica AND per unire le condizioni. Inoltre, le condizioni di esclusione hanno la precedenza sulle condizioni di inclusione. Ad esempio, se si includono oggetti con estensione pdf ed si escludono oggetti di dimensioni superiori a 5 MB, il job analizza qualsiasi oggetto con estensione pdf, a meno che l'oggetto non sia più grande di 5 MB.

È possibile definire condizioni che derivano da una qualsiasi delle seguenti proprietà degli oggetti S3.

Estensione del nome del file

Ciò è correlato all'estensione del nome di file di un oggetto S3. È possibile utilizzare questo tipo di condizione per includere o escludere oggetti in base al tipo di file. Per eseguire questa operazione per più tipi di file, inserisci l'estensione del nome di file per ogni tipo e separa ogni voce con una virgola, ad esempio: **docx,pdf,xlsx**. Se inserisci più estensioni di nomi di file come valori per una condizione, Macie usa la logica OR per unire i valori.

Nota che i valori distinguono tra maiuscole e minuscole. Inoltre, Macie non supporta l'uso di valori parziali o caratteri jolly in questo tipo di condizione.

Per informazioni sui tipi di file che Macie può analizzare, consulta [Formati di file e di archiviazione supportati](#)

Ultima modifica

Ciò è correlato al campo Ultima modifica in Amazon S3. In Amazon S3, questo campo memorizza la data e l'ora in cui un oggetto S3 è stato creato o modificato l'ultima volta, a seconda di quale sia l'ultima.

Per un processo di rilevamento di dati sensibili, questa condizione può essere una data specifica, una data e un'ora specifiche o un intervallo di tempo esclusivo:

- Per analizzare gli oggetti che sono stati modificati l'ultima volta dopo una certa data o data e ora, inserisci i valori nei campi Da.
- Per analizzare gli oggetti che sono stati modificati l'ultima volta prima di una certa data o data e ora, inserite i valori nei campi To.
- Per analizzare gli oggetti che sono stati modificati l'ultima volta in un determinato intervallo di tempo, utilizzate i campi Da per inserire i valori per la prima data o data e ora nell'intervallo di tempo. Utilizzate i campi To per inserire i valori per l'ultima data o data e ora nell'intervallo di tempo.
- Per analizzare gli oggetti che sono stati modificati l'ultima volta in qualsiasi momento durante un determinato giorno, inserisci la data nel campo Data di inizio. Inserisci la data del giorno successivo nel campo Fino alla data. Quindi verifica che entrambi i campi relativi all'ora siano vuoti. (Macie considera un campo orario vuoto come `00:00:00`.) Ad esempio, per analizzare gli oggetti che sono stati modificati il 9 agosto 2023, immettete **2023/08/09** nel campo Data di inizio, immettete **2023/08/10** nel campo Alla data e non immettete un valore in nessuno dei campi relativi all'ora.

Immettete qualsiasi valore temporale nel formato UTC (Coordinated Universal Time) e utilizzate la notazione a 24 ore.

Prefisso

Ciò è correlato al campo Key in Amazon S3. In Amazon S3, questo campo memorizza il nome di un oggetto S3, incluso il prefisso dell'oggetto. Un prefisso è simile a un percorso di directory all'interno di un bucket. Consente di raggruppare oggetti simili in un bucket, proprio come si potrebbero archiviare file simili in una cartella su un file system. Per informazioni sui prefissi e sulle cartelle degli oggetti in Amazon S3, [consulta Organization objects in the Amazon S3 using folders nella Amazon Simple Storage Service User Guide](#).

Puoi utilizzare questo tipo di condizione per includere o escludere oggetti le cui chiavi (nomi) iniziano con un determinato valore. Ad esempio, per escludere tutti gli oggetti la cui chiave inizia con AWSLogs, immettete **AWSLogs** come valore una condizione Prefix, quindi scegliete Escludi.

Se inserisci più prefissi come valori per una condizione, Macie usa la logica OR per unire i valori. Ad esempio, se inserite **AWSLogs1** e **AWSLogs2** come valori per una condizione, qualsiasi oggetto la cui chiave inizia con AWSLogs1 o AWSLogs2 corrisponde ai criteri della condizione.

Quando inserite un valore per una condizione Prefix, tenete presente quanto segue:

- I valori distinguono tra maiuscole e minuscole
- Macie non supporta l'uso di caratteri jolly in questi valori.
- In Amazon S3, la chiave di un oggetto non include il nome del bucket che memorizza l'oggetto. Per questo motivo, non specificare i nomi dei bucket in questi valori.
- Se un prefisso include un delimitatore, includete il delimitatore nel valore. Ad esempio, immettete per definire una condizione **AWSLogs/eventlogs** per tutti gli oggetti la cui chiave inizia con /eventlogs. AWSLogs Macie supporta il delimitatore predefinito di Amazon S3, che è una barra (/), e i delimitatori personalizzati.

Tieni inoltre presente che un oggetto soddisfa i criteri di una condizione solo se la chiave dell'oggetto corrisponde esattamente al valore immesso, a partire dal primo carattere nella chiave dell'oggetto. Inoltre, Macie applica una condizione al valore Key completo di un oggetto, incluso il nome del file dell'oggetto.

Ad esempio, se la chiave di un oggetto è AWSLogs/eventlogs/testlog.csv e si inserisce uno dei seguenti valori per una condizione, l'oggetto soddisfa i criteri della condizione:

- **AWSLogs**

- **AWSLogs/event**
- **AWSLogs/eventlogs/**
- **AWSLogs/eventlogs/testlog**
- **AWSLogs/eventlogs/testlog.csv**

Tuttavia, se lo inserisci **eventlogs**, l'oggetto non corrisponde ai criteri: il valore della condizione non include la prima parte della chiave, /. AWSLogs Analogamente, se si immette **awslogs**, l'oggetto non corrisponde ai criteri a causa delle differenze nelle lettere maiuscole.

Dimensioni dello spazio di archiviazione

Ciò è correlato al campo Dimensione in Amazon S3. In Amazon S3, questo campo indica la dimensione totale di storage di un oggetto S3. Se un oggetto è un file compresso, questo valore non riflette la dimensione effettiva del file dopo la decompressione.

È possibile utilizzare questo tipo di condizione per includere o escludere oggetti più piccoli di una certa dimensione, più grandi di una certa dimensione o che rientrano in un determinato intervallo di dimensioni. Macie applica questo tipo di condizione a tutti i tipi di oggetti, compresi i file compressi o di archivio e i file in essi contenuti. Per informazioni sulle restrizioni basate sulle dimensioni per ogni formato supportato, consulta [Quote per Macie](#)

Tag

I tag associati a un oggetto S3. I tag sono etichette che è possibile definire e assegnare a determinati tipi di AWS risorse, inclusi gli oggetti S3. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Per informazioni sull'etichettatura degli oggetti S3, consulta [Categorizzazione dello storage mediante tag nella Guida per l'utente](#) di Amazon Simple Storage Service.

Per un processo di rilevamento di dati sensibili, puoi utilizzare questo tipo di condizione per includere o escludere oggetti con un tag specifico. Può trattarsi di una chiave di tag specifica o di una chiave di tag e di un valore di tag specifici (in coppia). Se specifichi più tag come valori per una condizione, Macie usa la logica OR per unire i valori. Ad esempio, se specifichi **Project1** e utilizzi **Project2** come chiavi di tag per una condizione, qualsiasi oggetto che ha la chiave di tag Project1 o Project2 soddisfa i criteri della condizione.

Nota che le chiavi e i valori dei tag fanno distinzione tra maiuscole e minuscole. Inoltre, Macie non supporta l'uso di valori parziali o caratteri jolly in questo tipo di condizione.

Creazione di un processo di rilevamento dei dati sensibili

Con Amazon Macie, puoi creare ed eseguire processi di rilevamento di dati sensibili per automatizzare il rilevamento, la registrazione e il reporting di dati sensibili nei bucket generici di Amazon Simple Storage Service (Amazon S3). Un processo di rilevamento di dati sensibili è una serie di attività di elaborazione e analisi automatizzate che Macie esegue per rilevare e segnalare dati sensibili negli oggetti Amazon S3. Man mano che l'analisi procede, Macie fornisce report dettagliati sui dati sensibili che trova e sulle analisi che esegue: i risultati dei dati sensibili, che riportano i dati sensibili che Macie trova nei singoli oggetti S3, e i risultati della scoperta dei dati sensibili, che registrano i dettagli sull'analisi dei singoli oggetti S3. Per ulteriori informazioni, consulta [Revisione dei risultati del lavoro](#).

Quando crei un job, inizi specificando quali bucket S3 memorizzano gli oggetti che vuoi che Macie analizzi durante l'esecuzione del job: bucket specifici che selezioni o bucket che soddisfano criteri specifici. Quindi specifichi la frequenza con cui eseguire il lavoro, una volta o periodicamente su base giornaliera, settimanale o mensile. Puoi anche scegliere delle opzioni per affinare l'ambito dell'analisi del lavoro. Le opzioni includono criteri personalizzati che derivano dalle proprietà degli oggetti S3, come tag, prefissi e data dell'ultima modifica di un oggetto.

Dopo aver definito la pianificazione e l'ambito del lavoro, si specifica quali identificatori di dati gestiti e identificatori di dati personalizzati utilizzare:

- Un identificatore di dati gestito è un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili, ad esempio numeri di carte di credito, chiavi di accesso AWS segrete o numeri di passaporto per un determinato paese o area geografica. Questi identificatori sono in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili per molti paesi e aree geografiche, inclusi diversi tipi di dati relativi alle credenziali, informazioni finanziarie e informazioni di identificazione personale (PII). Per ulteriori informazioni, consulta [Utilizzo di identificatori di dati gestiti](#).
- Un identificatore di dati personalizzato è un insieme di criteri definiti per rilevare dati sensibili. Con gli identificatori di dati personalizzati, puoi rilevare dati sensibili che riflettono scenari particolari, proprietà intellettuale o dati proprietari dell'organizzazione, ad esempio dipendenti IDs, numeri di account dei clienti o classificazioni interne dei dati. Puoi integrare gli identificatori di dati gestiti forniti da Macie. Per ulteriori informazioni, consulta [Creazione di identificatori di dati personalizzati](#).

È quindi possibile selezionare facoltativamente l'opzione Consenti l'uso degli elenchi. In Macie, un elenco consentito specifica il testo o uno schema di testo da ignorare. Si tratta in genere di eccezioni

relative ai dati sensibili per scenari o ambienti particolari, ad esempio nomi o numeri di telefono pubblici dell'organizzazione o dati di esempio utilizzati dall'organizzazione per i test. Per ulteriori informazioni, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).

Quando hai finito di scegliere queste opzioni, sei pronto per inserire le impostazioni generali del lavoro, come il nome e la descrizione del lavoro. Potrai quindi rivedere e salvare il lavoro.

Attività

- [Prima di iniziare: imposta le risorse chiave](#)
- [Passaggio 1: scegli i bucket S3](#)
- [Passaggio 2: rivedi le selezioni o i criteri del bucket S3](#)
- [Fase 3: Definire la pianificazione e ridefinire l'ambito](#)
- [Passaggio 4: selezionare gli identificatori di dati gestiti](#)
- [Passaggio 5: Seleziona identificatori di dati personalizzati](#)
- [Passaggio 6: Seleziona gli elenchi consentiti](#)
- [Passo 7: Inserisci le impostazioni generali](#)
- [Fase 8: Rivedi e crea](#)

Prima di iniziare: imposta le risorse chiave

Prima di creare un'offerta di lavoro, è consigliabile eseguire le seguenti operazioni:

- Verifica di aver configurato un repository per i risultati del rilevamento dei dati sensibili. A tale scopo, scegli Risultati Discovery nel riquadro di navigazione sulla console Amazon Macie. Per ulteriori informazioni su queste impostazioni, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).
- Crea qualsiasi identificatore di dati personalizzato che desideri venga utilizzato dal job. Per scoprire come, consulta [Creazione di identificatori di dati personalizzati](#).
- Crea tutti gli elenchi di autorizzazioni che desideri vengano utilizzati dal job. Per scoprire come, consulta [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#).
- Se desideri analizzare oggetti S3 crittografati, assicurati che Macie possa accedere e utilizzare le chiavi di crittografia appropriate. Per ulteriori informazioni, consulta [Analisi di oggetti S3 crittografati](#).

- Se desideri analizzare gli oggetti in un bucket S3 con una politica restrittiva sui bucket, assicurati che Macie sia autorizzato ad accedere agli oggetti. Per ulteriori informazioni, consulta [Consentire a Macie di accedere a bucket e oggetti S3](#).

Se si eseguono queste operazioni prima di creare un lavoro, si semplifica la creazione del lavoro e si contribuisce a garantire che il lavoro possa analizzare i dati desiderati.

Passaggio 1: scegli i bucket S3

Quando crei un lavoro, il primo passo è specificare in quali bucket S3 sono archiviati gli oggetti che vuoi che Macie analizzi durante l'esecuzione del lavoro. Per questo passaggio, hai due opzioni:

- **Seleziona bucket specifici:** con questa opzione, selezioni esplicitamente ogni bucket S3 da analizzare. Quindi, quando il processo viene eseguito, Macie analizza gli oggetti solo nei bucket selezionati.
- **Specificare i criteri dei bucket:** con questa opzione, si definiscono i criteri di runtime che determinano quali bucket S3 analizzare. I criteri consistono in una o più condizioni che derivano dalle proprietà del bucket. Quindi, quando il processo viene eseguito, Macie identifica i bucket che corrispondono ai criteri specificati e analizza gli oggetti in tali bucket.

Per informazioni dettagliate su queste opzioni, consulta [Opzioni relative all'ambito per i processi](#).

Le seguenti sezioni forniscono istruzioni per la scelta e la configurazione di ciascuna opzione. Scegliete la sezione relativa all'opzione desiderata.

Seleziona secchi specifici

Se scegli di selezionare esplicitamente ogni bucket S3 da analizzare, Macie ti fornisce un inventario dei bucket generici attualmente utilizzati. Regione AWS Puoi quindi utilizzare questo inventario per selezionare uno o più bucket per il lavoro. Per ulteriori informazioni su questo inventario, consulta [Selezione di bucket S3 specifici](#).

Se sei l'amministratore Macie di un'organizzazione, l'inventario include i bucket di proprietà degli account dei membri della tua organizzazione. Puoi selezionare fino a 1.000 di questi bucket, che coprono fino a 1.000 account.

Per selezionare bucket S3 specifici per il lavoro

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>

2. Nel riquadro di navigazione scegliere Jobs (Processi).
3. Scegli Crea processo.
4. Nella pagina Scegli i bucket S3, scegli Seleziona bucket specifici. Macie mostra una tabella con tutti i bucket generici del tuo account nella regione corrente.
5. Nella sezione Seleziona i bucket S3, scegli facoltativamente refresh



per recuperare i metadati dei bucket più recenti da Amazon S3.

Se l'icona delle informazioni



appare accanto ai nomi dei bucket, ti consigliamo di farlo. [Questa icona indica che un bucket è stato creato nelle ultime 24 ore, probabilmente dopo l'ultima volta che Macie ha recuperato i metadati del bucket e dell'oggetto da Amazon S3 come parte del ciclo di aggiornamento giornaliero.](#)

6. Nella tabella, seleziona la casella di controllo per ogni bucket che desideri venga analizzato dal job.

Tip

- Per trovare più facilmente bucket specifici, inserisci i criteri di filtro nella casella del filtro sopra la tabella. Puoi anche ordinare la tabella scegliendo un'intestazione di colonna.
- Per determinare se hai già configurato un lavoro per analizzare periodicamente gli oggetti in un bucket, consulta il campo Monitorato dal lavoro. Se in un campo viene visualizzato Sì, il bucket viene incluso in modo esplicito in un processo periodico oppure il bucket corrisponde ai criteri per un processo periodico nelle ultime 24 ore. Inoltre, lo stato di almeno uno di questi lavori non è Annullato. Macie aggiorna questi dati su base giornaliera.
- Per determinare quando un processo periodico o occasionale esistente ha analizzato più di recente gli oggetti in un bucket, consulta il campo Ultimo processo eseguito. Per ulteriori informazioni su quel lavoro, consulta i dettagli del bucket.
- Per visualizzare i dettagli di un bucket, scegli il nome del bucket. Oltre alle informazioni relative al lavoro, il pannello dei dettagli fornisce statistiche e altre informazioni sul

bucket, come le impostazioni di accesso pubblico del bucket. Per ulteriori informazioni su questi dati, consulta. [Revisione dell'inventario dei bucket S3](#)

7. Quando hai finito di selezionare i bucket, scegli Avanti.

Nel passaggio successivo, esaminerai e verificherai le tue selezioni.

Specificate i criteri del bucket

Se scegli di specificare criteri di runtime che determinano quali bucket S3 analizzare, Macie fornisce opzioni per aiutarti a scegliere campi, operatori e valori per le singole condizioni nei criteri. Per ulteriori informazioni su queste opzioni, consulta [Specificazione dei criteri del bucket S3](#).

Per specificare i criteri del bucket S3 per il job

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi).
3. Scegli Crea processo.
4. Nella pagina Scegli i bucket S3, scegli Specificare i criteri del bucket.
5. In Specificare i criteri del bucket, procedi come segue per aggiungere una condizione ai criteri:
 - a. Posizionate il cursore nella casella del filtro, quindi scegliete la proprietà del bucket da utilizzare per la condizione.
 - b. Nella prima casella, scegli un operatore per la condizione, Uguale o Non è uguale.
 - c. Nella casella successiva, inserisci uno o più valori per la proprietà.

A seconda del tipo e della natura della proprietà del bucket, Macie mostra diverse opzioni per l'immissione dei valori. Ad esempio, se si sceglie la proprietà Autorizzazione effettiva, Macie visualizza un elenco di valori tra cui scegliere. Se scegliete la proprietà Account ID, Macie visualizza una casella di testo in cui potete inserirne uno o più. Account AWS IDs Per inserire più valori in una casella di testo, inserisci ogni valore e separa ogni voce con una virgola.

- d. Scegli Applica. Macie aggiunge la condizione e la visualizza sotto la casella del filtro.

Per impostazione predefinita, Macie aggiunge la condizione con un'istruzione include. Ciò significa che il job è configurato per analizzare (includere) oggetti nei bucket che

corrispondono alla condizione. Per saltare (escludere) i bucket che corrispondono alla condizione, scegli **Includi** per la condizione, quindi scegli **Escludi**.

- e. Ripeti i passaggi precedenti per ogni condizione aggiuntiva che desideri aggiungere ai criteri.
6. Per verificare i criteri, espandi la sezione **Visualizza in anteprima** i risultati dei criteri. Questa sezione mostra una tabella con un massimo di 25 bucket generici che attualmente soddisfano i criteri.
7. Per rifinire i criteri, esegui una delle seguenti operazioni:
 - Per rimuovere una condizione, scegliete **X** come condizione.
 - Per modificare una condizione, rimuovila scegliendo **X** come condizione. Quindi aggiungi una condizione con le impostazioni corrette.
 - Per rimuovere tutte le condizioni, scegli **Cancella filtri**.

Macie aggiorna la tabella dei risultati dei criteri in base alle modifiche apportate.

8. Quando hai finito di specificare i criteri del bucket, scegli **Avanti**.

Nel passaggio successivo, esaminerai e verificherai i tuoi criteri.

Passaggio 2: rivedi le selezioni o i criteri del bucket S3

Per questo passaggio, verifica di aver scelto le impostazioni corrette nel passaggio precedente:

- Rivedi le selezioni dei bucket - Se hai selezionato bucket S3 specifici per il lavoro, esamina la tabella dei bucket e modifica le selezioni dei bucket se necessario. La tabella fornisce informazioni sull'ambito e sul costo previsti dell'analisi del job. I dati si basano sulle dimensioni e sui tipi di oggetti attualmente archiviati in un bucket.

Nella tabella, il campo **Costo stimato** indica il costo totale stimato (in dollari USA) dell'analisi degli oggetti in un bucket S3. Ogni stima riflette la quantità prevista di dati non compressi che il job analizzerà in un bucket. Se alcuni oggetti sono file compressi o archiviati, la stima presuppone che i file utilizzino un rapporto di compressione 3:1 e che il lavoro sia in grado di analizzare tutti i file estratti. Per ulteriori informazioni, consulta [Previsione e monitoraggio dei costi del lavoro](#).

- Rivedi i criteri del bucket - Se hai specificato i criteri del bucket per il lavoro, esamina ogni condizione nei criteri. Per modificare i criteri, scegliete **Precedente**, quindi utilizzate le opzioni di filtro nel passaggio precedente per inserire i criteri corretti. Al termine, selezionare **Next (Avanti)**.

Al termine della revisione e della verifica delle impostazioni, scegliete Avanti.

Fase 3: Definire la pianificazione e ridefinire l'ambito

Per questo passaggio, specifica la frequenza con cui desideri che il processo venga eseguito, una volta o periodicamente su base giornaliera, settimanale o mensile. Scegliete anche varie opzioni per affinare l'ambito dell'analisi del lavoro. Per maggiori informazioni su queste opzioni, consulta [Opzioni relative all'ambito per i processi](#).

Per definire la pianificazione e rifinire l'ambito del lavoro

1. Nella pagina Perfeziona l'ambito, specifica la frequenza con cui desideri che il processo venga eseguito:
 - Per eseguire il lavoro solo una volta, subito dopo aver finito di crearlo, scegli Processo singolo.
 - Per eseguire il lavoro periodicamente su base ricorrente, scegli Processo pianificato. Per Frequenza di aggiornamento, scegli se eseguire il processo giornalmente, settimanalmente o mensilmente. Quindi utilizzate l'opzione Includi oggetti esistenti per definire l'ambito della prima esecuzione del lavoro:
 - Selezionate questa casella di controllo per analizzare tutti gli oggetti esistenti subito dopo aver terminato la creazione del lavoro. Ogni esecuzione successiva analizza solo gli oggetti che vengono creati o modificati dopo l'esecuzione precedente.
 - Deselezionate questa casella di controllo per saltare l'analisi di tutti gli oggetti esistenti. La prima esecuzione del processo analizza solo gli oggetti che vengono creati o modificati dopo aver terminato la creazione del lavoro e prima dell'inizio della prima esecuzione. Ogni esecuzione successiva analizza solo gli oggetti che vengono creati o modificati dopo l'esecuzione precedente.

La deselezionazione di questa casella di controllo è utile nei casi in cui hai già analizzato i dati e desideri continuare ad analizzarli periodicamente. Ad esempio, se in precedenza hai utilizzato un altro servizio o un'applicazione per classificare i dati e hai recentemente iniziato a utilizzare Macie, puoi utilizzare questa opzione per garantire la continua scoperta e classificazione dei dati senza incorrere in costi inutili o duplicare i dati di classificazione.

2. (Facoltativo) Per specificare la percentuale di oggetti che si desidera che il lavoro analizzi, immettete la percentuale nella casella Profondità di campionamento.

Se questo valore è inferiore al 100%, Macie seleziona gli oggetti da analizzare a caso, fino alla percentuale specificata, e analizza tutti i dati in quegli oggetti. Il valore predefinito è 100%.

3. (Facoltativo) Per aggiungere criteri specifici che determinano quali oggetti S3 sono inclusi o esclusi dall'analisi del job, espandi la sezione Impostazioni aggiuntive, quindi inserisci i criteri. Questi criteri consistono in condizioni individuali che derivano dalle proprietà degli oggetti:
 - Per analizzare (includere) oggetti che soddisfano una condizione specifica, inserite il tipo e il valore della condizione, quindi scegliete Includi.
 - Per ignorare (escludere) gli oggetti che soddisfano una condizione specifica, inserite il tipo e il valore della condizione, quindi scegliete Escludi.

Ripeti questo passaggio per ogni condizione di inclusione o esclusione che desideri.

Se inserisci più condizioni, tutte le condizioni di esclusione hanno la precedenza sulle condizioni di inclusione. Ad esempio, se si includono oggetti con estensione pdf ed si escludono oggetti di dimensioni superiori a 5 MB, il processo analizza qualsiasi oggetto con estensione pdf, a meno che l'oggetto non sia più grande di 5 MB.

4. Al termine, selezionare Next (Avanti).

Passaggio 4: selezionare gli identificatori di dati gestiti

Per questo passaggio, specifica quali identificatori di dati gestiti desideri che il job utilizzi quando analizza gli oggetti S3. Sono disponibili due opzioni:

- Usa le impostazioni consigliate - Con questa opzione, il job analizza gli oggetti S3 utilizzando il set di identificatori di dati gestiti che consigliamo per i lavori. Questo set è progettato per rilevare categorie e tipi comuni di dati sensibili. Per esaminare un elenco di identificatori di dati gestiti attualmente presenti nel set, vedere [Identificatori di dati gestiti consigliati per i lavori](#). Aggiorniamo tale elenco ogni volta che aggiungiamo o rimuoviamo un identificatore di dati gestito dal set.
- Usa impostazioni personalizzate - Con questa opzione, il job analizza gli oggetti S3 utilizzando identificatori di dati gestiti selezionati dall'utente. Questi possono essere tutti o solo alcuni degli identificatori di dati gestiti attualmente disponibili. È inoltre possibile configurare il processo in modo che non utilizzi alcun identificatore di dati gestito. Il processo può invece utilizzare solo identificatori di dati personalizzati selezionati nel passaggio successivo. Per esaminare un elenco di identificatori di dati gestiti attualmente disponibili, consulta. [Riferimento rapido: identificatori di dati gestiti per tipo](#) Aggiorniamo tale elenco ogni volta che rilasciamo un nuovo identificatore di dati gestiti.

Quando scegli una delle due opzioni, Macie visualizza una tabella di identificatori di dati gestiti. Nella tabella, il campo Tipo di dati sensibili specifica l'identificatore univoco (ID) per un identificatore di dati gestito. Questo ID descrive il tipo di dati sensibili che l'identificatore di dati gestito è progettato per rilevare, ad esempio: `USA_PASSPORT_NUMBER` per i numeri di passaporto statunitensi, `CREDIT_CARD_NUMBER` per i numeri di carta di credito e `PGP_PRIVATE_KEY` per le chiavi private PGP. Per trovare identificatori specifici più rapidamente, puoi ordinare e filtrare la tabella per categoria o tipo di dati sensibili.

Per selezionare gli identificatori di dati gestiti per il lavoro

1. Nella pagina Seleziona identificatori di dati gestiti, in Opzioni di identificatori di dati gestiti, esegui una delle seguenti operazioni:

- Per utilizzare il set di identificatori di dati gestiti consigliato per i lavori, scegli Consigliato.

Se scegli questa opzione e hai configurato il processo per essere eseguito più di una volta, ogni esecuzione utilizza automaticamente tutti gli identificatori di dati gestiti presenti nel set consigliato all'avvio dell'esecuzione. Ciò include nuovi identificatori di dati gestiti che rilasciamo e aggiungiamo al set. Sono esclusi gli identificatori di dati gestiti che rimuoviamo dal set e che non consigliamo più per i lavori.

- Per utilizzare solo identificatori di dati gestiti specifici selezionati, scegli Personalizzato, quindi scegli Usa identificatori di dati gestiti specifici. Quindi, nella tabella, seleziona la casella di controllo per ogni identificatore di dati gestiti che desideri venga utilizzato dal processo.

Se scegli questa opzione e hai configurato il processo per essere eseguito più di una volta, ogni esecuzione utilizza solo gli identificatori di dati gestiti selezionati. In altre parole, il processo utilizza gli stessi identificatori di dati gestiti ogni volta che viene eseguito.

- Per utilizzare tutti gli identificatori di dati gestiti attualmente forniti da Macie, scegli Personalizzato, quindi scegli Usa identificatori di dati gestiti specifici. Quindi, nella tabella, seleziona la casella di controllo nell'intestazione della colonna di selezione per selezionare tutte le righe.

Se scegli questa opzione e hai configurato il processo per essere eseguito più di una volta, ogni esecuzione utilizza solo gli identificatori di dati gestiti selezionati. In altre parole, il processo utilizza gli stessi identificatori di dati gestiti ogni volta che viene eseguito.

- Per non utilizzare identificatori di dati gestiti e utilizzare solo identificatori di dati personalizzati, scegli Personalizzato, quindi scegli Non utilizzare identificatori di dati gestiti. Quindi, nel passaggio successivo, seleziona gli identificatori di dati personalizzati da utilizzare.

2. Al termine, selezionare Next (Avanti).

Passaggio 5: Seleziona identificatori di dati personalizzati

Per questo passaggio, selezionate gli identificatori di dati personalizzati che desiderate che il job utilizzi quando analizza gli oggetti S3. Il lavoro utilizzerà gli identificatori selezionati in aggiunta a tutti gli identificatori di dati gestiti per cui è stato configurato il lavoro. Per ulteriori informazioni sugli identificatori di dati personalizzati, consulta. [Creazione di identificatori di dati personalizzati](#)

Per selezionare identificatori di dati personalizzati per il lavoro

1. Nella pagina Seleziona identificatori di dati personalizzati, seleziona la casella di controllo per ogni identificatore di dati personalizzato che desideri venga utilizzato dal processo. Puoi selezionare fino a 30 identificatori di dati personalizzati.

Tip

Per rivedere o testare le impostazioni per un identificatore di dati personalizzato prima di selezionarlo, scegli l'icona del link



accanto al nome dell'identificatore. Macie apre una pagina che mostra le impostazioni dell'identificatore.

Puoi anche usare questa pagina per testare l'identificatore con dati di esempio. A tale scopo, inserisci fino a 1.000 caratteri di testo nella casella Dati di esempio, quindi scegli Test. Macie valuta i dati di esempio utilizzando l'identificatore, quindi riporta il numero di corrispondenze.

2. Al termine della selezione degli identificatori di dati personalizzati, scegli Avanti.

Passaggio 6: Seleziona gli elenchi consentiti

Per questo passaggio, selezionate gli elenchi di autorizzazione che desiderate che il job utilizzi quando analizza gli oggetti S3. Per ulteriori informazioni sugli elenchi consentiti, consulta. [Definizione delle eccezioni relative ai dati sensibili con gli elenchi consentiti](#)

Per selezionare gli elenchi consentiti per il lavoro

1. Nella pagina **Seleziona gli elenchi consentiti**, seleziona la casella di controllo per ogni elenco consentito che desideri venga utilizzato dal lavoro. Puoi selezionare fino a 10 elenchi.

Tip

Per rivedere le impostazioni di un elenco consentito prima di selezionarlo, scegli l'icona del collegamento



accanto al nome dell'elenco. Macie apre una pagina che mostra le impostazioni dell'elenco.

Se l'elenco specifica un'espressione regolare (regex), puoi anche usare questa pagina per testare l'espressione regolare con dati di esempio. A tale scopo, inserisci fino a 1.000 caratteri di testo nella casella **Dati di esempio**, quindi scegli **Test**. Macie valuta i dati di esempio utilizzando l'espressione regolare, quindi riporta il numero di corrispondenze.

2. Quando hai finito di selezionare gli elenchi consentiti, scegli **Avanti**.

Passo 7: Inserisci le impostazioni generali

Per questo passaggio, specifica un nome e, facoltativamente, una descrizione del lavoro. È inoltre possibile assegnare tag al lavoro. Un tag è un'etichetta che definisci e assigni a determinati tipi di AWS risorse. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

Per inserire le impostazioni generali per il lavoro

1. Nella pagina **Inserisci impostazioni generali**, inserisci un nome per il lavoro nella casella **Nome lavoro**. Il nome può contenere fino a un massimo di 500 caratteri.
2. (Facoltativo) In **Descrizione del lavoro**, inserire una breve descrizione del lavoro. La descrizione può contenere fino a 200 caratteri.
3. (Facoltativo) Per **Tag**, scegli **Aggiungi tag**, quindi inserisci fino a 50 tag da assegnare al lavoro.
4. Al termine, selezionare **Next (Avanti)**.

Fase 8: Rivedi e crea

Per questo passaggio finale, rivedi le impostazioni di configurazione del lavoro e verifica che siano corrette. Si tratta di un passo importante. Dopo aver creato un lavoro, non puoi modificare nessuna di queste impostazioni. Questo aiuta a garantire una cronologia immutabile delle rilevazioni e dei risultati delle scoperte di dati sensibili per i controlli o le indagini sulla privacy e la protezione dei dati da te eseguiti.

A seconda delle impostazioni del lavoro, puoi anche rivedere il costo totale stimato (in dollari USA) dell'esecuzione del lavoro una sola volta. Se hai selezionato bucket S3 specifici per il job, la stima si basa sulle dimensioni e sui tipi di oggetti nei bucket selezionati e sulla quantità di dati che il job può analizzare. Se hai specificato dei criteri relativi ai bucket per il job, la stima si basa sulle dimensioni e sui tipi di oggetti contenuti in un massimo di 500 bucket che attualmente soddisfano i criteri e sulla quantità di dati che il job può analizzare. Per maggiori informazioni su questa stima, consulta.

[Previsione e monitoraggio dei costi del lavoro](#)

Per rivedere e creare il lavoro

1. Nella pagina Rivedi e crea, rivedi ogni impostazione e verifica che sia corretta. Per modificare un'impostazione, scegli Modifica nella sezione che contiene l'impostazione, quindi inserisci l'impostazione corretta. Puoi anche utilizzare le schede di navigazione per andare alla pagina che contiene un'impostazione.
2. Al termine della verifica delle impostazioni, scegli Invia per creare e salvare il lavoro. Macie controlla le impostazioni e ti avvisa di eventuali problemi da risolvere.

Note

Se non hai configurato un repository per i risultati del rilevamento dei dati sensibili, Macie visualizza un avviso e non salva il lavoro. Per risolvere questo problema, scegli Configura nella sezione Repository for sensitive data discovery results. Quindi inserisci le impostazioni di configurazione per il repository. Per scoprire come, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#). Dopo aver inserito le impostazioni, torna alla pagina Rivedi e crea e scegli refresh



) nella sezione Repository for sensitive data discovery results della pagina.

Sebbene non sia consigliabile, puoi temporaneamente ignorare i requisiti del repository e salvare il lavoro. Se lo fai, rischi di perdere i risultati di discovery del processo: Macie

conserva i risultati solo per 90 giorni. Per sostituire temporaneamente il requisito, seleziona la casella di controllo relativa all'opzione di sostituzione.

3. Se Macie ti notifica dei problemi da risolvere, risolvi i problemi, quindi scegli nuovamente **Invia** per creare e salvare il lavoro.

Se hai configurato il lavoro in modo che venga eseguito una volta, su base giornaliera o nel giorno corrente della settimana o del mese, Macie inizia a eseguire il lavoro immediatamente dopo averlo salvato. Altrimenti, Macie si prepara a eseguire il lavoro nel giorno della settimana o del mese specificato. Per monitorare il lavoro, puoi [controllarne lo stato](#).

Analisi dei risultati di un processo di rilevamento di dati sensibili

Quando esegui un processo di rilevamento di dati sensibili, Amazon Macie calcola e riporta automaticamente determinati dati statistici relativi al processo. Ad esempio, Macie riporta il numero di volte in cui il job è stato eseguito e il numero approssimativo di oggetti Amazon Simple Storage Service (Amazon S3) che il job deve ancora elaborare durante l'esecuzione corrente. Macie produce anche diversi tipi di risultati per il job: eventi di log, rilevamenti di dati sensibili e risultati di scoperta di dati sensibili.

Argomenti

- [Tipi di risultati per i lavori di rilevamento di dati sensibili](#)
- [Revisione delle statistiche e dei risultati per un lavoro di rilevamento di dati sensibili](#)

Tipi di risultati per i lavori di rilevamento di dati sensibili

Man mano che un processo di individuazione di dati sensibili procede, Amazon Macie produce i seguenti tipi di risultati per il processo.

Registra evento

Si tratta di un record di un evento che si è verificato durante l'esecuzione del processo. Macie registra e pubblica automaticamente i dati per determinati eventi su Amazon Logs. CloudWatch I dati contenuti in questi registri registrano le modifiche all'avanzamento o allo stato del lavoro, ad esempio la data e l'ora esatte in cui il lavoro è iniziato o ha smesso di funzionare. I dati forniscono anche dettagli su eventuali errori a livello di account o bucket che si sono verificati durante l'esecuzione del job.

Gli eventi di registro possono aiutarti a monitorare un processo e a risolvere eventuali problemi che impedivano al job di analizzare i dati desiderati. Se un job utilizza criteri di runtime per determinare quali bucket S3 analizzare, gli eventi di registro possono anche aiutarti a determinare se e quali bucket S3 corrispondevano ai criteri al momento dell'esecuzione del job.

Puoi accedere agli eventi di registro utilizzando la CloudWatch console Amazon o l'API Amazon CloudWatch Logs. Per aiutarti a navigare tra gli eventi di registro di un processo, la console Amazon Macie fornisce un collegamento ad essi. Per ulteriori informazioni, consulta [Monitoraggio dei lavori con CloudWatch Logs](#).

Ricerca di dati sensibili

Questo è un rapporto di dati sensibili che Macie ha trovato in un oggetto S3. Ogni risultato fornisce un indice di gravità e dettagli come:

- La data e l'ora in cui Macie ha trovato i dati sensibili.
- La categoria e i tipi di dati sensibili trovati da Macie.
- Il numero di occorrenze di ogni tipo di dati sensibili rilevati da Macie.
- L'identificatore univoco del lavoro che ha prodotto il risultato.
- Il nome, le impostazioni di accesso pubblico, il tipo di crittografia e altre informazioni sul bucket S3 e sull'oggetto interessati.

A seconda del tipo di file o del formato di archiviazione dell'oggetto S3 interessato, i dettagli possono includere anche la posizione di ben 15 occorrenze dei dati sensibili trovati da Macie. Per riportare i dati sulla posizione, i dati sensibili rilevati utilizzano uno schema JSON [standardizzato](#).

Una ricerca di dati sensibili non include i dati sensibili trovati da Macie. Fornisce invece informazioni che è possibile utilizzare per ulteriori indagini e correzioni, se necessario.

Macie archivia i dati sensibili rilevati per 90 giorni. Puoi accedervi utilizzando la console Amazon Macie o l'API Amazon Macie. Puoi anche monitorarli ed elaborarli utilizzando altre applicazioni, servizi e sistemi. Per ulteriori informazioni, consulta [Revisione e analisi dei risultati](#).

Risultato della scoperta di dati sensibili

Questo è un record che registra i dettagli sull'analisi di un oggetto S3. Macie crea automaticamente un risultato di rilevamento dei dati sensibili per ogni oggetto per il quale configuri un processo per l'analisi. Ciò include oggetti in cui Macie non trova dati sensibili e quindi non produce risultati su dati sensibili, e oggetti che Macie non può analizzare a causa di errori o problemi come le impostazioni delle autorizzazioni o l'uso di un file o di un formato di archiviazione non supportato.

Se Macie trova dati sensibili in un oggetto S3, il risultato della scoperta dei dati sensibili include i dati della corrispondente ricerca di dati sensibili. Fornisce anche informazioni aggiuntive, come la posizione di ben 1.000 occorrenze di ogni tipo di dati sensibili che Macie ha trovato nell'oggetto. Per esempio:

- Il numero di colonna e di riga per una cella o un campo in una cartella di lavoro di Microsoft Excel, un file CSV o un file TSV
- Il percorso di un campo o di una matrice in un file JSON o JSON Lines
- Il numero di riga di una riga in un file di testo non binario diverso da un file CSV, JSON, JSON Lines o TSV, ad esempio un file HTML, TXT o XML
- Il numero di pagina di una pagina in un file Adobe Portable Document Format (PDF)
- L'indice dei record e il percorso di un campo in un record in un contenitore di oggetti Apache Avro o in un file Apache Parquet

Se l'oggetto S3 interessato è un file di archivio, ad esempio un file.tar o.zip, il risultato della scoperta dei dati sensibili fornisce anche dati dettagliati sulla posizione delle occorrenze di dati sensibili nei singoli file che Macie ha estratto dall'archivio. Macie non include queste informazioni nelle rilevazioni di dati sensibili per i file di archivio. Per riportare i dati sulla posizione, i risultati del rilevamento dei dati sensibili utilizzano uno schema [JSON standardizzato](#).

Un risultato di scoperta di dati sensibili non include i dati sensibili trovati da Macie. Fornisce invece un record di analisi che può essere utile per controlli o indagini sulla privacy e sulla protezione dei dati.

Macie archivia i risultati della scoperta dei dati sensibili per 90 giorni. Non puoi accedervi direttamente dalla console Amazon Macie o con l'API Amazon Macie. Invece, configuri Macie per crittografarli e archivarli in un bucket S3. Il bucket può fungere da archivio definitivo a lungo termine per tutti i risultati della scoperta di dati sensibili. È quindi possibile, facoltativamente, accedere e interrogare i risultati in tale repository. Per informazioni su come configurare queste impostazioni, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#)

Dopo aver configurato le impostazioni, Macie scrive i risultati del rilevamento dei dati sensibili in file JSON Lines (.jsonl), quindi li crittografa e aggiunge tali file al bucket S3 come file GNU Zip (.gz). Per aiutarti a navigare tra i risultati, la console Amazon Macie fornisce dei link ai risultati.

I risultati delle rilevazioni di dati sensibili e dei risultati della scoperta di dati sensibili aderiscono entrambi a schemi standardizzati. Questo può aiutarti facoltativamente a interrogarli, monitorarli ed elaborarli utilizzando altre applicazioni, servizi e sistemi.

Suggerimenti

Per un esempio dettagliato e istruttivo su come interrogare e utilizzare i risultati del rilevamento di dati sensibili per analizzare e segnalare potenziali rischi per la sicurezza dei dati, consulta il seguente post sul blog sulla AWS sicurezza: [Come interrogare e visualizzare i risultati del rilevamento dei dati sensibili di Macie con Amazon Athena](#) e Amazon. QuickSight Per esempi di query Amazon Athena da utilizzare per analizzare i risultati del rilevamento di dati sensibili, visita il repository di [Amazon Macie](#) Results Analytics su. GitHub Questo repository fornisce anche istruzioni per configurare Athena per recuperare e decrittografare i risultati e script per creare tabelle per i risultati.

Revisione delle statistiche e dei risultati per un lavoro di rilevamento di dati sensibili

Per esaminare le statistiche di elaborazione e i risultati di un processo di rilevamento di dati sensibili, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Segui questi passaggi per rivedere le statistiche e i risultati utilizzando la console.

Per accedere alle statistiche di elaborazione di un processo in modo programmatico, utilizza il [DescribeClassificationJob](#) funzionamento dell'API Amazon Macie. Per accedere programmaticamente ai risultati prodotti da un lavoro, utilizza l'[ListFindings](#) operazione e specifica l'identificatore univoco del lavoro in una condizione di filtro per il campo. `classificationDetails.jobId` Per scoprire come, consulta [Creazione e applicazione di filtri ai risultati di Macie](#). È quindi possibile utilizzare l'[GetFindings](#) operazione per recuperare i dettagli dei risultati.

Per esaminare le statistiche e i risultati di un lavoro

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi).
3. Nella pagina Lavori, scegli il nome del lavoro di cui desideri esaminare le statistiche e i risultati. Il pannello dei dettagli mostra statistiche, impostazioni e altre informazioni sul lavoro.
4. Nel pannello dei dettagli, effettuate una delle seguenti operazioni:
 - Per esaminare le statistiche di elaborazione relative al lavoro, consultate la sezione Statistiche del pannello. Questa sezione mostra statistiche come il numero di volte in cui il lavoro è stato eseguito e il numero approssimativo di oggetti che il lavoro deve ancora elaborare durante l'esecuzione corrente.

- Per esaminare gli eventi di registro relativi al processo, scegli Mostra risultati nella parte superiore del pannello, quindi scegli Mostra CloudWatch registri. Macie apre la CloudWatch console Amazon e visualizza una tabella degli eventi di registro che Macie ha pubblicato per il lavoro.
- Per esaminare tutti i dati sensibili rilevati dal lavoro, scegli Mostra risultati nella parte superiore del pannello, quindi scegli Mostra risultati. Macie apre la pagina dei risultati e mostra tutti i risultati del lavoro. Per esaminare i dettagli di un particolare risultato, scegli il risultato, quindi consulta il pannello dei dettagli.

Tip

Nel pannello dei dettagli del risultato, puoi utilizzare il link nel campo Posizione dettagliata dei risultati per passare al risultato di scoperta dei dati sensibili corrispondente in Amazon S3:

- Se il risultato si riferisce a un archivio di grandi dimensioni o a un file compresso, il link visualizza la cartella che contiene i risultati della ricerca del file. Un archivio o un file compresso è di grandi dimensioni se genera più di 100 risultati di ricerca.
 - Se il risultato si riferisce a un archivio o a un file compresso di piccole dimensioni, il link visualizza il file che contiene i risultati della ricerca per il file. Un archivio o un file compresso è di piccole dimensioni se genera 100 o meno risultati di rilevamento.
 - Se il risultato si applica a un altro tipo di file, il link visualizza il file che contiene i risultati della ricerca per il file.
- Per esaminare tutti i risultati della scoperta di dati sensibili prodotti dal lavoro, scegli Mostra risultati nella parte superiore del pannello, quindi scegli Mostra classificazioni. Macie apre la console Amazon S3 e visualizza la cartella che contiene tutti i risultati di scoperta del job. Questa opzione è disponibile solo dopo aver configurato Macie per [archiviare i risultati del rilevamento dei dati sensibili](#) in un bucket S3.

Gestione dei processi di rilevamento di dati sensibili

Per aiutarti a gestire i tuoi lavori di rilevamento di dati sensibili, Amazon Macie mantiene un inventario completo dei tuoi lavori in ciascuno di essi. Regione AWS Con questo inventario, puoi gestire i tuoi lavori come un'unica raccolta e accedere alle impostazioni di configurazione, alle statistiche di elaborazione e allo stato dei singoli lavori.

Ad esempio, puoi identificare tutti i lavori che hai configurato per essere eseguiti su base ricorrente per analisi, valutazione e monitoraggio periodici. È inoltre possibile esaminare un'analisi dettagliata delle impostazioni di configurazione per un lavoro. Ciò include le impostazioni che definiscono l'ambito dell'analisi. Include anche impostazioni che specificano i tipi di dati sensibili che Macie deve rilevare e segnalare durante l'esecuzione del lavoro. Se utilizzi la console Amazon Macie per gestire i tuoi lavori, i dettagli di ogni lavoro forniscono anche l'accesso diretto ai [dati sensibili rilevati e ad altri risultati prodotti](#) dal lavoro.

Oltre a queste attività, puoi creare varianti personalizzate di singoli lavori. È possibile copiare un lavoro esistente, modificare le impostazioni per la copia e quindi salvare la copia come nuovo lavoro. Ciò può essere utile nei casi in cui si desidera analizzare diversi set di dati nello stesso modo o lo stesso set di dati in modi diversi. Può anche essere utile se si desidera modificare le impostazioni di configurazione per un lavoro esistente: annullare il lavoro esistente, copiarlo, quindi modificare e salvare la copia come nuovo lavoro.

Argomenti

- [Revisione dell'inventario dei lavori di individuazione di dati sensibili](#)
- [Revisione delle impostazioni per un processo di rilevamento di dati sensibili](#)
- [Verifica dello stato di un processo di rilevamento di dati sensibili](#)
- [Modifica dello stato di un processo di rilevamento di dati sensibili](#)
- [Copiare un processo di rilevamento di dati sensibili](#)

Revisione dell'inventario dei lavori di individuazione di dati sensibili

Sulla console Amazon Macie, puoi esaminare un inventario completo dei tuoi attuali lavori di rilevamento di dati sensibili. Regione AWS L'inventario fornisce sia informazioni di riepilogo per tutti i tuoi lavori sia dettagli sui singoli lavori. Le informazioni di riepilogo includono: lo stato attuale di ogni processo, se un processo viene eseguito su base periodica e pianificata e se un lavoro è configurato per analizzare oggetti in specifici bucket Amazon Simple Storage Service (Amazon S3) o bucket S3 che soddisfano i criteri di runtime. Per i singoli lavori, puoi anche accedere a dettagli come un'analisi dettagliata delle impostazioni di configurazione del lavoro. Se un processo è già stato eseguito, i dettagli forniscono anche l'accesso diretto ai dati sensibili rilevati e ad altri tipi di risultati prodotti dal lavoro.

Per esaminare l'inventario delle offerte di lavoro

Segui questi passaggi per esaminare l'inventario dei lavori utilizzando la console Amazon Macie. Per accedere al tuo inventario in modo programmatico, utilizza il [ListClassificationJobs](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi). La pagina Lavori si apre e mostra il numero di lavori nel tuo inventario e una tabella di tali lavori.
3. Nella parte superiore della pagina, scegli facoltativamente refresh  per recuperare lo stato corrente di ogni lavoro.
4. Nella tabella Jobs, esamina le informazioni di riepilogo relative ai tuoi job:
 - Job name: il nome del job.
 - Risorse: indica se il job è configurato per analizzare oggetti in bucket S3 specifici o bucket che soddisfano i criteri di runtime. Se hai selezionato in modo esplicito i bucket per il lavoro da analizzare, questo campo indica il numero di bucket selezionati. Se il lavoro è stato configurato per utilizzare criteri di runtime, il valore di questo campo è Basato su criteri.
 - Tipo di job: se il job è configurato per essere eseguito una sola volta (una tantum) o su base pianificata e periodica (Scheduled).
 - Stato: lo stato attuale del lavoro. Per ulteriori informazioni su questo valore, vedere [Verifica dello stato di un lavoro](#).
 - Creato in: quando è stato creato il lavoro.
5. Per analizzare il tuo inventario o trovare un lavoro specifico più rapidamente, esegui una delle seguenti operazioni:
 - Per ordinare la tabella in base a un campo specifico, scegli l'intestazione di colonna del campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna.
 - Per mostrare solo i lavori che hanno un valore specifico per un campo, posiziona il cursore nella casella del filtro. Nel menu visualizzato, scegli il campo da utilizzare per il filtro e inserisci il valore per il filtro. Quindi, scegliere Apply (Applica).
 - Per nascondere i lavori che hanno un valore specifico per un campo, posiziona il cursore nella casella del filtro. Nel menu visualizzato, scegli il campo da utilizzare per il filtro e inserisci il valore per il filtro. Quindi, scegliere Apply (Applica). Nella casella del filtro, scegli l'icona uguale .

per il filtro. Questo modifica l'operatore del filtro da equals a not equals ().



- Per rimuovere un filtro, scegliete l'icona di rimozione del filtro



corrispondente al filtro da rimuovere.

6. Per esaminare le impostazioni e i dettagli aggiuntivi per un particolare lavoro, scegli il nome del lavoro. Quindi consulta il pannello dei dettagli. Per informazioni su questi dettagli, vedere [Revisione delle impostazioni di configurazione per un lavoro](#).

Revisione delle impostazioni per un processo di rilevamento di dati sensibili

Sulla console Amazon Macie, puoi utilizzare il pannello dei dettagli nella pagina Lavori per rivedere le impostazioni di configurazione e altre informazioni sui singoli processi di rilevamento di dati sensibili. Ad esempio, puoi consultare un elenco dei bucket Amazon Simple Storage Service (Amazon S3) per i quali un job è configurato per analizzare. Puoi anche determinare quali identificatori di dati gestiti e personalizzati un job è configurato per utilizzare durante l'analisi degli oggetti in quei bucket.

Tieni presente che non puoi modificare alcuna impostazione di configurazione per un lavoro esistente. Ciò contribuisce a garantire una cronologia immutabile delle rilevazioni e dei risultati delle scoperte di dati sensibili per i controlli o le indagini sulla privacy e la protezione dei dati da voi eseguiti.

[Se desideri modificare un lavoro esistente, puoi annullarlo](#). Quindi [copiate il lavoro](#), configurate la copia per utilizzare le impostazioni desiderate e salvate la copia come nuovo lavoro. In tal caso, è inoltre necessario adottare misure per garantire che il nuovo lavoro non analizzi nuovamente i dati esistenti nello stesso modo. A tale scopo, annota la data e l'ora in cui annulli il lavoro esistente. Quindi configurate l'ambito del nuovo lavoro in modo da includere solo gli oggetti che vengono creati o modificati dopo l'annullamento del lavoro originale. Ad esempio, è possibile utilizzare [i criteri degli oggetti](#) per definire una condizione di esclusione che specifica quando è stato annullato il lavoro originale.

Per rivedere le impostazioni di configurazione per un lavoro

Segui questi passaggi per rivedere le impostazioni di configurazione di un lavoro utilizzando la console Amazon Macie. Per rivedere le impostazioni a livello di codice, utilizza il [DescribeClassificationJob](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>

2. Nel riquadro di navigazione scegliere Jobs (Processi). La pagina Lavori si apre e mostra il numero di lavori nel tuo inventario e una tabella di tali lavori.
3. Nella tabella Lavori, scegli il nome del lavoro di cui desideri rivedere le impostazioni. Per trovare il lavoro più rapidamente, puoi filtrare la tabella utilizzando le opzioni di filtro sopra la tabella. È inoltre possibile ordinare la tabella in ordine crescente o decrescente in base a determinati campi.

Quando si sceglie un lavoro nella tabella, il pannello dei dettagli mostra le impostazioni di configurazione del lavoro e altre informazioni sul lavoro. A seconda delle impostazioni del lavoro, il pannello contiene le seguenti sezioni.

Informazioni generali

Questa sezione fornisce informazioni generali sulla mansione. Ad esempio, mostra l'Amazon Resource Name (ARN) del job, l'ultima data di avvio del job e lo stato corrente del job. Se hai messo in pausa il processo, questa sezione indica anche quando lo hai messo in pausa e quando il lavoro o l'ultima esecuzione del lavoro è scaduto o scadrà se non lo riprendi.

Statistiche

Questa sezione mostra le statistiche di elaborazione per il lavoro. Ad esempio, specifica il numero di volte in cui il job è stato eseguito e il numero approssimativo di oggetti S3 che il job deve ancora elaborare durante l'esecuzione corrente.

Scope (Ambito)

Questa sezione indica la frequenza di esecuzione del job. Mostra anche le impostazioni che perfezionano l'ambito del lavoro, ad esempio la [profondità di campionamento](#) e tutti i [criteri relativi agli oggetti che includono o escludono gli oggetti](#) S3 dall'analisi.

Bucket S3

Questa sezione viene visualizzata nel pannello se il lavoro è configurato per analizzare i bucket selezionati in modo esplicito al momento della creazione del lavoro. Indica il numero di elementi per Account AWS cui il job è configurato per analizzare i dati. Indica inoltre il numero di bucket che il job è configurato per analizzare e i nomi di tali bucket (raggruppati per account).

Per mostrare l'elenco completo degli account e dei bucket in formato JSON, scegli il numero nel campo Totale bucket.

Criteri del bucket S3

Questa sezione viene visualizzata nel pannello se il job utilizza criteri di runtime per determinare quali bucket analizzare. Elenca i criteri per cui il job è configurato. Per mostrare i criteri in formato JSON, scegli Dettagli. Quindi scegli la scheda Criteri nella finestra che appare.

Per esaminare un elenco di bucket che attualmente corrispondono ai criteri, scegli Dettagli. Quindi scegli la scheda Bucket corrispondenti nella finestra che appare. Facoltativamente, scegli refresh



per recuperare i dati più recenti. La scheda elenca fino a 25 bucket che attualmente corrispondono ai criteri.

Tip

Se il processo è già stato eseguito, puoi anche determinare se alcuni bucket corrispondevano ai criteri al momento dell'esecuzione del processo e, in caso affermativo, ai nomi di tali bucket. A tale scopo, esamina gli eventi di registro relativi al processo: scegli Mostra risultati nella parte superiore del pannello, quindi scegli Mostra registri. CloudWatch Macie apre la CloudWatch console Amazon e visualizza una tabella di eventi di registro per il lavoro. Gli eventi includono un BUCKET_MATCHED_THE_CRITERIA evento per ogni bucket che corrisponde ai criteri ed è stato incluso nell'analisi del job. Per ulteriori informazioni, consulta [Monitoraggio dei lavori con CloudWatch Logs](#).

Identificatori di dati personalizzati

Questa sezione viene visualizzata nel pannello se il lavoro è configurato per utilizzare uno o più [identificatori di dati personalizzati](#). Specifica i nomi di tali identificatori di dati personalizzati.

Consenti elenchi

Questa sezione viene visualizzata nel pannello se il lavoro è configurato per utilizzare uno o più [elenchi di autorizzazioni](#). Specifica i nomi di tali elenchi. Per rivedere le impostazioni e lo stato di un elenco, scegliete l'icona del collegamento



accanto al nome dell'elenco.

Identificatori di dati gestiti

Questa sezione indica per quali [identificatori di dati gestiti](#) è configurato il job. Ciò è determinato dal tipo di selezione dell'identificatore di dati gestito per il lavoro:

- Consigliato: utilizza gli identificatori di dati gestiti presenti nel [set consigliato](#) durante l'esecuzione del processo.
- Includi selezionati: utilizza solo gli identificatori di dati gestiti elencati nella sezione Selezioni.
- Includi tutto: utilizza tutti gli identificatori di dati gestiti disponibili durante l'esecuzione del processo.
- Escludi selezionati: utilizza tutti gli identificatori di dati gestiti disponibili durante l'esecuzione del processo, ad eccezione di quelli elencati nella sezione Selezioni.
- Escludi tutto: non utilizzare identificatori di dati gestiti. Utilizza solo gli identificatori di dati personalizzati specificati.

Per rivedere queste impostazioni in formato JSON, scegli Dettagli.

Tag

Questa sezione viene visualizzata nel pannello se i tag sono assegnati al lavoro. Elenca questi tag. Un tag è un'etichetta che definisci e assegni a determinati tipi di AWS risorse. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

Per rivedere e salvare le impostazioni del lavoro in formato JSON, scegli l'identificatore univoco per il lavoro (Job ID) nella parte superiore del pannello. Quindi scegli Scarica.

Verifica dello stato di un processo di rilevamento di dati sensibili

Quando si crea un processo di rilevamento di dati sensibili, il relativo stato iniziale è Attivo (In esecuzione) o Attivo (Inattivo), a seconda del tipo e della pianificazione del processo. Il lavoro passa quindi attraverso stati aggiuntivi, che è possibile monitorare man mano che il lavoro procede.

Tip

Oltre a monitorare lo stato generale di un lavoro, è possibile monitorare eventi specifici che si verificano man mano che un lavoro procede. Puoi farlo utilizzando i dati di registrazione che Amazon Macie pubblica automaticamente su Amazon Logs. CloudWatch I dati contenuti in questi log forniscono un registro delle modifiche allo stato di un processo e dettagli su eventuali errori a livello di account o bucket che si verificano durante l'esecuzione di un processo. Per ulteriori informazioni, consulta [Monitoraggio dei lavori con CloudWatch Logs](#).

Per verificare lo stato di un processo

Segui questi passaggi per verificare lo stato di un lavoro utilizzando la console Amazon Macie. Per controllare lo stato di un processo a livello di codice, utilizza il [DescribeClassificationJob](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi). La pagina Lavori si apre e mostra il numero di lavori nel tuo inventario e una tabella di tali lavori.
3. Nella parte superiore della pagina, scegli refresh  per recuperare lo stato corrente di ogni lavoro.
4. Nella tabella Jobs, individuate il job di cui desiderate controllare lo stato. Per trovare il lavoro più rapidamente, puoi filtrare la tabella utilizzando le opzioni di filtro sopra la tabella. È inoltre possibile ordinare la tabella in ordine crescente o decrescente in base a determinati campi.
5. Fate riferimento al campo Stato nella tabella. Questo campo indica lo stato attuale del lavoro.

Lo stato di un lavoro può essere uno dei seguenti.

Attivo (inattivo)

Per un processo periodico, l'esecuzione precedente è completa e la successiva esecuzione pianificata è in sospenso. Questo valore non si applica ai lavori occasionali.

Attivo (in esecuzione)

Per un lavoro occasionale, il lavoro è attualmente in corso. Per un processo periodico, è in corso un'esecuzione pianificata.

Annullato

Per qualsiasi tipo di lavoro, il lavoro è stato interrotto definitivamente (annullato).

Un lavoro ha questo stato se l'hai annullato esplicitamente o, se si tratta di un lavoro occasionale, hai messo in pausa il lavoro e non l'hai ripreso entro 30 giorni. Un lavoro può avere questo stato anche se in precedenza hai [sospeso](#) Macie in corso. Regione AWS

Completo

Per un processo singolo, il processo è stato eseguito correttamente e ora è completo. Questo valore non si applica ai lavori periodici. Al contrario, lo stato di un processo periodico diventa Attivo (Inattivo) quando ogni esecuzione viene completata correttamente.

In pausa (di Macie)

Per qualsiasi tipo di lavoro, il lavoro è stato interrotto temporaneamente (messo in pausa) da Macie.

Un lavoro ha questo stato se il completamento del lavoro o l'esecuzione di un lavoro supera la [quota mensile di rilevamento di dati sensibili](#) per il tuo account. Quando ciò accade, Macie mette automaticamente in pausa il lavoro. Macie riprende automaticamente il lavoro all'inizio del mese solare successivo e la quota mensile per il tuo account viene reimpostata, oppure tu aumenti la quota per il tuo account.

Se sei l'amministratore Macie di un'organizzazione e hai configurato il processo per analizzare i dati degli account dei membri, il job può avere questo stato anche se il completamento del lavoro o dell'esecuzione di un lavoro supera la quota mensile di scoperta di dati sensibili per un account membro.

Se un processo è in esecuzione e l'analisi degli oggetti idonei raggiunge questa quota per un account membro, il processo interrompe l'analisi degli oggetti di proprietà dell'account. Al termine dell'analisi degli oggetti per tutti gli altri account che non hanno raggiunto la quota, Macie sospende automaticamente il lavoro. Se si tratta di un lavoro una tantum, Macie lo riprende automaticamente all'inizio del mese di calendario successivo oppure la quota viene aumentata per tutti gli account interessati, a seconda dell'evento che si verifica per primo. Se si tratta di un processo periodico, Macie lo riprende automaticamente quando è programmato l'inizio dell'esecuzione successiva o inizia il mese di calendario successivo, a seconda di quale evento si verifica per primo. Se un'esecuzione pianificata inizia prima dell'inizio del mese di calendario successivo o la quota per un account interessato viene aumentata, il job non analizza gli oggetti di proprietà dell'account.

In pausa (per utente)

Per qualsiasi tipo di lavoro, il lavoro è stato temporaneamente interrotto (messo in pausa) dall'utente.

Se metti in pausa un lavoro occasionale e non lo riprendi entro 30 giorni, il lavoro scade e Macie lo annulla. Se metti in pausa un lavoro periodico mentre è in esecuzione e non lo riprendi entro

30 giorni, l'esecuzione del lavoro scade e Macie annulla l'esecuzione. Per verificare la data di scadenza di un processo o di un'esecuzione di lavoro in pausa, scegli il nome del lavoro nella tabella, quindi fai riferimento al campo Scadenze nella sezione Dettagli sullo stato del pannello dei dettagli.

Se un processo viene annullato o sospeso, è possibile fare riferimento ai dettagli del processo per determinare se il lavoro è iniziato a funzionare o, per un lavoro periodico, è stato eseguito almeno una volta prima di essere annullato o sospeso. A tale scopo, scegliete il nome del lavoro nella tabella Lavori, quindi fate riferimento al pannello dei dettagli. Nel pannello, il campo Numero di esecuzioni indica il numero di volte in cui il processo è stato eseguito. Il campo Ultima esecuzione indica la data e l'ora più recenti in cui il processo ha iniziato a essere eseguito.

A seconda dello stato corrente del lavoro, è possibile opzionalmente sospendere, riprendere o annullare il lavoro. Per ulteriori informazioni, consulta [Modifica dello stato di un lavoro](#).

Modifica dello stato di un processo di rilevamento di dati sensibili

Dopo aver creato un processo di rilevamento di dati sensibili, è possibile sospenderlo temporaneamente o annullarlo definitivamente. Quando metti in pausa un processo in esecuzione attiva, Amazon Macie inizia immediatamente a sospendere tutte le attività di elaborazione relative al lavoro. Quando annulli un lavoro in esecuzione attiva, Macie inizia immediatamente a interrompere tutte le attività di elaborazione relative al lavoro. Non puoi riprendere o riavviare un lavoro dopo che è stato annullato.

Se metti in pausa un lavoro occasionale, puoi riprenderlo entro 30 giorni. Quando riprendi il lavoro, Macie riprende immediatamente l'elaborazione dal punto in cui lo hai messo in pausa. Macie non riavvia il lavoro dall'inizio. Se non riprendi un lavoro occasionale entro 30 giorni dalla sua sospensione, il lavoro scade e Macie lo annulla.

Se metti in pausa un lavoro periodico, puoi riprenderlo in qualsiasi momento. Se riprendi un lavoro periodico e il lavoro era inattivo quando lo hai messo in pausa, Macie riprende il lavoro in base alla pianificazione e ad altre impostazioni di configurazione che hai scelto al momento della creazione del lavoro. Se riprendi un lavoro periodico e il lavoro era in esecuzione attivamente quando lo hai messo in pausa, il modo in cui Macie riprende il lavoro dipende da quando riprendi il lavoro:

- Se riprendi il lavoro entro 30 giorni dalla sua sospensione, Macie riprende immediatamente l'ultima esecuzione pianificata dal punto in cui hai messo in pausa il lavoro. Macie non riavvia l'esecuzione dall'inizio.

- Se non riprendi il lavoro entro 30 giorni dalla sua sospensione, l'ultima esecuzione pianificata scade e Macie annulla tutte le attività di elaborazione rimanenti per l'esecuzione. Quando successivamente riprendi il lavoro, Macie lo riprende in base alla pianificazione e ad altre impostazioni di configurazione che hai scelto al momento della creazione del lavoro.

Per aiutarti a determinare quando scadrà un lavoro o un'esecuzione di lavoro in pausa, Macie aggiunge una data di scadenza ai dettagli del lavoro mentre il lavoro è in pausa. Inoltre, ti informiamo circa sette giorni prima della scadenza del lavoro o dell'esecuzione del lavoro. Ti invieremo nuovamente una notifica quando il lavoro o l'esecuzione del lavoro scade e viene annullato. Per avvisarti, inviamo un'email all'indirizzo associato al tuo. Account AWS Creiamo anche AWS Health eventi e Amazon CloudWatch Events per il tuo account. Per controllare la data di scadenza utilizzando la console, scegli il nome del lavoro nella tabella della pagina Lavori. Quindi fai riferimento al campo Scadenze nella sezione Dettagli sullo stato del pannello dei dettagli. Per controllare la data a livello di codice, utilizza il [DescribeClassificationJob](#) funzionamento dell'API Amazon Macie.

Per mettere in pausa, riprendere o annullare un lavoro

Per mettere in pausa, riprendere o annullare un lavoro utilizzando la console Amazon Macie, segui questi passaggi. Per eseguire questa operazione a livello di codice, utilizza il [UpdateClassificationJob](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi). La pagina Lavori si apre e mostra il numero di lavori nel tuo inventario e una tabella di tali lavori.
3. Nella parte superiore della pagina, scegli refresh
()
per recuperare lo stato corrente di ogni lavoro.
4. Nella tabella Lavori, seleziona la casella di controllo relativa al lavoro che desideri sospendere, riprendere o annullare. Per trovare il lavoro più rapidamente, puoi filtrare la tabella utilizzando le opzioni di filtro sopra la tabella. È inoltre possibile ordinare la tabella in ordine crescente o decrescente in base a determinati campi.
5. Nel menu Azioni, effettuate una delle seguenti operazioni:
 - Per sospendere temporaneamente il lavoro, scegliete Pausa. Questa opzione è disponibile solo se lo stato corrente del lavoro è Attivo (inattivo), Attivo (In esecuzione) o In pausa (da Macie).

- Per riprendere il lavoro, scegli Riprendi. Questa opzione è disponibile solo se lo stato attuale del lavoro è In pausa (Per utente).
- Per annullare definitivamente il lavoro, scegli Annulla. Se scegli questa opzione, non puoi successivamente riprendere o riavviare il lavoro.

Copiare un processo di rilevamento di dati sensibili

Per creare rapidamente un processo di rilevamento di dati sensibili simile a un lavoro esistente, puoi creare una copia del lavoro esistente. È quindi possibile modificare le impostazioni della copia e salvare la copia come nuovo lavoro. Ciò può essere utile nei casi in cui si desidera analizzare diversi set di dati nello stesso modo o lo stesso set di dati in modi diversi. Può anche essere utile se si desidera modificare le impostazioni di configurazione per un lavoro esistente: annullare il lavoro esistente, copiarlo, quindi modificare e salvare la copia come nuovo lavoro.

Per copiare un lavoro

Segui questi passaggi per copiare un lavoro utilizzando la console Amazon Macie. Per copiare un lavoro a livello di codice, utilizza l'[DescribeClassificationJob](#) operazione dell'API Amazon Macie per recuperare le impostazioni di configurazione per il lavoro che desideri copiare. Quindi usa l'[CreateClassificationJob](#) operazione per creare una copia del lavoro.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione scegliere Jobs (Processi). La pagina Lavori si apre e mostra il numero di lavori nel tuo inventario e una tabella di tali lavori.
3. Nella tabella Lavori, seleziona la casella di controllo relativa al lavoro che desideri copiare. Per trovare il lavoro più rapidamente, puoi filtrare la tabella utilizzando le opzioni di filtro sopra la tabella. È inoltre possibile ordinare la tabella in ordine crescente o decrescente in base a determinati campi.
4. Nel menu Azioni, scegli Copia su nuovo.
5. Completa i passaggi sulla console per rivedere e modificare le impostazioni per la copia del lavoro. Per la fase Ridefinisci l'ambito, valuta la possibilità di scegliere opzioni che impediscano al job di analizzare nuovamente i dati esistenti nello stesso modo:
 - Per un lavoro occasionale, utilizzate [i criteri relativi agli oggetti](#) per includere solo gli oggetti che sono stati creati o modificati dopo un certo periodo di tempo. Ad esempio, se stai creando una copia di un lavoro che hai annullato, aggiungi una condizione Ultima modifica che specifica la data e l'ora in cui hai annullato il lavoro esistente.

- Per un lavoro periodico, deseleziona la casella di controllo **Includi oggetti esistenti**. In tal caso, la prima esecuzione del processo analizza solo gli oggetti che vengono creati o modificati dopo la creazione del lavoro e prima della prima esecuzione del lavoro. È inoltre possibile utilizzare [i criteri relativi agli oggetti](#) per escludere gli oggetti che sono stati modificati l'ultima volta prima di una determinata data e ora.

Per ulteriori dettagli su questo e altri passaggi, vedere [Creazione di un processo di rilevamento dei dati sensibili](#).

6. Al termine, scegli **Invia** per salvare la copia come nuovo lavoro.

Se hai configurato il lavoro in modo che venga eseguito una volta, su base giornaliera o nel giorno corrente della settimana o del mese, Macie inizia a eseguire il lavoro immediatamente dopo averlo salvato. Altrimenti, Macie si prepara a eseguire il lavoro nel giorno della settimana o del mese specificato. Per monitorare il lavoro, puoi [controllarne lo stato](#).

Monitoraggio dei processi di rilevamento di dati sensibili con CloudWatch Logs

Oltre a [monitorare lo stato generale](#) di un processo di rilevamento di dati sensibili, è possibile monitorare e analizzare eventi specifici che si verificano man mano che il lavoro procede. Puoi farlo utilizzando dati di registrazione quasi in tempo reale che Amazon Macie pubblica automaticamente su Amazon Logs. CloudWatch Logs I dati contenuti in questi log forniscono una registrazione delle modifiche all'avanzamento o allo stato di un lavoro. Ad esempio, è possibile utilizzare i dati per determinare la data e l'ora esatte in cui un processo è iniziato, è stato sospeso o ha terminato l'esecuzione.

I dati di registro forniscono inoltre dettagli su eventuali errori a livello di account o bucket che si verificano durante l'esecuzione di un processo. Ad esempio, Macie registra un evento se le impostazioni delle autorizzazioni per un bucket Amazon Simple Storage Service (Amazon S3) impediscono a un job di analizzare gli oggetti nel bucket. L'evento indica quando si è verificato l'errore e identifica il bucket interessato e il proprietario del bucket. Account AWS I dati per questi tipi di eventi possono aiutarti a identificare, analizzare e correggere gli errori che impediscono a Macie di analizzare i dati desiderati.

Con Amazon CloudWatch Logs, puoi monitorare, archiviare e accedere ai file di registro da più sistemi, applicazioni e Servizi AWS, incluso Macie. Puoi anche interrogare e analizzare i dati di registro e configurare CloudWatch Logs in modo che ti avvisino quando si verificano determinati

eventi o vengono raggiunte determinate soglie. CloudWatch Logs fornisce anche funzionalità per l'archiviazione dei dati di log e l'esportazione dei dati in Amazon S3. Per ulteriori informazioni sui CloudWatch log, consulta la [Amazon CloudWatch Logs User Guide](#).

Argomenti

- [Come funziona la registrazione per i lavori di rilevamento di dati sensibili](#)
- [Revisione dei log per i processi di rilevamento di dati sensibili](#)
- [Comprensione degli eventi di registro per i lavori di rilevamento di dati sensibili](#)

Come funziona la registrazione per i lavori di rilevamento di dati sensibili

Quando inizi a eseguire processi di rilevamento di dati sensibili, Amazon Macie crea e configura automaticamente le risorse appropriate in Amazon CloudWatch Logs per registrare gli eventi per tutti i tuoi lavori. Macie pubblica quindi automaticamente i dati degli eventi su tali risorse quando i lavori vengono eseguiti. La politica di autorizzazione per il [ruolo collegato al servizio](#) Macie per il tuo account consente a Macie di eseguire queste attività per tuo conto. Non è necessario adottare alcuna misura per creare o configurare risorse in CloudWatch Logs per registrare i dati degli eventi relativi ai lavori.

In CloudWatch Logs, i log sono organizzati in gruppi di log. Ogni gruppo di log contiene flussi di log. Ogni flusso di registro contiene eventi di registro. Lo scopo generale di ciascuna di queste risorse è il seguente:

- Un gruppo di log è una raccolta di flussi di log che condividono le stesse impostazioni di conservazione, monitoraggio e controllo degli accessi, ad esempio la raccolta di log per tutti i processi di rilevamento di dati sensibili.
- Un flusso di log è una sequenza di eventi di registro che condividono la stessa origine, ad esempio un singolo processo di rilevamento di dati sensibili.
- Un evento di registro è un record di un'attività registrata da un'applicazione o da una risorsa, ad esempio un singolo evento che Macie ha registrato e pubblicato per un particolare processo di rilevamento di dati sensibili.

Macie pubblica gli eventi per tutti i processi di rilevamento dei dati sensibili in un unico gruppo di log. Ogni processo ha un flusso di log unico in quel gruppo di log. Il gruppo di log ha il prefisso e il nome seguenti:

```
/aws/macie/classificationjobs
```

Se questo gruppo di log esiste già, Macie lo usa per memorizzare gli eventi di registro relativi ai tuoi lavori. Questo può essere utile se l'organizzazione utilizza la configurazione automatizzata [AWS CloudFormation](#), ad esempio per creare gruppi di log con periodi di conservazione predefiniti, impostazioni di crittografia, tag, filtri metrici e così via, per gli eventi di lavoro.

Se questo gruppo di log non esiste, Macie lo crea con le impostazioni predefinite utilizzate da CloudWatch Logs per i nuovi gruppi di log. Le impostazioni includono un periodo di conservazione dei log di Never Expire, il che significa che CloudWatch Logs archivia i log a tempo indeterminato. È possibile modificare il periodo di conservazione per il gruppo di log. Per sapere come, consulta [Lavorare con gruppi di log e flussi di log](#) nella Amazon CloudWatch Logs User Guide.

All'interno di questo gruppo di log, Macie crea un flusso di log unico per ogni job che esegui, la prima volta che il job viene eseguito. Il nome del flusso di log è l'identificatore univoco del processo, ad esempio nel seguente formato: 85a55dc0fa6ed0be5939d0408example

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

Ogni flusso di log contiene tutti gli eventi di registro che Macie ha registrato e pubblicato per il job corrispondente. Per i lavori periodici, questo include gli eventi per tutte le esecuzioni del lavoro. Se elimini il flusso di log per un job periodico, Macie crea nuovamente lo stream alla successiva esecuzione del job. Se elimini il flusso di log per un lavoro singolo, non puoi ripristinarlo.

Tieni presente che la registrazione è abilitata per impostazione predefinita per tutti i tuoi lavori. Non puoi disabilitarlo o impedire in altro modo a Macie di pubblicare eventi di lavoro su CloudWatch Logs. Se non desideri archiviare i log, puoi ridurre il periodo di conservazione per il gruppo di log a un minimo di un giorno. Al termine del periodo di conservazione, CloudWatch Logs elimina automaticamente i dati degli eventi scaduti dal gruppo di log.

Revisione dei log per i processi di rilevamento di dati sensibili

Dopo aver iniziato a eseguire processi di rilevamento di dati sensibili in Amazon Macie, puoi rivedere i log dei tuoi lavori utilizzando Amazon Logs. CloudWatch CloudWatch Logs offre funzionalità progettate per aiutarti a rivedere, analizzare e monitorare i dati dei log. È possibile utilizzare queste funzionalità per utilizzare i flussi di log e gli eventi relativi ai job come si farebbe con qualsiasi altro tipo di dati di registro in CloudWatch Logs.

Ad esempio, puoi cercare e filtrare dati aggregati per identificare tipi specifici di eventi che si sono verificati per tutti i tuoi lavori in un intervallo di tempo specifico. Oppure puoi eseguire una revisione mirata di tutti gli eventi che si sono verificati per un determinato lavoro. CloudWatch Logs offre anche

opzioni per il monitoraggio dei dati di registro, la definizione di filtri metrici e la creazione di allarmi personalizzati.

Tip

Per accedere rapidamente ai dati di registro per un determinato lavoro, puoi utilizzare la console Amazon Macie. A tale scopo, scegli il nome del lavoro nella pagina Lavori. Nella parte superiore del pannello dei dettagli, scegli Mostra risultati, quindi scegli Mostra CloudWatch registri. Macie apre la CloudWatch console Amazon e visualizza una tabella di eventi di registro per il lavoro.

Per esaminare i log relativi ai lavori di rilevamento di dati sensibili

Segui questi passaggi per accedere e rivedere i dati di registro utilizzando la CloudWatch console Amazon. Per esaminare i dati a livello di codice, utilizza l'API [Amazon CloudWatch Logs](#).

1. Apri la console all' CloudWatch indirizzo. <https://console.aws.amazon.com/cloudwatch/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui hai eseguito i lavori di cui desideri esaminare i registri.
3. Nel pannello di navigazione scegli Log, quindi Gruppi di log.
4. Nella pagina Log groups, scegli il gruppo/log. `aws/macie/classificationjobs` CloudWatch visualizza una tabella di flussi di log per i lavori che hai eseguito. Esiste uno stream unico per ogni job. Il nome di ogni stream è correlato all'identificatore univoco di un lavoro.
5. Nella scheda Registra flussi, esegui una delle seguenti operazioni:
 - Per esaminare gli eventi di registro per un particolare lavoro, scegliete il flusso di log per il lavoro. Per trovare lo stream più facilmente, inserisci l'identificatore univoco del lavoro nella casella del filtro sopra la tabella. Dopo aver scelto il flusso di log, CloudWatch visualizza una tabella di eventi di registro per il lavoro.
 - Per esaminare gli eventi di registro per tutti i tuoi lavori, scegli Cerca in tutti i flussi di registro. CloudWatch visualizza una tabella di eventi di registro per tutti i tuoi lavori.
6. (Facoltativo) Nella casella del filtro sopra la tabella, inserisci termini, frasi o valori che specificano le caratteristiche degli eventi specifici da esaminare. Per ulteriori informazioni, consulta [Ricerca nei dati di log utilizzando modelli di filtro](#) nella Amazon CloudWatch Logs User Guide.
7. Per esaminare i dettagli di uno specifico evento di registro, scegli expand



nella riga relativa all'evento. CloudWatch visualizza i dettagli dell'evento in formato JSON. Per ulteriori informazioni su questi dettagli, consulta [Comprensione degli eventi di registro per i lavori](#).

Man mano che acquisisci familiarità con i dati contenuti nel registro degli eventi, puoi eseguire attività aggiuntive per semplificare l'analisi e il monitoraggio dei dati. Ad esempio, puoi [creare filtri di metriche](#) che trasformano i dati di registro in metriche numeriche. CloudWatch Puoi anche [creare allarmi personalizzati](#) che semplificano l'identificazione e la risposta a eventi di registro specifici. Per ulteriori informazioni, consulta la [Amazon CloudWatch Logs User Guide](#).

Comprensione degli eventi di registro per i lavori di rilevamento di dati sensibili

Per aiutarti a monitorare i processi di rilevamento di dati sensibili, Amazon Macie pubblica automaticamente i dati di registrazione dei lavori su Amazon Logs. CloudWatch I dati contenuti in questi registri forniscono una registrazione delle modifiche all'avanzamento o allo stato di un lavoro. Ad esempio, è possibile utilizzare i dati per determinare la data e l'ora esatte in cui l'esecuzione di un processo è iniziata o è terminata. I dati forniscono inoltre dettagli su alcuni tipi di errori che possono verificarsi durante l'esecuzione di un processo. Questi dati possono aiutarti a identificare, analizzare e correggere gli errori che impediscono a Macie di analizzare i dati che desideri.

Quando inizi a eseguire lavori, Macie crea e configura automaticamente le risorse appropriate in CloudWatch Logs per registrare gli eventi per tutti i tuoi lavori. Macie pubblica quindi automaticamente i dati degli eventi su tali risorse quando i lavori vengono eseguiti. Per ulteriori informazioni, consulta [Come funziona la registrazione per i lavori](#).

Utilizzando CloudWatch Logs, è quindi possibile interrogare e analizzare i dati di registro relativi ai lavori. Ad esempio, puoi cercare e filtrare dati aggregati per identificare tipi specifici di eventi che si sono verificati per tutti i tuoi lavori in un intervallo di tempo specifico. Oppure puoi eseguire una revisione mirata di tutti gli eventi che si sono verificati per un determinato lavoro. CloudWatch Logs offre anche opzioni per il monitoraggio dei dati di registro, la definizione di filtri metrici e la creazione di allarmi personalizzati. Ad esempio, è possibile configurare CloudWatch Logs per avvisare l'utente se si verifica un determinato tipo di evento durante l'esecuzione dei job. Per ulteriori informazioni, consulta la [Amazon CloudWatch Logs User Guide](#).

Argomenti

- [Registra lo schema degli eventi per i lavori di rilevamento di dati sensibili](#)
- [Tipi di eventi di registro per i lavori di rilevamento di dati sensibili](#)
 - [Eventi Job status](#)

- [Eventi di errore a livello di account](#)
- [Eventi di errore a livello di bucket](#)

Registra lo schema degli eventi per i lavori di rilevamento di dati sensibili

Ogni evento di registro per un processo di rilevamento di dati sensibili è un oggetto JSON che contiene un set standard di campi ed è conforme allo schema degli eventi di Amazon CloudWatch Logs. Alcuni tipi di eventi dispongono di campi aggiuntivi che forniscono informazioni particolarmente utili per quel tipo di evento. Ad esempio, gli eventi relativi agli errori a livello di account includono l'ID dell'account dell'utente interessato. Account AWS Gli eventi relativi agli errori a livello di bucket includono il nome del bucket Amazon Simple Storage Service (Amazon S3) interessato.

L'esempio seguente mostra lo schema degli eventi di registro per i processi di rilevamento di dati sensibili. In questo esempio, l'evento riporta che Amazon Macie non è stato in grado di analizzare alcun oggetto in un bucket S3 perché Amazon S3 ha negato l'accesso al bucket.

```
{
  "adminAccountId": "123456789012",
  "jobId": "85a55dc0fa6ed0be5939d0408example",
  "eventType": "BUCKET_ACCESS_DENIED",
  "occurredAt": "2024-04-14T17:11:30.574809Z",
  "description": "Macie doesn't have permission to access the affected S3 bucket.",
  "jobName": "My_Macie_Job",
  "operation": "ListObjectsV2",
  "runDate": "2024-04-14T17:08:30.345809Z",
  "affectedAccount": "111122223333",
  "affectedResource": {
    "type": "S3_BUCKET_NAME",
    "value": "amzn-s3-demo-bucket"
  }
}
```

Nell'esempio precedente, Macie ha tentato di elencare gli oggetti del bucket utilizzando l'operazione [ListObjectsV2 dell'API](#) Amazon S3. Quando Macie ha inviato la richiesta ad Amazon S3, Amazon S3 ha negato l'accesso al bucket.

I seguenti campi sono comuni a tutti gli eventi di registro per i lavori di rilevamento di dati sensibili:

- `adminAccountId`— L'identificatore univoco di chi Account AWS ha creato il lavoro.
- `jobId`— L'identificatore univoco del lavoro.

- `eventType`— Il tipo di evento che si è verificato.
- `occurredAt`— La data e l'ora, in formato UTC (Coordinated Universal Time) e ISO 8601 esteso, in cui si è verificato l'evento.
- `description`— Una breve descrizione dell'evento.
- `jobName`— Il nome del lavoro.

A seconda del tipo e della natura di un evento, un evento di registro può contenere anche i seguenti campi:

- `affectedAccount`— L'identificatore univoco del Account AWS proprietario della risorsa interessata.
- `affectedResource`— Un oggetto JSON che fornisce dettagli sulla risorsa interessata. Nell'oggetto, il `type` campo specifica un campo che memorizza i metadati relativi a una risorsa. Il `value` campo specifica il valore del campo (`.`). `type`
- `operation`— L'operazione che Macie ha tentato di eseguire e che ha causato l'errore.
- `runDate`— La data e l'ora, in formato UTC (Coordinated Universal Time) e ISO 8601 esteso, in cui è stato avviato il processo o l'esecuzione del processo applicabile.

Tipi di eventi di registro per i lavori di rilevamento di dati sensibili

Amazon Macie pubblica eventi di registro per tre categorie di eventi che possono verificarsi per un processo di rilevamento di dati sensibili:

- Eventi di stato del lavoro, che registrano le modifiche allo stato o all'avanzamento di un processo o di un'esecuzione di un lavoro.
- Eventi di errore a livello di account, che registrano gli errori che hanno impedito a Macie di analizzare i dati di Amazon S3 per uno specifico caso. Account AWS
- Eventi di errore a livello di bucket, che registrano gli errori che hanno impedito a Macie di analizzare i dati in un bucket S3 specifico.

Gli argomenti di questa sezione elencano e descrivono i tipi di eventi pubblicati da Macie per ogni categoria.

Eventi Job status

Un evento relativo allo stato di un processo registra una modifica allo stato o all'avanzamento di un processo o dell'esecuzione di un processo. Per i lavori periodici, Macie registra e pubblica questi eventi sia per l'intero processo che per le singole esecuzioni di lavoro.

L'esempio seguente utilizza dati di esempio per mostrare la struttura e la natura dei campi in un evento di stato del lavoro. In questo esempio, un SCHEDULED_RUN_COMPLETED evento indica che l'esecuzione pianificata di un processo periodico è terminata. L'esecuzione è iniziata il 14 aprile 2024 alle 17:09:30 UTC, come indicato dal campo. runDate La corsa è terminata il 14 aprile 2024 alle 17:16:30 UTC, come indicato dal campo. occurredAt

```
{
  "adminAccountId": "123456789012",
  "jobId": "ffad0e71455f38a4c7c220f3cexample",
  "eventType": "SCHEDULED_RUN_COMPLETED",
  "occurredAt": "2024-04-14T17:16:30.574809Z",
  "description": "The scheduled job run finished running.",
  "jobName": "My_Daily_Macie_Job",
  "runDate": "2024-04-14T17:09:30.574809Z"
}
```

La tabella seguente elenca e descrive i tipi di eventi sullo stato del lavoro che Macie registra e pubblica su Logs. CloudWatch La colonna Tipo di evento indica il nome di ogni evento così come appare nel eventType campo di un evento. La colonna Descrizione fornisce una breve descrizione dell'evento così come appare nel description campo di un evento. Le informazioni aggiuntive forniscono informazioni sul tipo di lavoro a cui si applica l'evento. La tabella viene ordinata prima in base all'ordine cronologico generale in cui potrebbero verificarsi gli eventi e quindi in ordine alfabetico crescente per tipo di evento.

Tipo di evento	Descrizione	Informazioni aggiuntive
POSTO DI LAVORO CREATO	Il lavoro è stato creato.	Si applica ai lavori occasionali e periodici.
ONE_JOB_STARTED	Il processo è iniziato a funzionare.	Si applica solo ai lavori occasionali.

Tipo di evento	Descrizione	Informazioni aggiuntive
SCHEDULED_RUN_STARTED	L'esecuzione del processo pianificato è iniziata.	Si applica solo ai lavori periodici. Per registrare l'inizio di un lavoro singolo, Macie pubblica un evento ONE_TIME_JOB_STARTED, non questo tipo di evento.
BUCKET_MATCHED_THE_CRITERIA	Il bucket interessato corrisponde ai criteri del bucket specificati per il job.	Si applica ai job occasionali e periodici che utilizzano i criteri dei bucket di runtime per determinare quali bucket S3 analizzare. L'affectedResource oggetto specifica il nome del bucket che corrisponde ai criteri ed è stato incluso nell'analisi del job.
NO_BUCKETS_MATCHED_THE_CRITERIA	Il processo è iniziato a funzionare ma attualmente nessun bucket corrisponde ai criteri del bucket specificati per il lavoro. Il processo non ha analizzato alcun dato.	Si applica ai job occasionali e periodici che utilizzano i criteri dei bucket di runtime per determinare quali bucket S3 analizzare.
SCHEDULED_RUN_COMPLETED	L'esecuzione del processo pianificato è terminata.	Si applica solo ai lavori periodici. Per registrare il completamento di un lavoro singolo, Macie pubblica un evento JOB_COMPLETED, non questo tipo di evento.

Tipo di evento	Descrizione	Informazioni aggiuntive
JOB_PAUSED_BY_USER	Il processo è stato messo in pausa da un utente.	Si applica ai lavori occasionali e periodici interrotti temporaneamente (in pausa).
JOB_RESUMED_BY_USER	Il lavoro è stato ripreso da un utente.	Si applica ai lavori occasionali e periodici interrotti temporaneamente (in pausa) e successivamente ripresi.
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	Il lavoro è stato sospeso da Macie. Il completamento del lavoro supererebbe la quota mensile per l'account interessato.	Si applica ai lavori occasionali e periodici che Macie ha interrotto temporaneamente (in pausa). Macie sospende automaticamente un processo quando un'ulteriore elaborazione da parte del lavoro o dell'esecuzione di un lavoro supera la quota mensile di rilevamento di dati sensibili per uno o più account per i quali il lavoro analizza i dati. Per evitare questo problema, valuta la possibilità di aumentare la quota per gli account interessati.

Tipo di evento	Descrizione	Informazioni aggiuntive
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	Il lavoro è stato ripreso da Macie. La quota di servizio mensile è stata revocata per l'account interessato.	Si applica ai lavori occasionali e periodici che Macie ha interrotto temporaneamente (in pausa) e successivamente ripresi. Se Macie ha messo automaticamente in pausa un lavoro occasionale, Macie riprende automaticamente il lavoro all'inizio del mese successivo o oppure la quota mensile di rilevamento dei dati sensibili viene aumentata per tutti gli account interessati, a seconda dell'evento che si verifica per primo. Se Macie ha messo automaticamente in pausa un lavoro periodico, Macie riprende automaticamente il lavoro quando è programmato l'inizio dell'esecuzione successiva o inizia il mese successivo, a seconda di quale evento si verifica per primo.

Tipo di evento	Descrizione	Informazioni aggiuntive
JOB_ANNULLATO	Il lavoro è stato annullato.	Si applica ai lavori occasionali e periodici che hai interrotto definitivamente (annullati) o, per i lavori occasionali, messi in pausa e non ripresi entro 30 giorni. Se sospendi o disabiliti Macie, questo tipo di evento si applica anche ai lavori che erano attivi o in pausa quando hai sospeso o disabilitato Macie. Macie annulla automaticamente i tuoi lavori in un Regione AWS se sospendi o disabiliti Macie nella regione.
LAVORO_COMPLETATO	L'esecuzione del processo è terminata.	Si applica solo ai lavori occasionali. Per registrare il completamento di un job eseguito per un job periodico, Macie pubblica un evento SCHEDULED_RUN_COMPLETED, non questo tipo di evento.

Eventi di errore a livello di account

Un evento di errore a livello di account registra un errore che ha impedito a Macie di analizzare gli oggetti nei bucket S3 di proprietà di uno specifico. Account AWS Il `affectedAccount` campo di ogni evento specifica l'ID dell'account.

L'esempio seguente utilizza dati di esempio per mostrare la struttura e la natura dei campi in un evento di errore a livello di account. In questo esempio, un `ACCOUNT_ACCESS_DENIED` evento

indica che Macie non è stata in grado di analizzare gli oggetti in nessun bucket S3 di proprietà di un account. 444455556666

```
{
  "adminAccountId": "123456789012",
  "jobId": "85a55dc0fa6ed0be5939d0408example",
  "eventType": "ACCOUNT_ACCESS_DENIED",
  "occurredAt": "2024-04-14T17:08:30.585709Z",
  "description": "Macie doesn't have permission to access S3 bucket data for the affected account.",
  "jobName": "My_Macie_Job",
  "operation": "ListBuckets",
  "runDate": "2024-04-14T17:05:27.574809Z",
  "affectedAccount": "444455556666"
}
```

La tabella seguente elenca e descrive i tipi di eventi di errore a livello di account che Macie registra e pubblica su Logs. CloudWatch La colonna Tipo di evento indica il nome di ogni evento così come appare nel campo di un evento. eventType La colonna Descrizione fornisce una breve descrizione dell'evento così come appare nel description campo di un evento. La colonna Informazioni aggiuntive fornisce tutti i suggerimenti applicabili per analizzare o risolvere l'errore che si è verificato. La tabella è ordinata in ordine alfabetico crescente per tipo di evento.

Tipo di evento	Descrizione	Informazioni aggiuntive
ACCOUNT_ACCESS_DENIED	Macie non è autorizzata ad accedere ai dati del bucket S3 per l'account interessato.	Ciò si verifica in genere perché i bucket di proprietà dell'account hanno politiche restrittive. Per informazioni su come risolvere questo problema, consulta. Consentire a Macie di accedere a bucket e oggetti S3 Il valore del operation campo nell'evento può aiutarti a determinare quali impostazioni delle autorizzazioni hanno

Tipo di evento	Descrizione	Informazioni aggiuntive
		impedito a Macie di accedere ai dati S3 per l'account. Questo campo indica l'operazione Amazon S3 che Macie ha tentato di eseguire quando si è verificato l'errore.
ACCOUNT_DISABLED	Il lavoro ha ignorato le risorse di proprietà dell'account interessato. Macie è stata disattivata per l'account.	Per risolvere questo problema, riattiva Macie per l'account nello stesso. Regione AWS
ACCOUNT_DISASSOCIATED	Il job ha ignorato le risorse di proprietà dell'account interessato. L'account non è più associato al tuo account amministratore Macie come account membro.	Ciò si verifica se, in qualità di amministratore Macie di un'organizzazione, configuri un processo per analizzare i dati per un account membro e l'account viene successivamente rimosso dall'organizzazione. Per risolvere questo problema, associa nuovamente l'account interessato al tuo account amministratore Macie come account membro. Per ulteriori informazioni, consulta Gestione di più account.
ACCOUNT_ISOLATED	Il job ha ignorato le risorse di proprietà dell'account interessato. Account AWS Era isolato.	–

Tipo di evento	Descrizione	Informazioni aggiuntive
ACCOUNT_REGION_DISABLED	Il lavoro ha ignorato le risorse di proprietà dell'account interessato. Account AWS Non è attivo nella versione corrente Regione AWS.	–
ACCOUNT_SUSPENDED	Il lavoro è stato annullato o le risorse di proprietà dell'account interessato sono state ignorate. Macie è stata sospesa per l'account.	Se l'account specificato è il tuo account, Macie ha annullato automaticamente il lavoro quando hai sospeso Macie nella stessa regione. Per risolvere il problema, riattiva Macie nella regione. Se l'account specificato è un account membro, riattiva Macie per quell'account nella stessa regione.
ACCOUNT_TERMINATO	Il job ha ignorato le risorse di proprietà dell'account interessato. Il Account AWS è stato terminato.	–

Eventi di errore a livello di bucket

Un evento di errore a livello di bucket registra un errore che ha impedito a Macie di analizzare gli oggetti in uno specifico bucket S3. Il `affectedAccount` campo di ogni evento specifica l'ID dell'account del proprietario del bucket. Account AWS L'`affectedResource` oggetto in ogni evento specifica il nome del bucket.

L'esempio seguente utilizza dati di esempio per mostrare la struttura e la natura dei campi in un evento di errore a livello di bucket. In questo esempio, un `BUCKET_ACCESS_DENIED` evento indica che Macie non è stata in grado di analizzare alcun oggetto nel bucket S3 denominato. `amzn-s3-`

demo-bucket Quando Macie ha tentato di elencare gli oggetti del bucket utilizzando l'operazione [ListObjectsV2](#) dell'API Amazon S3, Amazon S3 ha negato l'accesso al bucket.

```
{
  "adminAccountId": "123456789012",
  "jobId": "85a55dc0fa6ed0be5939d0408example",
  "eventType": "BUCKET_ACCESS_DENIED",
  "occurredAt": "2024-04-14T17:11:30.574809Z",
  "description": "Macie doesn't have permission to access the affected S3 bucket.",
  "jobName": "My_Macie_Job",
  "operation": "ListObjectsV2",
  "runDate": "2024-04-14T17:09:30.685209Z",
  "affectedAccount": "111122223333",
  "affectedResource": {
    "type": "S3_BUCKET_NAME",
    "value": "amzn-s3-demo-bucket"
  }
}
```

La tabella seguente elenca e descrive i tipi di eventi di errore a livello di bucket che Macie registra e pubblica su Logs. CloudWatch La colonna Tipo di evento indica il nome di ogni evento così come appare nel campo di un evento. eventType La colonna Descrizione fornisce una breve descrizione dell'evento così come appare nel description campo di un evento. La colonna Informazioni aggiuntive fornisce tutti i suggerimenti applicabili per analizzare o risolvere l'errore che si è verificato. La tabella è ordinata in ordine alfabetico crescente per tipo di evento.

Tipo di evento	Descrizione	Informazioni aggiuntive
BUCKET_ACCESS_DENIED	Macie non è autorizzata ad accedere al bucket S3 interessato.	Ciò si verifica in genere perché un bucket ha una politica restrittiva. Per informazioni su come risolvere questo problema, consulta. Consentire a Macie di accedere a bucket e oggetti S3 Il valore del operation campo nell'evento può aiutarti

Tipo di evento	Descrizione	Informazioni aggiuntive
		a determinare quali impostazioni delle autorizzazioni hanno impedito a Macie di accedere al bucket. Questo campo indica l'operazione Amazon S3 che Macie ha tentato di eseguire quando si è verificato l'errore.
BUCKET_DETAILS_AVAILABLE	Un problema temporaneo impediva a Macie di recuperare i dettagli sul bucket e sugli oggetti del bucket.	Questo si verifica se un problema temporaneo ha impedito a Macie di recuperare i metadati del bucket e dell'oggetto necessari per analizzare gli oggetti del bucket. Ad esempio, si è verificata un'eccezione di Amazon S3 quando Macie ha cercato di verificare che fosse autorizzato ad accedere al bucket. Per risolvere il problema relativo a un lavoro occasionale, prendi in considerazione la possibilità di creare ed eseguire un nuovo lavoro monouso per analizzare e gli oggetti nel bucket. Per un lavoro pianificato, Macie proverà a recuperare e nuovamente i metadati durante la prossima esecuzione del lavoro.

Tipo di evento	Descrizione	Informazioni aggiuntive
BUCKET_DOES_NON_EXIST	Il bucket S3 interessato non esiste più.	Ciò si verifica in genere perché un bucket è stato eliminato.
BUCKET_IN_DIFFERENT_REGION	Il bucket S3 interessato è stato spostato in un altro. Regione AWS	–
BUCKET_OWNER_CHANGED	Il proprietario del bucket S3 interessato è cambiato. Macie non ha più il permesso di accedere al bucket.	Ciò si verifica in genere se la proprietà di un bucket è stata trasferita a un utente Account AWS che non fa parte dell'organizzazione. Il affectedAccount campo nell'evento indica l'ID dell'account che in precedenza possedeva il bucket.

Previsione e monitoraggio dei costi per i lavori di scoperta di dati sensibili

I prezzi di Amazon Macie si basano in parte sulla quantità di dati che analizzi eseguendo processi di rilevamento di dati sensibili. Per prevedere e monitorare i costi stimati per l'esecuzione di lavori di rilevamento di dati sensibili, puoi rivedere le stime dei costi fornite da Macie quando crei un lavoro e dopo aver iniziato a eseguirlo.

Per rivedere e monitorare i costi effettivi, puoi utilizzare AWS Billing and Cost Management. AWS Billing and Cost Management offre funzionalità progettate per aiutarti a tenere traccia e analizzare i costi e gestire Servizi AWS i budget per il tuo account o la tua organizzazione. Fornisce inoltre funzionalità che possono aiutarti a prevedere i costi di utilizzo sulla base di dati storici. Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Billing](#).

Per informazioni sui prezzi di Macie, consulta i prezzi di [Amazon Macie](#).

Argomenti

- [Previsione del costo di un lavoro di scoperta di dati sensibili](#)
- [Monitoraggio dei costi stimati per i lavori di rilevamento di dati sensibili](#)

Previsione del costo di un lavoro di scoperta di dati sensibili

Quando crei un processo di rilevamento di dati sensibili, Amazon Macie può calcolare e visualizzare i costi stimati durante due fasi chiave del processo di creazione del lavoro: quando esamini la tabella dei bucket S3 che hai selezionato per il lavoro (fase 2) e quando rivedi tutte le impostazioni per il processo (passaggio 8). Queste stime possono aiutarti a determinare se modificare le impostazioni del lavoro prima di salvarlo. La disponibilità e la natura delle stime dipendono dalle impostazioni scelte per il lavoro.

Revisione dei costi stimati per i singoli bucket (fase 2)

Se selezioni esplicitamente singoli bucket per un lavoro da analizzare, puoi rivedere il costo stimato dell'analisi degli oggetti in ciascuno di quei bucket. Macie visualizza queste stime durante la fase 2 del processo di creazione del lavoro, quando rivedi le selezioni dei bucket. Nella tabella relativa a questo passaggio, il campo Costo stimato indica il costo totale stimato (in dollari USA) dell'esecuzione del lavoro una volta per analizzare gli oggetti in un bucket.

Ogni stima riflette la quantità prevista di dati non compressi che il job analizzerà in un bucket, in base alle dimensioni e ai tipi di oggetti attualmente archiviati nel bucket. La stima riflette anche i prezzi attuali di Macie. Regione AWS

Nella stima dei costi di un bucket sono inclusi solo gli oggetti classificabili. Un oggetto classificabile è un oggetto S3 che utilizza una [classe di storage Amazon S3](#) supportata e ha un'estensione del nome di file per un formato di file o di storage [supportato](#). Se alcuni oggetti classificabili sono file compressi o di archivio, la stima presuppone che i file utilizzino un rapporto di compressione 3:1 e che il job possa analizzare tutti i file estratti.

Revisione del costo totale stimato di un lavoro (fase 8)

Se crei un lavoro singolo o crei e configuri un lavoro periodico per includere oggetti S3 esistenti, Macie calcola e visualizza il costo totale stimato del lavoro durante la fase finale del processo di creazione del lavoro. Puoi rivedere questa stima mentre esamini e verifichi tutte le impostazioni selezionate per il lavoro.

Questa stima indica il costo totale previsto (in dollari USA) dell'esecuzione del processo una volta nella regione corrente. La stima riflette la quantità prevista di dati non compressi che il job

analizzerà. Si basa sulle dimensioni e sui tipi di oggetti attualmente archiviati nei bucket che hai selezionato in modo esplicito per il lavoro o fino a 500 bucket che attualmente soddisfano i criteri del bucket specificati per il lavoro, a seconda delle impostazioni del lavoro.

Tieni presente che questa stima non riflette alcuna opzione che hai selezionato per rifinire e ridurre l'ambito del lavoro, ad esempio una profondità di campionamento inferiore o criteri che escludono determinati oggetti S3 dal lavoro. Inoltre, non riflette la tua [quota mensile di ricerca di dati sensibili](#), che potrebbe limitare l'ambito e il costo dell'analisi del lavoro, né gli sconti che potrebbero essere applicati al tuo account.

Oltre al costo totale stimato del lavoro, la stima fornisce dati aggregati che offrono informazioni sull'ambito e sul costo previsti del lavoro:

- I valori delle dimensioni indicano la dimensione totale di archiviazione degli oggetti che il job può e non può analizzare.
- I valori di conteggio degli oggetti indicano il numero totale di oggetti che il job può e non può analizzare.

In questi valori, un oggetto Classificabile è un oggetto S3 che utilizza una [classe di storage Amazon S3](#) supportata e ha un'estensione del nome di file per un formato di file o di storage [supportato](#). Solo gli oggetti classificabili sono inclusi nella stima dei costi. Un oggetto non classificabile è un oggetto che non utilizza una classe di archiviazione supportata o non ha un'estensione del nome di file per un file o un formato di archiviazione supportato. Questi oggetti non sono inclusi nella stima dei costi.

La stima fornisce dati aggregati aggiuntivi per oggetti S3 che sono file compressi o di archivio. Il valore Compressed indica la dimensione totale di storage degli oggetti che utilizzano una classe di storage Amazon S3 supportata e hanno un'estensione per un tipo di file compresso o di archivio supportato. Il valore Uncompressed indica la dimensione approssimativa di questi oggetti se sono decompressi, in base a un rapporto di compressione specificato. Questi dati sono importanti per il modo in cui Macie analizza i file compressi e i file di archivio.

Quando Macie analizza un file compresso o di archivio, ispeziona sia il file completo che il contenuto del file. Per controllare il contenuto del file, Macie decomprime il file, quindi ispeziona ogni file estratto che utilizza un formato supportato. La quantità effettiva di dati analizzata da un job dipende quindi da:

- Se un file utilizza la compressione e, in tal caso, il rapporto di compressione utilizzato.
- Il numero, la dimensione e il formato dei file estratti.

Per impostazione predefinita, Macie presuppone quanto segue quando calcola le stime dei costi per un lavoro:

- Tutti i file compressi e di archivio utilizzano un rapporto di compressione 3:1.
- Tutti i file estratti utilizzano un formato di file o di archiviazione supportato.

Queste ipotesi possono portare a una stima delle dimensioni più ampia dell'ambito dei dati che il lavoro analizzerà e, di conseguenza, a una stima dei costi più elevata per il lavoro.

È possibile ricalcolare il costo totale stimato del lavoro in base a un rapporto di compressione diverso. A tale scopo, scegliete il rapporto dall'elenco Scegli un rapporto di compressione stimato nella sezione Costo stimato. Macie aggiorna quindi la stima in base alla selezione effettuata.

Per ulteriori informazioni su come Macie calcola i costi stimati, consulta. [Comprendere i costi di utilizzo stimati](#)

Monitoraggio dei costi stimati per i lavori di rilevamento di dati sensibili

Se stai già eseguendo processi di rilevamento di dati sensibili, la pagina Utilizzo sulla console Amazon Macie può aiutarti a monitorare il costo stimato di tali lavori. La pagina mostra i costi stimati (in dollari USA) per l'utilizzo di Macie nella versione corrente Regione AWS durante il mese solare corrente. Per informazioni su come Macie calcola queste stime, vedi. [Comprendere i costi di utilizzo stimati](#)

Per rivedere i costi stimati per l'esecuzione dei lavori

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri rivedere i costi stimati.
3. Nel riquadro di navigazione, scegli Utilizzo.
4. Nella pagina Utilizzo, consulta la ripartizione dei costi stimati per il tuo account. La voce Sensitive Data Discovery Job riporta il costo totale stimato dei lavori eseguiti finora durante il mese corrente nella regione corrente.

Se sei l'amministratore Macie di un'organizzazione, la sezione Costi stimati mostra i costi stimati complessivi dell'organizzazione per il mese corrente nella regione corrente. Per mostrare il costo totale stimato dei lavori eseguiti per un account specifico, scegli l'account nella tabella. La sezione Costi stimati mostra quindi una ripartizione dei costi stimati per l'account, incluso il costo

stimato dei lavori eseguiti. Per mostrare questi dati per un account diverso, scegli l'account nella tabella. Per cancellare la selezione dell'account, scegli X accanto all'ID dell'account.

Per rivedere e monitorare i costi effettivi, usa [AWS Billing and Cost Management](#).

Identificatori di dati gestiti consigliati per i lavori di rilevamento di dati sensibili

Per ottimizzare i risultati dei processi di rilevamento di dati sensibili, è possibile configurare singoli processi in modo che utilizzino automaticamente il set di identificatori di dati gestiti consigliato per i lavori. Un identificatore di dati gestiti è un insieme di criteri e tecniche integrati progettati per rilevare un tipo specifico di dati sensibili, ad esempio chiavi di accesso AWS segrete, numeri di carte di credito o numeri di passaporto per un particolare paese o area geografica.

Il set consigliato di identificatori di dati gestiti è progettato per rilevare categorie e tipi comuni di dati sensibili. Sulla base della nostra ricerca, è in grado di rilevare categorie e tipi generali di dati sensibili, ottimizzando al contempo i risultati lavorativi riducendo il rumore. Man mano che rilasciamo nuovi identificatori di dati gestiti, li aggiungiamo a questo set se è probabile che ottimizzino ulteriormente i risultati del tuo lavoro. Nel tempo, potremmo anche aggiungere o rimuovere gli identificatori di dati gestiti esistenti dal set. Se aggiungiamo o rimuoviamo un identificatore di dati gestiti dal set consigliato, aggiorniamo questa pagina per indicare la natura e la tempistica della modifica. Per ricevere avvisi automatici su queste modifiche, puoi iscriverti al feed RSS nella pagina della cronologia dei documenti di [Macie](#).

Quando crei un processo di rilevamento di dati sensibili, specifichi quali identificatori di dati gestiti desideri che il processo utilizzi per analizzare gli oggetti nei bucket Amazon Simple Storage Service (Amazon S3). Per configurare un processo in modo che utilizzi il set consigliato di identificatori di dati gestiti, scegli l'opzione Consigliato al momento della creazione del lavoro. Il processo utilizzerà quindi automaticamente tutti gli identificatori di dati gestiti presenti nel set consigliato all'inizio dell'esecuzione del lavoro. Se si configura un processo per l'esecuzione più di una volta, ogni esecuzione utilizzerà automaticamente tutti gli identificatori di dati gestiti presenti nel set consigliato all'avvio dell'esecuzione.

Negli argomenti seguenti sono elencati gli identificatori di dati gestiti attualmente inclusi nel set consigliato, organizzati per categoria e tipo di dati sensibili. Specificano l'identificatore univoco (ID) per ogni identificatore di dati gestiti del set. Questo ID descrive il tipo di dati sensibili che un identificatore di dati gestiti è progettato per rilevare, ad esempio: per le chiavi private PGP e PGP_PRIVATE_KEY USA_PASSPORT_NUMBER per i numeri di passaporto degli Stati Uniti.

Argomenti

- [Credenziali](#)
- [Informazioni finanziarie](#)
- [Informazioni personali di identificazione \(PII\)](#)
- [Aggiornamenti al set consigliato](#)

Per dettagli sugli identificatori di dati gestiti specifici o per un elenco completo di tutti gli identificatori di dati gestiti attualmente forniti da Macie, consulta [Utilizzo di identificatori di dati gestiti](#).

Credenziali

Per rilevare le occorrenze dei dati relativi alle credenziali negli oggetti S3, il set consigliato utilizza i seguenti identificatori di dati gestiti.

Tipo di dati sensibili	ID identificatore dei dati gestiti
AWS chiave di accesso segreta	AWS_CREDENTIALS
Intestazione HTTP Basic Authorization	HTTP_BASIC_AUTH_HEADER
Chiave privata OpenSSH	OPENSSSH_PRIVATE_KEY
Chiave privata PGP	PGP_PRIVATE_KEY
Chiave privata Public Key Cryptography Standard (PKCS)	PKCS
Chiave privata PuTTY	PUTTY_PRIVATE_KEY

Informazioni finanziarie

Per rilevare le occorrenze di informazioni finanziarie negli oggetti S3, il set consigliato utilizza i seguenti identificatori di dati gestiti.

Tipo di dati sensibili	ID identificatore dei dati gestiti
Dati a banda magnetica della carta di credito	CREDIT_CARD_MAGNETIC_STRIPE

Tipo di dati sensibili	ID identificatore dei dati gestiti
Numero di carta di credito	CREDIT_CARD_NUMBER (per i numeri di carte di credito in prossimità di una parola chiave)

Informazioni personali di identificazione (PII)

Per rilevare le occorrenze di informazioni di identificazione personale (PII) negli oggetti S3, il set consigliato utilizza i seguenti identificatori di dati gestiti.

Tipo di dati sensibili	ID identificatore dei dati gestiti
Numero identificativo della patente di guida	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (per gli Stati Uniti), UK_DRIVERS_LICENSE
Numero di lista elettorale	UK_ELECTORAL_ROLL_NUMBER
Numeri di carta d'identità	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Numero NINO (National Insurance Number)	UK_NATIONAL_INSURANCE_NUMBER
Numero di passaporto	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Social Insurance Number (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Social Security number (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Tipo di dati sensibili	ID identificatore dei dati gestiti
Numero identificativo del contribuente o codice fiscale	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Aggiornamenti al set consigliato

La tabella seguente descrive le modifiche al set di identificatori di dati gestiti consigliati per i lavori di rilevamento di dati sensibili. Per ricevere avvisi automatici su queste modifiche, iscriviti al feed RSS nella pagina della cronologia dei documenti di [Macie](#).

Modifica	Descrizione	Data
Disponibilità generale	Versione iniziale del set consigliato.	27 giugno 2023

Analisi di oggetti Amazon S3 crittografati

Quando abiliti Amazon Macie for your Account AWS, Macie crea un [ruolo collegato al servizio](#) che concede a Macie le autorizzazioni necessarie per chiamare Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e altro per tuo conto. Servizi AWS Un ruolo collegato al servizio semplifica il processo di configurazione di un ruolo Servizio AWS perché non è necessario aggiungere manualmente le autorizzazioni affinché il servizio completi le azioni per tuo conto. Per ulteriori informazioni su questo tipo di ruolo, consulta i [ruoli IAM](#) nella Guida per l'utente. AWS Identity and Access Management

La politica di autorizzazione per il ruolo collegato al servizio Macie (AWSServiceRoleForAmazonMacie) consente a Macie di eseguire azioni che includono il recupero di informazioni sui bucket e sugli oggetti S3 e il recupero e l'analisi di oggetti nei bucket S3.

Se il tuo account è l'account amministratore Macie di un'organizzazione, la politica consente inoltre a Macie di eseguire queste azioni per tuo conto per gli account dei membri dell'organizzazione.

Se un oggetto S3 è crittografato, la politica di autorizzazione per il ruolo collegato al servizio Macie in genere concede a Macie le autorizzazioni necessarie per decrittografare l'oggetto. Tuttavia, ciò dipende dal tipo di crittografia utilizzato. Può anche dipendere dal fatto che Macie sia autorizzato a utilizzare la chiave di crittografia appropriata.

Argomenti

- [Opzioni di crittografia per oggetti Amazon S3](#)
- [Consentire a Macie di utilizzare un servizio gestito dal cliente AWS KMS key](#)

Opzioni di crittografia per oggetti Amazon S3

Amazon S3 supporta diverse opzioni di crittografia per oggetti S3. Per la maggior parte di queste opzioni, Amazon Macie può decrittografare un oggetto utilizzando il ruolo collegato al servizio Macie per il tuo account. Tuttavia, ciò dipende dal tipo di crittografia utilizzato per crittografare un oggetto.

Crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3)

Se un oggetto viene crittografato utilizzando la crittografia lato server con una chiave gestita Amazon S3 (SSE-S3), Macie può decrittografare l'oggetto.

Per ulteriori informazioni su questo tipo di crittografia, consulta la sezione [Uso della crittografia lato server con le chiavi gestite di Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

Crittografia lato server con AWS KMS keys (DSSE-KMS e SSE-KMS)

Se un oggetto viene crittografato utilizzando la crittografia lato server a due livelli o la crittografia lato server con una crittografia gestita (DSSE-KMS o SSE-KMS), Macie può decrittografare l'oggetto. AWS AWS KMS key

Se un oggetto è crittografato utilizzando la crittografia lato server a doppio livello o la crittografia lato server con una crittografia gestita dal cliente AWS KMS key (DSSE-KMS o SSE-KMS), Macie può decrittografare l'oggetto solo se si [consente a Macie di utilizzare la chiave](#). Questo è il caso degli oggetti crittografati con chiavi KMS gestite interamente all'interno e chiavi KMS in un archivio di chiavi esterno. AWS KMS Se a Macie non è consentito utilizzare la chiave KMS applicabile, Macie può solo archiviare e riportare i metadati relativi all'oggetto.

Per ulteriori informazioni su questi tipi di crittografia, consulta [Utilizzo della crittografia lato server a doppio livello con AWS KMS keys e Utilizzo della crittografia lato server con la Guida per l'utente di Amazon AWS KMS keys Simple Storage Service](#).

 Tip

Puoi generare automaticamente un elenco di tutti i clienti gestiti AWS KMS keys a cui Macie deve accedere per analizzare gli oggetti nei bucket S3 per il tuo account. A tale scopo, esegui lo script AWS KMS Permission Analyzer, disponibile nel repository [Amazon Macie Scripts](#) su GitHub. Lo script può anche generare uno script aggiuntivo di comandi (.). AWS Command Line Interface AWS CLI Facoltativamente, puoi eseguire questi comandi per aggiornare le impostazioni e le politiche di configurazione richieste per le chiavi KMS che specifichi.

Crittografia lato server con chiavi fornite dal cliente (SSE-C)

Se un oggetto è crittografato utilizzando la crittografia lato server con una chiave fornita dal cliente (SSE-C), Macie non può decrittografare l'oggetto. Macie può solo archiviare e riportare i metadati dell'oggetto.

Per ulteriori informazioni su questo tipo di crittografia, consulta la sezione [Uso della crittografia lato server con chiavi fornite dal cliente nella Guida per l'utente di Amazon Simple Storage Service](#).

Crittografia lato client

Se un oggetto è crittografato utilizzando la crittografia lato client, Macie non può decrittografare l'oggetto. Macie può solo archiviare e riportare i metadati dell'oggetto. Ad esempio, Macie può riportare le dimensioni dell'oggetto e i tag associati all'oggetto.

Per informazioni su questo tipo di crittografia nel contesto di Amazon S3, consulta [Proteggere i dati utilizzando la crittografia lato client nella Guida per l'utente di Amazon Simple Storage Service](#).

Puoi [filtrare l'inventario dei bucket](#) in Macie per determinare in quali bucket S3 sono archiviati oggetti che utilizzano determinati tipi di crittografia. Puoi anche determinare quali bucket utilizzano determinati tipi di crittografia lato server per impostazione predefinita quando archiviano nuovi oggetti.

La tabella seguente fornisce esempi di filtri che puoi applicare al tuo inventario dei bucket per trovare queste informazioni.

Per mostrare i bucket che...	Applica questo filtro...
Archivia oggetti che utilizzano la crittografia SSE-C	Il numero di oggetti mediante crittografia è fornito dal cliente e il valore da = 1
Archivia oggetti che utilizzano la crittografia DSSE-KMS o SSE-KMS	Il conteggio degli oggetti tramite crittografia viene gestito e il valore From = 1 AWS KMS
Archivia oggetti che utilizzano la crittografia SSE-S3	Il numero di oggetti tramite crittografia è gestito da Amazon S3 e From = 1
Archivia oggetti che utilizzano la crittografia lato client (o non sono crittografati)	Il numero di oggetti mediante crittografia è Nessuna crittografia e Da = 1
Crittografa nuovi oggetti per impostazione predefinita utilizzando la crittografia DSSE-KMS	Crittografia predefinita = aws:kms:dsse
Crittografa nuovi oggetti per impostazione predefinita utilizzando la crittografia SSE-KMS	Crittografia predefinita = aws:kms
Crittografa nuovi oggetti per impostazione predefinita utilizzando la crittografia SSE-S3	Crittografia predefinita = AES256

Se un bucket è configurato per crittografare nuovi oggetti per impostazione predefinita utilizzando la crittografia DSSE-KMS o SSE-KMS, puoi anche determinare quale viene utilizzato. AWS KMS key Per fare ciò, scegli il bucket nella pagina dei bucket S3. Nel pannello dei dettagli del bucket, sotto Crittografia lato server, fai riferimento al campo. AWS KMS key Questo campo mostra l'Amazon Resource Name (ARN) o l'identificatore univoco (ID chiave) per la chiave.

Consentire a Macie di utilizzare un servizio gestito dal cliente AWS KMS key

Se un oggetto Amazon S3 è crittografato utilizzando la crittografia lato server a doppio livello o la crittografia lato server con una crittografia gestita dal cliente (AWS KMS key DSSE-KMS o SSE-KMS), Amazon Macie può decrittografare l'oggetto solo se gli è consentito l'uso della chiave. Il modo

in cui fornire questo accesso dipende dal fatto che l'account proprietario della chiave possieda anche il bucket S3 che memorizza l'oggetto:

- Se lo stesso account possiede l' AWS KMS key and the bucket, un utente dell'account deve aggiornare la policy della chiave.
- Se un account possiede il bucket AWS KMS key e un altro account possiede il bucket, un utente dell'account che possiede la chiave deve consentire l'accesso alla chiave da più account.

Questo argomento descrive come eseguire queste attività e fornisce esempi per entrambi gli scenari. Per ulteriori informazioni su come consentire l'accesso ai servizi gestiti dai clienti AWS KMS keys, consulta [l'accesso e le autorizzazioni con chiave KMS nella Guida](#) per gli AWS Key Management Service sviluppatori.

Consentire l'accesso dello stesso account a una chiave gestita dal cliente

Se lo stesso account possiede AWS KMS key sia il bucket S3 che il bucket S3, un utente dell'account deve aggiungere una dichiarazione alla policy relativa alla chiave. L'istruzione aggiuntiva deve consentire al ruolo collegato al servizio Macie dell'account di decrittografare i dati utilizzando la chiave. Per informazioni dettagliate sull'aggiornamento di una policy chiave, consulta [Changing a key policy nella Developer Guide](#).AWS Key Management Service

Nella dichiarazione:

- L'Principalelemento deve specificare l'Amazon Resource Name (ARN) del ruolo collegato al servizio Macie per l'account proprietario del bucket e del bucket S3. AWS KMS key

Se l'account è in modalità opt-in Regione AWS, l'ARN deve includere anche il codice regionale appropriato per la regione. Ad esempio, se l'account si trova nella regione del Medio Oriente (Bahrein), che ha il codice regionale me-south-1, l'Principalelemento deve specificare `arn:aws:iam::123456789012:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` dov'è l'ID dell'account. **123456789012** Per un elenco dei codici regionali per le regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

- L'Actionarray deve specificare l'azione. `kms:Decrypt` Questa è l'unica AWS KMS azione che Macie deve essere autorizzata a eseguire per decrittografare un oggetto S3 crittografato con la chiave.

Di seguito è riportato un esempio dell'istruzione da aggiungere alla policy per un. AWS KMS key

```
{
  "Sid": "Allow the Macie service-linked role to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Nell'esempio precedente:

- Il `AWS` campo nell'`Principal` elemento specifica l'ARN del ruolo `AWSServiceRoleForAmazonMacie` collegato al servizio Macie () per l'account. Consente al ruolo collegato al servizio Macie di eseguire l'azione specificata dall'informativa sulla politica. `123456789012` è un esempio di ID di account. Sostituisci questo valore con l'ID dell'account che possiede la chiave KMS e il bucket S3.
- L'`Action` array specifica l'azione che il ruolo collegato al servizio Macie può eseguire utilizzando la chiave KMS: decrittografare il testo cifrato crittografato con la chiave.

La posizione in cui si aggiunge questa dichiarazione a una politica chiave dipende dalla struttura e dagli elementi attualmente contenuti nella politica. Quando aggiungete l'istruzione, assicuratevi che la sintassi sia valida. Le politiche chiave utilizzano il formato JSON. Ciò significa che è necessario aggiungere anche una virgola prima o dopo l'istruzione, a seconda di dove si aggiunge l'istruzione alla politica.

Consentire l'accesso tra più account a una chiave gestita dal cliente

Se un account possiede il AWS KMS key (proprietario della chiave) e un altro account possiede il bucket S3 (proprietario del bucket), il proprietario della chiave deve fornire al proprietario del bucket l'accesso multiaccount alla chiave KMS. Per fare ciò, il proprietario della chiave si assicura innanzitutto che la politica della chiave consenta al proprietario del bucket di utilizzare la chiave e di creare una concessione per la chiave. Il proprietario del bucket crea quindi una concessione per la chiave. Una sovvenzione è uno strumento politico che consente ai AWS mandanti di utilizzare le chiavi KMS nelle operazioni crittografiche se le condizioni specificate dalla concessione sono

soddisfatte. In questo caso, la concessione delega le autorizzazioni pertinenti al ruolo collegato al servizio Macie per l'account del proprietario del bucket.

Per informazioni dettagliate sull'aggiornamento di una politica chiave, consulta [Modifica di una politica chiave nella Guida per gli sviluppatori](#). AWS Key Management Service Per ulteriori informazioni sulle sovvenzioni, consulta [Grants AWS KMS nella AWS Key Management Service Developer Guide](#).

Fase 1: Aggiorna la politica chiave

Nella politica chiave, il proprietario della chiave deve assicurarsi che la politica includa due dichiarazioni:

- La prima istruzione consente al proprietario del bucket di utilizzare la chiave per decrittografare i dati.
- La seconda istruzione consente al proprietario del bucket di creare una concessione per il ruolo collegato al servizio Macie per il proprio account (del proprietario del bucket).

Nella prima istruzione, l'Principalelemento deve specificare l'ARN dell'account del proprietario del bucket. L'Actionarray deve specificare l'azione. kms:Decrypt Questa è l'unica AWS KMS azione che Macie deve poter eseguire per decriptare un oggetto cifrato con la chiave. Di seguito è riportato un esempio di questa dichiarazione nella politica per un. AWS KMS key

```
{
  "Sid": "Allow account 111122223333 to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Nell'esempio precedente:

- Il AWS campo nell'Principalelemento specifica l'ARN dell'account del proprietario del bucket (). **111122223333** Consente al proprietario del bucket di eseguire l'azione specificata dalla dichiarazione politica. **111122223333** è un esempio di ID di account. Sostituisci questo valore con l'ID dell'account del proprietario del bucket.

- L'Actionarray specifica l'azione che il proprietario del bucket è autorizzato a eseguire utilizzando la chiave KMS: decrittografare il testo cifrato crittografato con la chiave.

La seconda dichiarazione della policy chiave consente al proprietario del bucket di creare una concessione per il ruolo collegato al servizio Macie per il proprio account. In questa istruzione, l'Principalelemento deve specificare l'ARN dell'account del proprietario del bucket. L'Actionarray deve specificare l'azione. kms:CreateGrant Un Condition elemento può filtrare l'accesso kms:CreateGrant all'azione specificata nell'istruzione. Di seguito è riportato un esempio di questa dichiarazione nella politica per un AWS KMS key.

```
{
  "Sid": "Allow account 111122223333 to create a grant",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:CreateGrant"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
    }
  }
}
```

Nell'esempio precedente:

- Il AWS campo nell'Principalelemento specifica l'ARN dell'account del proprietario del bucket (). 111122223333 Consente al proprietario del bucket di eseguire l'azione specificata dalla dichiarazione politica. 111122223333 è un esempio di ID di account. Sostituisci questo valore con l'ID dell'account del proprietario del bucket.
- L'Actionarray specifica l'azione che il proprietario del bucket è autorizzato a eseguire sulla chiave KMS: creare una concessione per la chiave.
- L'Conditionelemento utilizza l'[operatore di StringEquals condizione](#) e la [chiave di kms:GranteePrincipal condizione](#) per filtrare l'accesso all'azione specificata dall'informativa. In questo caso, il proprietario del bucket può creare una concessione solo per l'account

`specificatoGranteePrincipal`, che è l'ARN del ruolo collegato al servizio Macie per il proprio account. In quell'ARN, **111122223333** c'è un esempio di ID account. Sostituisci questo valore con l'ID dell'account del proprietario del bucket.

Se l'account del proprietario del bucket è abilitato Regione AWS, includi anche il codice regionale appropriato nell'ARN del ruolo collegato al servizio Macie. Ad esempio, se l'account si trova nella regione Medio Oriente (Bahrein), che ha il codice regionale `me-south-1`, sostituiscilo con `macie.amazonaws.com` `macie.me-south-1.amazonaws.com`. Per un elenco dei codici regionali per le regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

Il luogo in cui il proprietario della chiave aggiunge queste istruzioni alla politica chiave dipende dalla struttura e dagli elementi attualmente contenuti nella politica. Quando il proprietario della chiave aggiunge le istruzioni, deve assicurarsi che la sintassi sia valida. Le politiche chiave utilizzano il formato JSON. Ciò significa che il proprietario della chiave deve aggiungere anche una virgola prima o dopo ogni istruzione, a seconda di dove aggiunge l'istruzione alla politica.

Fase 2: Creare una sovvenzione

Dopo che il proprietario della chiave ha aggiornato la policy chiave secondo necessità, il proprietario del bucket deve creare una concessione per la chiave. La concessione delega le autorizzazioni pertinenti al ruolo collegato al servizio Macie per il loro account (del proprietario del bucket). Prima che il proprietario del bucket crei la concessione, deve verificare di essere autorizzato a eseguire l'azione per il proprio account. `kms:CreateGrant` Questa azione consente loro di aggiungere una sovvenzione a una sovvenzione esistente gestita AWS KMS key dal cliente.

Per creare la concessione, il proprietario del bucket può utilizzare il [CreateGrant](#) funzionamento dell'AWS Key Management Service API. Quando il proprietario del bucket crea la concessione, deve specificare i seguenti valori per i parametri richiesti:

- **KeyId**— L'ARN della chiave KMS. Per l'accesso tra account a una chiave KMS, questo valore deve essere un ARN. Non può essere un ID chiave.
- **GranteePrincipal**— L'ARN del ruolo collegato al servizio Macie (`AWSServiceRoleForAmazonMacie` per il loro account. Questo valore dovrebbe essere `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie:111122223333` dov'è l'ID dell'account del proprietario del bucket.

Se l'account si trova in una regione che accetta l'iscrizione, l'ARN deve includere il codice regionale appropriato. Ad esempio, se il suo account si trova nella regione del Medio Oriente (Bahrein), che ha il codice regionale `me-south-1`, l'ARN dovrebbe essere `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` essere, `111122223333` dov'è l'ID dell'account del proprietario del bucket.

- **Operations**— L'azione di decrittografia (`Decrypt`). AWS KMS Decrypt Questa è l'unica AWS KMS azione che Macie deve poter eseguire per decrittare un oggetto cifrato con la chiave KMS.

[Per creare una concessione per una chiave KMS gestita dal cliente utilizzando AWS Command Line Interface \(AWS CLI\), esegui il comando `create-grant`.](#) L'esempio seguente mostra come. L'esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws kms create-grant ^  
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^  
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/  
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^  
--operations "Decrypt"
```

Dove:

- `key-id` specifica l'ARN della chiave KMS a cui applicare la concessione.
- `grantee-principal` specifica l'ARN del ruolo collegato al servizio Macie per l'account autorizzato a eseguire l'azione specificata dalla concessione. Questo valore deve corrispondere all'ARN specificato dalla `kms:GranteePrincipal` condizione della seconda istruzione nella policy chiave.
- `operations` specifica l'azione che la concessione consente al principale specificato di eseguire: decrittografare il testo cifrato crittografato con la chiave KMS.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{  
  "GrantToken": "<grant token>",  
  "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"  
}
```

Dove `GrantToken` è una stringa univoca, non segreta, a lunghezza variabile e con codifica in base64 che rappresenta la concessione creata e ne rappresenta l'identificatore univoco. `GrantId`

Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili

Quando esegui un processo di rilevamento di dati sensibili o Amazon Macie esegue un rilevamento automatico di dati sensibili, Macie crea un record di analisi per ogni oggetto Amazon Simple Storage Service (Amazon S3) incluso nell'ambito dell'analisi. Questi record, denominati risultati di rilevamento di dati sensibili, registrano i dettagli sull'analisi eseguita da Macie su singoli oggetti S3. Ciò include oggetti in cui Macie non rileva dati sensibili e che quindi non producono risultati, e oggetti che Macie non può analizzare a causa di errori o problemi. Se Macie rileva dati sensibili in un oggetto, il record include i dati del risultato corrispondente e informazioni aggiuntive. I risultati dell'individuazione di dati sensibili forniscono record di analisi che possono essere utili per controlli o indagini sulla privacy e sulla protezione dei dati.

Macie archivia i risultati della scoperta dei dati sensibili per soli 90 giorni. Per accedere ai risultati e consentirne l'archiviazione e la conservazione a lungo termine, configura Macie per crittografare i risultati con una chiave AWS Key Management Service (AWS KMS) e archivarli in un bucket S3. Il bucket può fungere da archivio definitivo a lungo termine per tutti i risultati della scoperta di dati sensibili. È quindi possibile, facoltativamente, accedere e interrogare i risultati in tale repository.

Questo argomento illustra il processo di configurazione di un repository AWS Management Console per i risultati della scoperta di dati sensibili. La configurazione è una combinazione di un AWS KMS key che crittografa i risultati, un bucket S3 generico che archivia i risultati e impostazioni Macie che specificano la chiave e il bucket da utilizzare. Se preferisci configurare le impostazioni di Macie a livello di codice, puoi utilizzare il [PutClassificationExportConfiguration](#) funzionamento dell'API Amazon Macie.

Quando configuri le impostazioni in Macie, le tue scelte si applicano solo a quelle correnti. Regione AWS Se sei l'amministratore Macie di un'organizzazione, le tue scelte si applicano solo al tuo account. Non si applicano agli account dei membri associati. Se abiliti il rilevamento automatico di dati sensibili o esegui processi di rilevamento di dati sensibili per analizzare i dati degli account dei membri, Macie archivia i risultati dell'individuazione dei dati sensibili nell'archivio del tuo account amministratore.

Se usi Macie in più di una Regione AWS, configura le impostazioni del repository per ogni regione in cui usi Macie. Facoltativamente, puoi archiviare i risultati del rilevamento di dati sensibili per più regioni nello stesso bucket S3. Tuttavia, tieni presente i seguenti requisiti:

- Per memorizzare i risultati per una regione AWS abilitata per impostazione predefinita Account AWS, ad esempio la regione Stati Uniti orientali (Virginia settentrionale), devi scegliere un bucket in una regione abilitata per impostazione predefinita. I risultati non possono essere archiviati in un bucket in una regione opzionale (regione disattivata per impostazione predefinita).
- Per memorizzare i risultati per una regione opt-in, come la regione del Medio Oriente (Bahrein), devi scegliere un bucket nella stessa regione o in una regione abilitata per impostazione predefinita. I risultati non possono essere archiviati in un bucket in un'altra regione opt-in.

Per determinare se una regione è abilitata per impostazione predefinita, consulta [Abilita o disabilita Regioni AWS nel tuo account nella Guida](#) per l'Gestione dell'account AWS utente. Oltre ai requisiti precedenti, valuta anche se desideri [recuperare campioni di dati sensibili](#) che Macie riporta nei singoli risultati. Per recuperare campioni di dati sensibili da un oggetto S3 interessato, tutte le seguenti risorse e dati devono essere archiviati nella stessa area: l'oggetto interessato, il risultato applicabile e il corrispondente risultato della scoperta dei dati sensibili.

Attività

- [Prima di iniziare: impara i concetti chiave](#)
- [Fase 1: Verifica le tue autorizzazioni](#)
- [Fase 2: Configurare un AWS KMS key](#)
- [Passaggio 3: scegli un bucket S3](#)

Prima di iniziare: impara i concetti chiave

Amazon Macie crea automaticamente un risultato di rilevamento di dati sensibili per ogni oggetto Amazon S3 che analizza o tenta di analizzare quando esegui un processo di rilevamento di dati sensibili o esegue un rilevamento automatico di dati sensibili. Questo include:

- Oggetti in cui Macie rileva dati sensibili e quindi producono anche risultati su dati sensibili.
- Oggetti in cui Macie non rileva dati sensibili e quindi non producono risultati su dati sensibili.
- Oggetti che Macie non può analizzare a causa di errori o problemi come le impostazioni delle autorizzazioni o l'uso di un file o di un formato di archiviazione non supportato.

Se Macie rileva dati sensibili in un oggetto S3, il risultato della scoperta dei dati sensibili include i dati della corrispondente ricerca di dati sensibili. Fornisce anche informazioni aggiuntive, come la posizione di ben 1.000 occorrenze di ogni tipo di dati sensibili che Macie ha trovato nell'oggetto. Per esempio:

- Il numero di colonna e di riga per una cella o un campo in una cartella di lavoro di Microsoft Excel, un file CSV o un file TSV
- Il percorso di un campo o di una matrice in un file JSON o JSON Lines
- Il numero di riga di una riga in un file di testo non binario diverso da un file CSV, JSON, JSON Lines o TSV, ad esempio un file HTML, TXT o XML
- Il numero di pagina di una pagina in un file Adobe Portable Document Format (PDF)
- L'indice dei record e il percorso di un campo in un record in un contenitore di oggetti Apache Avro o in un file Apache Parquet

Se l'oggetto S3 interessato è un file di archivio, ad esempio un file.tar o.zip, il risultato della scoperta dei dati sensibili fornisce anche dati dettagliati sulla posizione delle occorrenze di dati sensibili nei singoli file che Macie ha estratto dall'archivio. Macie non include queste informazioni nelle rilevazioni di dati sensibili per i file di archivio. Per riportare i dati sulla posizione, i risultati del rilevamento dei dati sensibili utilizzano uno schema [JSON standardizzato](#).

Un risultato di scoperta di dati sensibili non include i dati sensibili trovati da Macie. Fornisce invece un record di analisi che può essere utile per audit o indagini.

Macie archivia i risultati della scoperta dei dati sensibili per 90 giorni. Non puoi accedervi direttamente dalla console Amazon Macie o con l'API Amazon Macie. Segui invece i passaggi descritti in questo argomento per configurare Macie in modo AWS KMS key che crittografi i risultati con un file specificato da te e memorizzi i risultati in un bucket S3 generico da te specificato. Macie scrive quindi i risultati nei file JSON Lines (.jsonl), aggiunge i file al bucket come file GNU Zip (.gz) e crittografa i dati utilizzando la crittografia SSE-KMS. A partire dall'8 novembre 2023, Macie firma anche gli oggetti S3 risultanti con un codice di autenticazione dei messaggi basato su Hash (HMAC). AWS KMS key

Dopo aver configurato Macie per archiviare i risultati del rilevamento dei dati sensibili in un bucket S3, il bucket può fungere da archivio definitivo a lungo termine per i risultati. È quindi possibile, facoltativamente, accedere e interrogare i risultati in quel repository.

Suggerimenti

Per un esempio dettagliato e istruttivo su come interrogare e utilizzare i risultati del rilevamento di dati sensibili per analizzare e segnalare potenziali rischi per la sicurezza dei dati, consulta il seguente post sul blog sulla AWS sicurezza: [Come interrogare e visualizzare i risultati del rilevamento dei dati sensibili di Macie con Amazon Athena](#) e Amazon QuickSight. Per esempi di query Amazon Athena da utilizzare per analizzare i risultati del rilevamento di dati sensibili, visita il repository di [Amazon Macie Results Analytics](#) su GitHub. Questo repository fornisce anche istruzioni per configurare Athena per recuperare e decrittografare i risultati e script per creare tabelle per i risultati.

Fase 1: Verifica le tue autorizzazioni

Prima di configurare un repository per i risultati del rilevamento dei dati sensibili, verifica di disporre delle autorizzazioni necessarie per crittografare e archiviare i risultati. Per verificare le tue autorizzazioni, utilizza AWS Identity and Access Management (IAM) per esaminare le policy IAM associate alla tua identità IAM. Quindi confronta le informazioni contenute in tali policy con il seguente elenco di azioni che devi essere autorizzato a eseguire per configurare il repository.

Amazon Macie

Per Macie, verifica di avere il permesso di eseguire la seguente azione:

`macie2:PutClassificationExportConfiguration`

Questa azione ti consente di aggiungere o modificare le impostazioni del repository in Macie.

Amazon S3

Per Amazon S3, verifica di essere autorizzato a eseguire le seguenti azioni:

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

Queste azioni consentono di accedere e configurare un bucket S3 generico che può fungere da repository.

AWS KMS

Per utilizzare la console Amazon Macie per aggiungere o modificare le impostazioni del repository, verifica anche di essere autorizzato a eseguire le seguenti azioni: AWS KMS

- `kms:DescribeKey`
- `kms:ListAliases`

Queste azioni ti consentono di recuperare e visualizzare informazioni AWS KMS keys relative al tuo account. Puoi quindi scegliere una di queste chiavi per crittografare i risultati del rilevamento dei dati sensibili.

Se prevedi di crearne una nuova AWS KMS key per crittografare i dati, devi anche avere il permesso di eseguire le seguenti azioni: `kms:CreateKey`, `kms:GetKeyPolicy`, e `kms:PutKeyPolicy`

Se non sei autorizzato a eseguire le azioni richieste, chiedi assistenza AWS all'amministratore prima di procedere al passaggio successivo.

Fase 2: Configurare un AWS KMS key

Dopo aver verificato le autorizzazioni, stabilisci quale AWS KMS key vuoi che Macie utilizzi per crittografare i risultati del rilevamento dei dati sensibili. La chiave deve essere una chiave KMS con crittografia simmetrica gestita dal cliente e abilitata nello stesso Regione AWS bucket S3 in cui desideri archiviare i risultati.

La chiave può essere esistente nel tuo account o AWS KMS key di proprietà di un altro account. **AWS KMS key** Se desideri utilizzare una nuova chiave KMS, crea la chiave prima di procedere. Se desideri utilizzare una chiave esistente di proprietà di un altro account, ottieni l'Amazon Resource Name (ARN) della chiave. Dovrai inserire questo ARN quando configuri le impostazioni del repository in Macie. [Per informazioni sulla creazione e la revisione delle impostazioni per le chiavi KMS, consulta la Guida per gli sviluppatori.AWS Key Management Service](#)

Note

La chiave può trovarsi AWS KMS key in un archivio di chiavi esterno. Tuttavia, la chiave potrebbe quindi essere più lenta e meno affidabile di una chiave gestita interamente

all'interno AWS KMS. Puoi ridurre questo rischio archiviando i risultati del rilevamento dei dati sensibili in un bucket S3 configurato per utilizzare la chiave come chiave S3 Bucket. In questo modo si riduce il numero di AWS KMS richieste da effettuare per crittografare i risultati del rilevamento dei dati sensibili.

Per informazioni sull'utilizzo delle chiavi KMS negli archivi di chiavi esterni, consulta Archivi di [chiavi esterni nella Guida](#) per gli AWS Key Management Service sviluppatori. Per informazioni sull'uso di S3 Bucket Keys, consulta [Ridurre il costo di SSE-KMS con Amazon S3 Bucket Keys nella Guida per l'utente di Amazon](#) Simple Storage Service.

Dopo aver determinato quale chiave KMS vuoi che Macie utilizzi, consenti a Macie il permesso di usare la chiave. Altrimenti, Macie non sarà in grado di crittografare o archiviare i risultati nell'archivio. Per autorizzare Macie a usare la chiave, aggiorna la politica relativa alla chiave. Per informazioni dettagliate sulle politiche chiave e sulla gestione dell'accesso alle chiavi KMS, consulta [le politiche chiave AWS KMS nella Guida](#) per gli AWS Key Management Service sviluppatori.

Per aggiornare la politica chiave

1. Apri la AWS KMS console in <https://console.aws.amazon.com/kms>.
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Scegli la chiave che vuoi che Macie utilizzi per crittografare i risultati del rilevamento dei dati sensibili.
4. Nella scheda Policy della chiave, seleziona Modifica.
5. Copia la seguente dichiarazione negli appunti e aggiungila alla policy:

```
{
  "Sid": "Allow Macie to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "macie.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```

    "aws:SourceAccount": "111122223333"
  },
  "ArnLike": {
    "aws:SourceArn": [
      "arn:aws:macie2:Region:111122223333:export-configuration:*",
      "arn:aws:macie2:Region:111122223333:classification-job/*"
    ]
  }
}

```

Note

Quando si aggiunge l'istruzione alla policy, assicurarsi che la sintassi sia valida. Le politiche utilizzano il formato JSON. Ciò significa che è necessario aggiungere anche una virgola prima o dopo l'istruzione, a seconda di dove si aggiunge l'istruzione alla politica. Se aggiungete l'istruzione come ultima istruzione, aggiungete una virgola dopo la parentesi corta di chiusura dell'istruzione precedente. Se la aggiungete come prima istruzione o tra due istruzioni esistenti, aggiungete una virgola dopo la parentesi graffa che chiude l'istruzione.

6. Aggiorna l'istruzione con i valori corretti per il tuo ambiente:

- Nei `Condition` campi, sostituisci i valori segnaposto, dove:
 - **111122223333** è l'ID dell'account per il tuo Account AWS
 - **Region** è l'applicazione Regione AWS in cui stai usando Macie e vuoi consentire a Macie di usare la chiave.

Se usi Macie in più regioni e desideri consentire a Macie di utilizzare la chiave in altre regioni, aggiungi le `aws:SourceArn` condizioni per ogni regione aggiuntiva. Per esempio:

```

"aws:SourceArn": [
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
  "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
  "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]

```


In alternativa, puoi consentire a Macie di utilizzare la chiave in tutte le regioni. Per fare ciò, sostituisci il valore del segnaposto con il carattere jolly (*). Per esempio:

```
"aws:SourceArn": [  
  "arn:aws:macie2*:111122223333:export-configuration:*",  
  "arn:aws:macie2*:111122223333:classification-job/*"  
]
```

- Se utilizzi Macie in una regione che richiede l'attivazione, aggiungi il codice regionale appropriato al valore del campo. Service Ad esempio, se utilizzi Macie nella regione Medio Oriente (Bahrein), che ha il codice regionale me-south-1, sostituiscilo con. `macie.amazonaws.com` `macie.me-south-1.amazonaws.com` Per un elenco delle regioni in cui Macie è attualmente disponibile e il codice regionale per ciascuna di esse, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

Tieni presente che i Condition campi utilizzano due chiavi di condizione globali IAM:

- [aws: SourceAccount](#) — Questa condizione consente a Macie di eseguire le azioni specificate solo per il tuo account. Più specificamente, determina quale account può eseguire le azioni specificate per le risorse e le azioni specificate dalla `aws:SourceArn` condizione.

Per consentire a Macie di eseguire le azioni specificate per account aggiuntivi, aggiungi l'ID account per ogni account aggiuntivo a questa condizione. Per esempio:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- [aws: SourceArn](#) — Questa condizione Servizi AWS impedisce ad altri di eseguire le azioni specificate. Inoltre impedisce a Macie di utilizzare la chiave mentre esegue altre azioni per il tuo account. In altre parole, consente a Macie di crittografare gli oggetti S3 con la chiave solo se: gli oggetti sono risultati del rilevamento di dati sensibili e i risultati riguardano il rilevamento automatico di dati sensibili o i processi di scoperta di dati sensibili creati dall'account specificato nella regione specificata.

Per consentire a Macie di eseguire le azioni specificate per account aggiuntivi, aggiungi questa condizione ARNs per ogni account aggiuntivo. Per esempio:

```
"aws:SourceArn": [  
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
```

```
[  
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",  
  "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",  
  "arn:aws:macie2:us-east-1:444455556666:classification-job/*"  
]
```

Gli account specificati dalle `aws:SourceArn` condizioni `aws:SourceAccount` e devono corrispondere.

Queste condizioni aiutano a evitare che Macie venga usato come [vice confuso](#) durante le transazioni con AWS KMS. Anche se non lo consigliamo, puoi rimuovere queste condizioni dall'informativa.

7. Al termine dell'aggiunta e dell'aggiornamento dell'istruzione, scegli Salva modifiche.

Passaggio 3: scegli un bucket S3

Dopo aver verificato le autorizzazioni e configurato il AWS KMS key, sei pronto a specificare quale bucket S3 desideri utilizzare come repository per i risultati del rilevamento dei dati sensibili. Sono disponibili due opzioni:

- Usa un nuovo bucket S3 creato da Macie: se scegli questa opzione, Macie crea automaticamente un nuovo bucket S3 per uso generico nella versione attuale per i risultati del discovery. Regione AWS Macie applica anche una policy sul bucket. La policy consente a Macie di aggiungere oggetti al bucket. Richiede inoltre che gli oggetti siano crittografati con quanto specificato, utilizzando AWS KMS key la crittografia SSE-KMS. Per rivedere la politica, scegli Visualizza politica sulla console Amazon Macie dopo aver specificato un nome per il bucket e la chiave KMS da utilizzare.
- Usa un bucket S3 esistente che hai creato: se preferisci archiviare i risultati del discovery in un particolare bucket S3 da te creato, crea il bucket prima di procedere. Il bucket deve essere un bucket generico. Inoltre, le impostazioni e i criteri del bucket devono consentire a Macie di aggiungere oggetti al bucket. Questo argomento spiega quali impostazioni controllare e come aggiornare la policy. Fornisce inoltre esempi di dichiarazioni da aggiungere alla politica.

Le seguenti sezioni forniscono istruzioni per ciascuna opzione. Scegliete la sezione relativa all'opzione desiderata.

Usa un nuovo bucket S3 creato da Macie

Se preferisci usare un nuovo bucket S3 creato da Macie per te, l'ultimo passaggio del processo consiste nel configurare le impostazioni del repository in Macie.

Per configurare le impostazioni del repository in Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, in Impostazioni, scegli Risultati Discovery.
3. In Repository for sensitive data discovery results, scegli Crea bucket.
4. Nella casella Crea un bucket, inserisci un nome per il bucket.

Il nome deve essere univoco per tutti i bucket S3. Inoltre, il nome può essere composto solo da lettere minuscole, numeri, punti (.) e trattini (-). Per ulteriori requisiti di denominazione, consulta le [regole di denominazione dei bucket](#) nella Guida per l'utente di Amazon Simple Storage Service.

5. Espandere la sezione Advanced (Avanzate).
6. (Facoltativo) Per specificare un prefisso da utilizzare nel percorso verso una posizione nel bucket, inserisci il prefisso nella casella Prefisso dei risultati di Data discovery.

Quando inserisci un valore, Macie aggiorna l'esempio sotto la casella per mostrare il percorso della posizione del bucket in cui verranno archiviati i risultati del rilevamento.

7. Per Blocca tutti gli accessi pubblici, scegli Sì per abilitare tutte le impostazioni di blocco di accesso pubblico per il bucket.

Per informazioni su queste impostazioni, consulta [Bloccare l'accesso pubblico allo storage Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

8. In Impostazioni di crittografia, specifica quelle AWS KMS key che desideri che Macie utilizzi per crittografare i risultati:
 - Per utilizzare una chiave del tuo account, scegli Seleziona una chiave dal tuo account. Quindi, nell'AWS KMS keyelenco, scegli la chiave da usare. L'elenco mostra le chiavi KMS con crittografia simmetrica gestite dal cliente per il tuo account.
 - Per utilizzare una chiave di proprietà di un altro account, scegli Inserisci l'ARN di una chiave di un altro account. Quindi, nella casella AWS KMS key ARN, inserisci l'Amazon Resource Name (ARN) della chiave da utilizzare, ad esempio. **arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab**

9. Quando hai finito di inserire le impostazioni, scegli Salva.

Macie verifica le impostazioni per verificare che siano corrette. Se alcune impostazioni non sono corrette, Macie visualizza un messaggio di errore per aiutarti a risolvere il problema.

Dopo aver salvato le impostazioni del repository, Macie aggiunge al repository i risultati di rilevamento esistenti degli ultimi 90 giorni. Macie inizia anche ad aggiungere nuovi risultati di scoperta al repository.

Usa un bucket S3 esistente che hai creato

Se preferisci archiviare i risultati del rilevamento dei dati sensibili in un particolare bucket S3, devi creare, creare e configurare il bucket prima di configurare le impostazioni in Macie. Quando crei il bucket, tieni presente i seguenti requisiti:

- Il secchio deve essere un secchio per uso generico. Non può essere un altro tipo di bucket, ad esempio un bucket di directory.
- Per memorizzare i risultati di scoperta per una regione abilitata per impostazione predefinita Account AWS, ad esempio la regione Stati Uniti orientali (Virginia settentrionale), il bucket deve trovarsi in una regione abilitata per impostazione predefinita. I risultati non possono essere archiviati in un bucket in una regione opzionale (regione disattivata per impostazione predefinita).
- Per archiviare i risultati di scoperta per una regione che ha scelto di aderire, ad esempio la regione del Medio Oriente (Bahrein), il bucket deve trovarsi nella stessa regione o in una regione abilitata per impostazione predefinita. I risultati non possono essere archiviati in un bucket in un'altra regione opt-in.

Per determinare se una regione è abilitata per impostazione predefinita, consulta [Abilita o disabilita Regioni AWS nel tuo account nella Guida](#) per l'Gestione dell'account AWS utente.

Dopo aver creato il bucket, aggiorna la policy del bucket per consentire a Macie di recuperare informazioni sul bucket e aggiungere oggetti al bucket. Puoi quindi configurare le impostazioni in Macie.

Per aggiornare la policy relativa al bucket

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli il bucket in cui desideri archiviare i risultati della scoperta.
3. Scegli la scheda Autorizzazioni.

4. Seleziona Modifica nella sezione Policy bucket.
5. Copia la seguente politica di esempio negli appunti:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow Macie to use the GetBucketLocation operation",
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:macie2:Region:111122223333:export-configuration:*",
            "arn:aws:macie2:Region:111122223333:classification-job/*"
          ]
        }
      }
    },
    {
      "Sid": "Allow Macie to add objects to the bucket",
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional prefix/*]",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:macie2:Region:111122223333:export-configuration:*",

```

```

        "arn:aws:macie2:Region:111122223333:classification-job/*"
    ]
}
},
{
    "Sid": "Deny unencrypted object uploads. This is optional",
    "Effect": "Deny",
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional prefix/*]",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption": "aws:kms"
        }
    }
},
{
    "Sid": "Deny incorrect encryption headers. This is optional",
    "Effect": "Deny",
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional prefix/*]",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id":
"arn:aws:kms:Region:111122223333:key/KMSKeyId"
        }
    }
},
{
    "Sid": "Deny non-HTTPS access",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "Bool": {
            "aws:SecureTransport": "false"
        }
    }
}

```

```

    }
  }
]
}

```

6. Incolla la policy di esempio nell'editor di policy Bucket sulla console Amazon S3.
7. Aggiorna la policy di esempio con i valori corretti per il tuo ambiente:
 - Nell'istruzione facoltativa che nega le intestazioni di crittografia errate:
 - Sostituisci *amzn-s3-demo-bucket* con il nome del tuo bucket. Per specificare anche un prefisso per un percorso verso una posizione nel bucket, *[optional prefix/]* sostituisilo con il prefisso. Altrimenti, rimuovete il valore segnaposto. *[optional prefix/]*
 - In `StringNotEquals` questa condizione, *arn:aws:kms:Region:111122223333:key/KMSKeyId* sostituisilo con l'Amazon Resource Name (ARN) AWS KMS key da utilizzare per la crittografia dei risultati della scoperta.
 - In tutte le altre istruzioni, sostituisci i valori segnaposto, dove:
 - *amzn-s3-demo-bucket* è il nome del bucket.
 - *[optional prefix/]* è il prefisso per un percorso verso una posizione nel bucket. Rimuovi questo valore segnaposto se non desideri specificare un prefisso.
 - *111122223333* è l'ID dell'account per il tuo. Account AWS
 - *Region* è la Regione AWS applicazione in cui stai usando Macie e vuoi consentire a Macie di aggiungere i risultati delle scoperte.

Se usi Macie in più regioni e desideri consentire a Macie di aggiungere risultati al bucket per altre regioni, aggiungi `aws:SourceArn` le condizioni per ogni regione aggiuntiva. Per esempio:

```

"aws:SourceArn": [
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
  "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
  "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]

```

In alternativa, puoi consentire a Macie di aggiungere risultati al bucket per tutte le regioni in cui usi Macie. A tale scopo, sostituisci il valore del segnaposto con il carattere jolly (*). Per esempio:

```
"aws:SourceArn": [  
    "arn:aws:macie2*:111122223333:export-configuration:*",  
    "arn:aws:macie2*:111122223333:classification-job/*"  
]
```

- Se utilizzi Macie in una regione che prevede l'attivazione, aggiungi il codice regionale appropriato al valore del Service campo in ogni istruzione che specifica l'entità del servizio Macie. Ad esempio, se utilizzi Macie nella regione Medio Oriente (Bahrein), che ha il codice regionale me-south-1, sostituisilo con in ogni istruzione applicabile. `macie.amazonaws.com` `macie.me-south-1.amazonaws.com` Per un elenco delle regioni in cui Macie è attualmente disponibile e il codice regionale per ciascuna di esse, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

Tieni presente che la politica di esempio include istruzioni che consentono a Macie di determinare in quale regione risiede il bucket (`GetBucketLocation`) e di aggiungere oggetti al bucket (`PutObject`). Queste istruzioni definiscono le condizioni che utilizzano due chiavi di condizione globali IAM:

- [aws: SourceAccount](#) — Questa condizione consente a Macie di aggiungere i risultati del rilevamento di dati sensibili al bucket solo per il tuo account. Impedisce a Macie di aggiungere al bucket i risultati di scoperta di altri account. Più specificamente, la condizione specifica quale account può utilizzare il bucket per le risorse e le azioni specificate dalla condizione. `aws:SourceArn`

Per memorizzare i risultati di account aggiuntivi nel bucket, aggiungi l'ID account per ogni account aggiuntivo a questa condizione. Per esempio:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- [aws: SourceArn](#) — Questa condizione limita l'accesso al bucket in base alla fonte degli oggetti che vengono aggiunti al bucket. Impedisce ad altri Servizi AWS di aggiungere oggetti al bucket. Inoltre impedisce a Macie di aggiungere oggetti al bucket mentre esegue altre azioni per il tuo account. Più specificamente, la condizione consente a Macie di aggiungere oggetti al bucket solo se: gli oggetti sono risultati di scoperta di dati sensibili e i risultati riguardano il

rilevamento automatico di dati sensibili o i lavori di scoperta di dati sensibili creati dall'account specificato nella regione specificata.

Per consentire a Macie di eseguire le azioni specificate per account aggiuntivi, aggiungi ARNs per ogni account aggiuntivo questa condizione. Per esempio:

```
"aws:SourceArn": [  
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",  
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",  
  "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",  
  "arn:aws:macie2:us-east-1:444455556666:classification-job/*"  
]
```

Gli account specificati dalle `aws:SourceArn` condizioni `aws:SourceAccount` e devono corrispondere.

Entrambe le condizioni aiutano a evitare che Macie venga usato come [assistente confuso](#) durante le transazioni con Amazon S3. Anche se non lo consigliamo, puoi rimuovere queste condizioni dalla bucket policy.

8. Al termine dell'aggiornamento della policy del bucket, scegli Salva modifiche.

Ora puoi configurare le impostazioni del repository in Macie.

Per configurare le impostazioni del repository in Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, in Impostazioni, scegli Risultati Discovery.
3. In Repository for sensitive data discovery results, scegli Existing bucket.
4. Per Scegli un bucket, seleziona il bucket in cui desideri archiviare i risultati del discovery.
5. Per specificare un prefisso per un percorso verso una posizione nel bucket, espandi la sezione Avanzate. Quindi, per il prefisso dei risultati di Data discovery, inserisci il prefisso.

Quando inserisci un valore, Macie aggiorna l'esempio sotto la casella per mostrare il percorso verso la posizione del bucket in cui verranno archiviati i risultati del rilevamento.

6. In Impostazioni di crittografia, specifica quelle AWS KMS key che desideri che Macie utilizzi per crittografare i risultati:

- Per utilizzare una chiave del tuo account, scegli **Seleziona una chiave dal tuo account**. Quindi, nell'AWS KMS console, scegli la chiave da usare. L'elenco mostra le chiavi KMS con crittografia simmetrica gestite dal cliente per il tuo account.
- Per utilizzare una chiave di proprietà di un altro account, scegli **Inserisci l'ARN di una chiave di un altro account**. Quindi, nella casella AWS KMS key ARN, inserisci l'ARN della chiave da utilizzare, ad esempio. **arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab**

7. Quando hai finito di inserire le impostazioni, scegli **Salva**.

Macie verifica le impostazioni per verificare che siano corrette. Se alcune impostazioni non sono corrette, Macie visualizza un messaggio di errore per aiutarti a risolvere il problema.

Dopo aver salvato le impostazioni del repository, Macie aggiunge al repository i risultati di rilevamento esistenti degli ultimi 90 giorni. Macie inizia anche ad aggiungere nuovi risultati di scoperta al repository.

Note

Se successivamente modifichi l'impostazione del prefisso dei risultati di scoperta dei dati, aggiorna anche la policy del bucket in Amazon S3. Le dichiarazioni politiche che specificano il prefisso precedente devono specificare il nuovo prefisso. Altrimenti, a Macie non sarà consentito aggiungere i risultati della ricerca al bucket.

Tip

Per ridurre i costi di crittografia lato server, configura anche il bucket S3 per utilizzare una chiave S3 Bucket e specifica AWS KMS key quella che hai configurato per la crittografia dei risultati del rilevamento dei dati sensibili. L'uso di una S3 Bucket Key riduce il numero di chiamate a, il che può ridurre i costi delle richieste. AWS KMS AWS KMS Se la chiave KMS si trova in un archivio di chiavi esterno, l'uso di una chiave S3 Bucket può anche ridurre al minimo l'impatto sulle prestazioni dell'utilizzo della chiave. Per ulteriori informazioni, consulta [Ridurre il costo di SSE-KMS con Amazon S3 Bucket Keys nella Guida per l'utente di Amazon Simple Storage Service](#).

Classi e formati di storage supportati

Per aiutarti a scoprire dati sensibili nel tuo patrimonio di dati Amazon Simple Storage Service (Amazon S3), Amazon Macie supporta la maggior parte delle classi di storage di Amazon S3 e un'ampia varietà di formati di file e storage. Questo supporto si applica all'uso di identificatori di [dati gestiti e all'uso di identificatori](#) di [dati personalizzati per analizzare oggetti S3](#).

Affinché Macie possa analizzare un oggetto S3, l'oggetto deve essere archiviato in un bucket Amazon S3 generico utilizzando una classe di storage supportata. L'oggetto deve inoltre utilizzare un file o un formato di archiviazione supportato. Gli argomenti di questa sezione elencano le classi di archiviazione e i formati di file e di archiviazione attualmente supportati da Macie.

Tip

Sebbene Macie sia ottimizzato per Amazon S3, puoi utilizzarlo per scoprire dati sensibili nelle risorse che attualmente memorizzi altrove. Puoi farlo spostando i dati su Amazon S3 in modo temporaneo o permanente. Ad esempio, esporta le istantanee di Amazon Relational Database Service o Amazon Aurora su Amazon S3 in formato Apache Parquet. Oppure esporta una tabella Amazon DynamoDB in Amazon S3. È quindi possibile creare un processo di rilevamento dei dati sensibili per analizzare i dati in Amazon S3.

Argomenti

- [Classi di storage Amazon S3 supportate](#)
- [Formati di file e storage supportati](#)

Classi di storage Amazon S3 supportate

Per il rilevamento di dati sensibili, Amazon Macie supporta le seguenti classi di storage Amazon S3:

- Ridondanza ridotta (RRS)
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering
- S3 One Zone-Accesso non frequente (S3 One Zone-IA)
- S3 Standard
- S3 Standard-Accesso non frequente (S3 Standard-IA)

Macie non analizza oggetti S3 che utilizzano altre classi di storage Amazon S3, come S3 Glacier Deep Archive o S3 Express One Zone. Inoltre, Macie non analizza gli oggetti archiviati nei bucket di directory S3.

Se configuri un processo di rilevamento di dati sensibili per analizzare oggetti S3 che non utilizzano una classe di storage Amazon S3 supportata, Macie ignora tali oggetti durante l'esecuzione del processo. Macie non tenta di recuperare o analizzare i dati negli oggetti: gli oggetti vengono trattati come oggetti inclassificabili. Un oggetto inclassificabile è un oggetto che non utilizza una classe di archiviazione supportata o un file o un formato di archiviazione supportati. Macie analizza solo gli oggetti che utilizzano una classe di archiviazione supportata e un file o un formato di archiviazione supportati.

Allo stesso modo, se configuri Macie per eseguire il rilevamento automatico di dati sensibili, gli oggetti inclassificabili non sono idonei per la selezione e l'analisi. Macie seleziona solo gli oggetti che utilizzano una classe di storage Amazon S3 supportata e un file o un formato di storage supportato.

[Per identificare i bucket S3 che memorizzano oggetti inclassificabili, puoi filtrare l'inventario del bucket S3.](#) Per ogni bucket del tuo inventario, ci sono campi che riportano il numero e la dimensione totale di archiviazione degli oggetti inclassificabili nel bucket.

Per informazioni dettagliate sulle classi di storage fornite da Amazon S3, consulta [Using Amazon S3 Storage Classes nella Amazon Simple Storage Service User Guide](#).

Formati di file e storage supportati

Quando Amazon Macie analizza un oggetto S3, Macie recupera la versione più recente dell'oggetto da Amazon S3, quindi esegue un'ispezione approfondita del contenuto dell'oggetto. Questa ispezione tiene conto del file o del formato di archiviazione dei dati. Macie può analizzare i dati in molti formati diversi, inclusi i formati di compressione e archiviazione di uso comune.

Quando Macie analizza i dati in un file compresso o di archivio, Macie ispeziona sia il file completo che il contenuto del file. Per controllare il contenuto del file, Macie decompone il file, quindi ispeziona ogni file estratto che utilizza un formato supportato. Macie può eseguire questa operazione per un massimo di 1.000.000 di file e fino a una profondità annidata di 10 livelli. Per informazioni sulle quote aggiuntive applicabili all'individuazione di dati sensibili, consulta [Quote per Macie](#)

La tabella seguente elenca e descrive i tipi di file e formati di archiviazione che Macie può analizzare per rilevare dati sensibili. Per ogni tipo supportato, la tabella elenca anche le estensioni dei nomi di file applicabili.

Tipo di file o archiviazione	Descrizione	Estensioni dei nomi di file
Big Data	Contenitori di oggetti Apache Avro e file Apache Parquet	.avro, .parquet
Compressione o archiviazione	Archivi compressi GNU Zip, archivi TAR e archivi compressi ZIP	.gz, .gzip, .tar, .zip
Documento	File Adobe Portable Document Format, cartelle di lavoro Microsoft Excel e documenti Microsoft Word	.doc, .docx, .pdf, .xls, .xlsx
Messaggio di posta elettronica	File di posta elettronica il cui contenuto è conforme ai requisiti specificati da una RFC IETF per i messaggi di posta elettronica, come RFC 2822	.eml
Testo	File di testo non binari. Alcuni esempi sono: file con valori separati da virgole (CSV), file Extensible Markup Language (XML), file HTML (Hypertext Markup Language), file JSON (JavaScript Object Notation), file JSON Lines, documenti in chiaro, file con valori separati da tabulazioni (TSV) e file YAML	A seconda del tipo di file di testo non binario: .csv, .htm, .html, .json, .jsonl, .tsv e altri

Macie non analizza i dati nelle immagini o nei contenuti audio, video e altri tipi di contenuti multimediali.

Se configuri un processo di rilevamento di dati sensibili per analizzare oggetti S3 che non utilizzano un formato di file o di archiviazione supportato, Macie ignora tali oggetti durante l'esecuzione del lavoro. Macie non tenta di recuperare o analizzare i dati negli oggetti: gli oggetti vengono trattati come oggetti inclassificabili. Un oggetto inclassificabile è un oggetto che non utilizza una classe di storage Amazon S3 supportata o un file o un formato di storage supportato. Macie analizza solo gli oggetti che utilizzano una classe di storage supportata e un file o un formato di archiviazione supportati.

Allo stesso modo, se configuri Macie per eseguire il rilevamento automatico di dati sensibili, gli oggetti inclassificabili non sono idonei per la selezione e l'analisi. Macie seleziona solo gli oggetti che utilizzano una classe di storage Amazon S3 supportata e un file o un formato di storage supportato.

[Per identificare i bucket S3 che memorizzano oggetti inclassificabili, puoi filtrare l'inventario dei bucket S3.](#) Per ogni bucket del tuo inventario, ci sono campi che riportano il numero e la dimensione totale di archiviazione degli oggetti inclassificabili nel bucket.

Revisione e analisi dei risultati di Macie

Amazon Macie genera risultati quando rileva potenziali violazioni delle policy o problemi con la sicurezza o la privacy dei bucket generici Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) o rileva dati sensibili in oggetti S3. Un risultato è un rapporto dettagliato di un potenziale problema o di dati sensibili rilevati da Macie. Ogni risultato fornisce un indice di gravità, informazioni sulla risorsa interessata e dettagli aggiuntivi, ad esempio quando e come Macie ha rilevato il problema o i dati. Macie archivia le tue policy e i risultati relativi ai dati sensibili per 90 giorni.

Puoi rivedere, analizzare e gestire i risultati nei seguenti modi.

Console Amazon Macie

Le pagine Findings sulla console Amazon Macie elencano i risultati e forniscono informazioni dettagliate sui singoli risultati. Queste pagine forniscono anche opzioni per raggruppare, filtrare e ordinare i risultati e per creare e gestire regole di soppressione. Le regole di soppressione possono aiutarvi a semplificare l'analisi dei risultati.

API Amazon Macie

Con l'API Amazon Macie, puoi interrogare e recuperare i dati dei risultati utilizzando uno strumento da riga di AWS comando o un AWS SDK o inviando richieste HTTPS direttamente a Macie. Per interrogare i dati, invii una richiesta all'API Amazon Macie e utilizzi i parametri supportati per specificare quali risultati desideri recuperare. Dopo aver inviato la richiesta, Macie restituisce i risultati in una risposta JSON. Puoi quindi passare i risultati a un altro servizio o applicazione per un'analisi più approfondita, l'archiviazione a lungo termine o la creazione di report. Per ulteriori informazioni, consulta [Amazon Macie API Reference](#).

Amazon EventBridge

Per supportare ulteriormente l'integrazione con altri servizi e sistemi, come i sistemi di monitoraggio o di gestione degli eventi, Macie pubblica i risultati su Amazon EventBridge come eventi. EventBridge, precedentemente Amazon CloudWatch Events, è un servizio di bus eventi senza server in grado di fornire un flusso di dati in tempo reale dalle tue applicazioni, applicazioni SaaS (Software as a Service) e come Macie. Servizi AWS Può indirizzare tali dati verso destinazioni come AWS Lambda funzioni, argomenti di Amazon Simple Notification Service e flussi Amazon Kinesis per un'ulteriore elaborazione automatizzata. L'uso di aiuta EventBridge anche a garantire la conservazione a lungo termine dei dati dei risultati. Per ulteriori informazioni EventBridge, consulta la [Amazon EventBridge User Guide](#).

Macie pubblica automaticamente gli eventi EventBridge per nuove scoperte. Inoltre, pubblica automaticamente gli eventi relativi alle ricorrenze successive dei risultati delle politiche esistenti. Poiché i dati sui risultati sono strutturati come EventBridge eventi, è possibile monitorare, analizzare e agire più facilmente in base ai risultati utilizzando altri servizi e strumenti. Ad esempio, è possibile EventBridge inviare automaticamente tipi specifici di nuovi risultati a una AWS Lambda funzione che, a sua volta, elabora e invia i dati al sistema di gestione degli incidenti e degli eventi di sicurezza (SIEM). Se esegui l'integrazione Notifiche all'utente AWS con Macie, puoi anche utilizzare gli eventi per ricevere automaticamente la notifica dei risultati tramite i canali di distribuzione da te specificati. Per ulteriori informazioni sull'utilizzo EventBridge degli eventi per monitorare ed elaborare i risultati, consulta [Elaborazione dei risultati con Amazon EventBridge](#).

AWS Security Hub

Per un'analisi aggiuntiva e più ampia del livello di sicurezza della tua organizzazione, puoi anche pubblicare i risultati su AWS Security Hub. Security Hub è un servizio che raccoglie dati di sicurezza Servizi AWS e soluzioni AWS Partner Network di sicurezza supportate per fornire una visione completa dello stato di sicurezza in tutto l'AWS ambiente. Security Hub ti aiuta anche a controllare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Per ulteriori informazioni su Security Hub, consulta la [Guida AWS Security Hub per l'utente](#). Per ulteriori informazioni sull'utilizzo di Security Hub per valutare ed elaborare i risultati, vedere [Valutazione dei risultati con AWS Security Hub](#).

Oltre ai risultati, Macie crea risultati di rilevamento di dati sensibili per gli oggetti S3 che analizza per scoprire dati sensibili. Un risultato di rilevamento dei dati sensibili è un report che registra i dettagli relativi all'analisi di un oggetto. Ciò include oggetti in cui Macie non trova dati sensibili e che quindi non producono risultati, e oggetti che Macie non può analizzare a causa di errori o problemi. I risultati dell'individuazione di dati sensibili forniscono record di analisi che possono essere utili per controlli o indagini sulla privacy e sulla protezione dei dati. Non puoi accedere ai risultati del rilevamento di dati sensibili direttamente sulla console Amazon Macie o con l'API Amazon Macie. Invece, configuri Macie per archiviare i risultati in un bucket S3. Facoltativamente, puoi quindi accedere e interrogare i risultati in quel bucket. Per informazioni su come configurare Macie per archiviare i risultati, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

Argomenti

- [Tipi di scoperte di Macie](#)
- [Punteggio di gravità per i risultati di Macie](#)
- [Lavorare con i risultati di esempio di Macie](#)

- [Revisione delle scoperte di Macie utilizzando la console](#)
- [Filtrare i risultati di Macie](#)
- [Analisi dei dati sensibili con i risultati di Macie](#)
- [Sopprimere le scoperte di Macie](#)

Tipi di scoperte di Macie

Amazon Macie genera due categorie di risultati: risultati relativi alle politiche e dati sensibili. Un risultato della policy è un rapporto dettagliato di una potenziale violazione delle policy o di un problema relativo alla sicurezza o alla privacy di un bucket generico di Amazon Simple Storage Service (Amazon S3). Macie genera i risultati delle policy nell'ambito delle sue attività in corso volte a valutare e monitorare i tuoi bucket generici per la sicurezza e il controllo degli accessi. Un rilevamento di dati sensibili è un rapporto dettagliato dei dati sensibili rilevati da Macie in un oggetto S3. Macie genera rilevamenti di dati sensibili come parte delle attività che svolge quando si eseguono lavori di rilevamento di dati sensibili o esegue il rilevamento automatico di dati sensibili.

All'interno di ogni categoria, esistono tipi specifici. Il tipo di risultato fornisce informazioni sulla natura del problema o sui dati sensibili rilevati da Macie. I dettagli di un risultato forniscono un [indice di gravità](#), informazioni sulla risorsa interessata e informazioni aggiuntive, ad esempio quando e come Macie ha rilevato il problema o dati sensibili. La gravità e i dettagli di ciascun risultato variano a seconda del tipo e della natura del risultato.

Argomenti

- [Tipi di risultati politici](#)
- [Tipi di dati sensibili rilevati](#)

Tip

Per esplorare e conoscere le diverse categorie e tipi di risultati che Macie può generare, [crea dei risultati di esempio](#). I risultati di esempio utilizzano dati di esempio e valori segnaposto per dimostrare i tipi di informazioni che ogni tipo di risultato potrebbe contenere.

Tipi di risultati politici

Amazon Macie genera una ricerca sulle policy quando le policy o le impostazioni per un bucket S3 generico vengono modificate in modo da ridurre la sicurezza o la privacy del bucket e degli oggetti in esso contenuti. Per informazioni su come Macie rileva e valuta queste modifiche, consulta [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#)

Tieni presente che Macie genera una ricerca di policy solo se la modifica avviene dopo aver abilitato Macie for your. Account AWS Ad esempio, se le impostazioni di blocco dell'accesso pubblico sono disabilitate per un bucket S3 dopo aver abilitato Macie, Macie genera una ricerca Policy: IAMUser / S3 per il bucket. BlockPublicAccessDisabled Se le impostazioni di blocco dell'accesso pubblico sono state disabilitate per un bucket quando hai abilitato Macie e continuano a esserlo, Macie non genera una ricerca Policy: /S3 per il bucket. IAMUser BlockPublicAccessDisabled

Se Macie rileva una ricorrenza successiva di un risultato di policy esistente, Macie aggiorna il risultato esistente aggiungendo dettagli sull'occorrenza successiva e incrementando il numero di ricorrenze. Macie archivia i risultati delle politiche per 90 giorni.

Macie può generare i seguenti tipi di risultati delle policy per un bucket S3 generico.

Policy:IAMUser/S3BlockPublicAccessDisabled

Tutte le impostazioni di accesso pubblico a blocchi a livello di bucket sono state disabilitate per il bucket. L'accesso pubblico al bucket è controllato dalle impostazioni di accesso pubblico a blocchi per l'account, dalle liste di controllo degli accessi (ACLs), dalla politica del bucket per il bucket e da altre impostazioni e politiche che si applicano al bucket.

Per approfondire la scoperta, inizia [esaminando i dettagli del bucket](#) in Macie. I dettagli includono un'analisi dettagliata delle impostazioni di accesso pubblico del bucket. Per informazioni dettagliate sulle impostazioni, consulta [Controllo degli accessi](#) e [Blocco dell'accesso pubblico allo storage Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

Policy:IAMUser/S3BucketEncryptionDisabled

Le impostazioni di crittografia predefinite per il bucket sono state ripristinate al comportamento di crittografia predefinito di Amazon S3, che consiste nel crittografare automaticamente i nuovi oggetti con una chiave gestita di Amazon S3.

A partire dal 5 gennaio 2023, Amazon S3 applica automaticamente la crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per gli oggetti che

vengono aggiunti ai bucket. Facoltativamente, puoi configurare le impostazioni di crittografia predefinite di un bucket per utilizzare invece la crittografia lato server con una chiave (SSE-KMS) o la crittografia lato server a doppio livello con una AWS KMS chiave (DSSE-KMS). AWS KMS Se Macie ha generato questo tipo di risultato prima del 5 gennaio 2023, il risultato indica che le impostazioni di crittografia predefinite sono state disabilitate per il bucket interessato. Ciò significa che le impostazioni del bucket non specificavano il comportamento di crittografia lato server predefinito per i nuovi oggetti. La possibilità di disabilitare le impostazioni di crittografia predefinite per un bucket non è più supportata da Amazon S3.

Per informazioni sulle impostazioni e le opzioni di crittografia predefinite per i bucket S3, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

Policy:IAMUser/S3BucketPublic

Una policy ACL o bucket per il bucket è stata modificata per consentire l'accesso a utenti anonimi o a tutte le identità autenticate (IAM). AWS Identity and Access Management

Per esaminare la scoperta, inizia [esaminando i dettagli del bucket](#) in Macie. I dettagli includono un'analisi dettagliata delle impostazioni di accesso pubblico del bucket. Per informazioni dettagliate sulle ACLs politiche dei bucket e sulle impostazioni di accesso per i bucket S3, consulta il [controllo degli accessi](#) nella Amazon Simple Storage Service User Guide.

Policy:IAMUser/S3BucketReplicatedExternally

La replica è stata abilitata e configurata per replicare gli oggetti dal bucket a un bucket per un utente esterno all'organizzazione (Account AWS non facente parte dell'organizzazione). Un'organizzazione è un insieme di account Macie gestiti centralmente come gruppo di account correlati tramite AWS Organizations o su invito di Macie.

In determinate condizioni, Macie potrebbe generare questo tipo di ricerca per un bucket che non è configurato per replicare oggetti in un bucket esterno. Account AWS [Ciò può verificarsi se il bucket di destinazione è stato creato in un altro Regione AWS ambiente nelle 24 ore precedenti, dopo che Macie ha recuperato i metadati del bucket e dell'oggetto da Amazon S3 come parte del ciclo di aggiornamento giornaliero.](#)

Per verificare il risultato, inizia aggiornando i dati dell'inventario in Macie. Quindi [rivedi i dettagli del bucket](#). I dettagli indicano se il bucket è configurato per replicare oggetti su altri bucket. Se il bucket è configurato per questa operazione, i dettagli includono l'ID account per ogni account che possiede un bucket di destinazione. Per informazioni dettagliate sulle impostazioni di replica per i bucket S3, consulta [Replicating objects nella](#) Amazon Simple Storage Service User Guide.

Una politica ACL o bucket per il bucket è stata modificata per consentire la condivisione del bucket con un utente esterno (Account AWS che non fa parte della) tua organizzazione. Un'organizzazione è un insieme di account Macie gestiti centralmente come gruppo di account correlati tramite AWS Organizations o su invito di Macie.

Per informazioni sulle ACLs policy relative ai bucket S3, consulta il [controllo degli accessi](#) nella Guida per l'utente di Amazon Simple Storage Service.

La policy del bucket è stata modificata per consentire la condivisione del bucket con un Amazon CloudFront Origin Access Identity (OAI), un CloudFront Origin Access Control (OAC) o sia un OAI che un CloudFront OAC. CloudFront Un CloudFront OAI o OAC consente agli utenti di accedere agli oggetti di un bucket tramite una o più distribuzioni specifiche. CloudFront

Per ulteriori informazioni CloudFront OAI OACs, consulta la sezione [Restrizione dell'accesso a un'origine Amazon S3](#) nella CloudFrontAmazon Developer Guide.

In alcuni casi, Macie genera una ricerca Policy: IAMUser /S3 anziché una BucketSharedExternally ricerca Policy: IAMUser BucketSharedWithCloudFront /S3 per un bucket. Questi casi sono:

- Il bucket è condiviso con un Account AWS utente esterno all'organizzazione, oltre a un CloudFront OAI o OAC.

- La policy del bucket specifica un ID utente canonico, anziché l'Amazon Resource Name (ARN), di un OAI. CloudFront

In questo modo si ottiene una maggiore severità della policy per il bucket.

Tipi di dati sensibili rilevati

Amazon Macie genera una rilevazione di dati sensibili quando rileva dati sensibili in un oggetto S3 che analizza per rilevare dati sensibili. Ciò include l'analisi che Macie esegue quando esegui un processo di rilevamento di dati sensibili o esegue il rilevamento automatico di dati sensibili.

Ad esempio, se crei ed esegui un processo di rilevamento di dati sensibili e Macie rileva i numeri di conto bancario in un oggetto S3, Macie genera un risultato SensitiveData un:S3Object/Financial per l'oggetto. Allo stesso modo, se Macie rileva i numeri di conto corrente bancario in un oggetto S3 che analizza durante un ciclo automatico di scoperta di dati sensibili, Macie genera un risultato un:S3Object/Financial per l'oggetto. SensitiveData

Se Macie rileva dati sensibili nello stesso oggetto S3 durante un'esecuzione di lavoro successiva o un ciclo di rilevamento automatico dei dati sensibili, Macie genera una nuova ricerca di dati sensibili per l'oggetto. A differenza dei risultati delle policy, tutti i risultati relativi ai dati sensibili vengono trattati come nuovi (unici). Macie archivia i dati sensibili rilevati per 90 giorni.

Macie può generare i seguenti tipi di rilevazioni di dati sensibili per un oggetto S3.

SensitiveData:S3Object/Credentials

L'oggetto contiene dati sensibili relativi alle credenziali, come chiavi di accesso AWS segrete o chiavi private.

SensitiveData:S3Object/CustomIdentifier

L'oggetto contiene testo che corrisponde ai criteri di rilevamento di uno o più identificatori di dati personalizzati. L'oggetto potrebbe contenere più di un tipo di dati sensibili.

SensitiveData:S3Object/Financial

L'oggetto contiene informazioni finanziarie riservate, come numeri di conti bancari o numeri di carte di credito.

SensitiveData:S3Object/Multiple

L'oggetto contiene più di una categoria di dati sensibili, ovvero qualsiasi combinazione di dati relativi a credenziali, informazioni finanziarie, informazioni personali o testo che corrisponda ai criteri di rilevamento di uno o più identificatori di dati personalizzati.

SensitiveData:S3Object/Personal

L'oggetto contiene informazioni personali sensibili: informazioni di identificazione personale (PII) come numeri di passaporto o numeri di identificazione della patente di guida, informazioni sanitarie personali (PHI) come numeri di assicurazione sanitaria o di identificazione medica o una combinazione di PII e PHI.

Per informazioni sui tipi di dati sensibili che Macie è in grado di rilevare utilizzando criteri e tecniche integrati, consulta. [Utilizzo di identificatori di dati gestiti](#) Per informazioni sui tipi di oggetti S3 che Macie può analizzare, vedi. [Classi e formati di archiviazione supportati](#)

Punteggio di gravità per i risultati di Macie

Quando Amazon Macie genera una policy o una ricerca di dati sensibili, assegna automaticamente una severità alla scoperta. La gravità di un risultato riflette le caratteristiche principali del risultato, il che può aiutarti a valutare e dare priorità al risultato. La gravità di un risultato non implica né indica in altro modo la criticità o l'importanza che una risorsa interessata potrebbe avere per l'organizzazione.

Per quanto riguarda le policy, la gravità si basa sulla natura di un potenziale problema di sicurezza o privacy di un bucket generico Amazon Simple Storage Service (Amazon S3). Per quanto riguarda i dati sensibili, la gravità si basa sulla natura e sul numero di occorrenze di dati sensibili rilevati da Macie in un oggetto S3.

In Macie, la gravità di un risultato è rappresentata in due modi.

Livello di severità

Si tratta di una rappresentazione qualitativa della gravità. I livelli di gravità variano da Low, per i meno gravi, a High, per i più gravi.

I livelli di gravità vengono visualizzati direttamente sulla console Amazon Macie. Sono disponibili anche nelle rappresentazioni JSON dei risultati sulla console Macie, dall'API Amazon Macie e nei risultati di rilevamento di dati sensibili correlati ai dati sensibili rilevati. I livelli di gravità sono inclusi

anche nella ricerca degli eventi che Macie pubblica su Amazon EventBridge e dei risultati su cui Macie pubblica. AWS Security Hub

Punteggio di gravità

Si tratta di una rappresentazione numerica della gravità. I punteggi di gravità vanno da 1 a 3 e corrispondono direttamente ai livelli di gravità:

Punteggio di gravità	Livello di gravità
1	Bassa
2	Media
3	Elevata

I punteggi di gravità non vengono visualizzati direttamente sulla console Amazon Macie. Tuttavia, sono disponibili nelle rappresentazioni JSON dei risultati sulla console Macie, dall'API Amazon Macie e nei risultati di rilevamento di dati sensibili correlati ai dati sensibili rilevati. I punteggi di gravità sono inclusi anche nella ricerca degli eventi che Macie pubblica su Amazon. EventBridge Non sono inclusi nei risultati pubblicati da Macie. AWS Security Hub

Gli argomenti di questa sezione indicano in che modo Macie determina la gravità dei risultati delle policy e dei dati sensibili.

Argomenti

- [Punteggio di severità per i risultati delle politiche](#)
- [Punteggio di gravità per le rilevazioni di dati sensibili](#)

Punteggio di severità per i risultati delle politiche

La gravità di un risultato relativo alle policy si basa sulla natura di un potenziale problema relativo alla sicurezza o alla privacy di un bucket S3 per uso generico. La tabella seguente elenca i livelli di gravità che Amazon Macie assegna a ciascun tipo di policy policy. Per una descrizione di ogni tipo, consulta.

[Tipi di risultati](#)

Tipo di risultato	Livello di gravità
Policy:IAMUser/S3BlockPublicAccessDisabled	Elevata
Policy:IAMUser/S3BucketEncryptionDisabled	Bassa
Policy:IAMUser/S3BucketPublic	Elevata
Policy:IAMUser/S3BucketReplicatedExternally	Elevata
Policy:IAMUser/S3BucketSharedExternally	Elevata
Policy:IAMUser/S3BucketSharedWithCloudFront	Media

La gravità di una constatazione politica non cambia in base al numero di ricorrenze della constatazione.

Punteggio di gravità per le rilevazioni di dati sensibili

La gravità di un rilevamento di dati sensibili si basa sulla natura e sul numero di occorrenze di dati sensibili rilevati da Amazon Macie in un oggetto S3. I seguenti argomenti indicano in che modo Macie determina la gravità di ogni tipo di rilevamento di dati sensibili:

- [SensitiveData:S3Object/Credentials](#)
- [SensitiveData:S3Object/CustomIdentifier](#)
- [SensitiveData:S3Object/Financial](#)
- [SensitiveData:S3Object/Personal](#)
- [SensitiveData:S3Object/Multiple](#)

Per informazioni dettagliate sui tipi di dati sensibili che Macie è in grado di rilevare e riportare nei risultati relativi ai dati sensibili, consulta [Utilizzo di identificatori di dati gestiti](#) e [Creazione di identificatori di dati personalizzati](#)

SensitiveData:S3Object/Credentials

A:La SensitiveData scoperta di S3Object/Credentials indica che Macie ha rilevato dati sensibili relativi a credenziali in un oggetto S3. Per questo tipo di ricerca, Macie determina la gravità in base al tipo e al numero di occorrenze dei dati delle credenziali rilevati da Macie nell'oggetto.

La tabella seguente indica i livelli di gravità che Macie assegna ai risultati che segnalano le occorrenze dei dati delle credenziali in un oggetto S3.

Tipo di dati sensibili	1 occorrenza	2—99 occorrenze	100 o più occorrenze
AWS chiave di accesso segreta	Elevata	Elevata	Elevata
chiave API di Google Cloud	Elevata	Elevata	Elevata
Intestazione HTTP Basic Authorization	Elevata	Elevata	Elevata
Token Web JSON (JWT)	Elevata	Elevata	Elevata
Chiave privata OpenSSH	Elevata	Elevata	Elevata
Chiave privata PGP	Elevata	Elevata	Elevata
Chiave privata Public-Key Cryptography Standard (PKCS)	Elevata	Elevata	Elevata
Chiave privata PuTTY	Elevata	Elevata	Elevata
Chiave API Stripe	Elevata	Elevata	Elevata

SensitiveData:S3Object/CustomIdentifier

A:S3Object/ SensitiveDatafinding CustomIdentifier indica che un oggetto S3 contiene testo che corrisponde ai criteri di rilevamento di uno o più identificatori di dati personalizzati. L'oggetto potrebbe contenere più di un tipo di dati sensibili.

Per impostazione predefinita, Macie assegna il livello di gravità Medio a questo tipo di ricerca. Se l'oggetto S3 interessato contiene almeno un'occorrenza di testo che corrisponde ai criteri di rilevamento di almeno un identificatore di dati personalizzato, Macie assegna automaticamente il livello di gravità Medio al risultato. La gravità del risultato non cambia in base al numero di occorrenze di testo che corrispondono ai criteri di un identificatore di dati personalizzato.

Tuttavia, la gravità di questo tipo di risultato può variare se sono state definite impostazioni di gravità personalizzate per un identificatore di dati personalizzato che ha prodotto il risultato. In tal caso, Macie determina la gravità nel modo seguente:

- Se l'oggetto S3 contiene testo che corrisponde ai criteri di rilevamento di un solo identificatore di dati personalizzato, Macie determina la gravità del risultato in base alle impostazioni di gravità per quell'identificatore.
- Se l'oggetto S3 contiene testo che corrisponde ai criteri di rilevamento di più di un identificatore di dati personalizzato, Macie determina la severità del risultato valutando le impostazioni di gravità per ogni identificatore di dati personalizzato, determinando quale di queste impostazioni produce la gravità più elevata e quindi assegnando tale severità massima al risultato.

Per rivedere le impostazioni di gravità per un identificatore di dati personalizzato, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Per rivedere le impostazioni sulla console, scegli Identificatori di dati personalizzati nel pannello di navigazione, quindi scegli il nome dell'identificatore di dati personalizzato. La sezione Severità mostra le impostazioni. Per recuperare le impostazioni a livello di codice, utilizzate l'[GetCustomDataIdentifier](#) operazione o, se utilizzate la AWS Command Line Interface, eseguite il comando. [get-custom-data-identifier](#) Per ulteriori informazioni sulle impostazioni, consulta. [Opzioni di configurazione per identificatori di dati personalizzati](#)

SensitiveData:S3Object/Financial

A:I SensitiveData risultati di S3Object/Financial indicano che Macie ha rilevato informazioni finanziarie sensibili in un oggetto S3. Per questo tipo di risultato, Macie determina la gravità in base al tipo e al numero di occorrenze delle informazioni finanziarie rilevate da Macie nell'oggetto.

La tabella seguente indica i livelli di gravità che Macie assegna ai risultati che segnalano le occorrenze di informazioni finanziarie in un oggetto S3.

Tipo di dati sensibili	1 occorrenza	2—99 occorrenze	100 o più occorrenze
Conto bancario numero 1	Elevata	Elevata	Elevata
Data di scadenza della carta di credito	Bassa	Media	Elevata
Dati sulla banda magnetica della carta di credito	Elevata	Elevata	Elevata
Carta di credito numero 2	Elevata	Elevata	Elevata
Codice di verifica della carta di credito	Media	Elevata	Elevata

1. I livelli di gravità sono gli stessi per qualsiasi tipo di numero di conto bancario: un Basic Bank Account Number (BBAN), un International Bank Account Number (IBAN) o un numero di conto bancario canadese o statunitense.
2. I livelli di gravità sono gli stessi per i numeri di carta di credito che sono o non sono in prossimità di una parola chiave.

Se un risultato riporta più tipi di informazioni finanziarie in un oggetto S3, Macie determina la gravità del risultato calcolando la gravità per ogni tipo di informazione finanziaria rilevata da Macie, determinando quale tipo produce la gravità più elevata e assegnando la massima severità al risultato. Ad esempio, se Macie rileva 10 date di scadenza delle carte di credito (livello di gravità medio) e 10 numeri di carta di credito (livello di gravità alto) in un oggetto, Macie assegna il livello di gravità Alto al risultato.

SensitiveData:S3Object/Personal

A:S3Object/Personal SensitiveDatafinding indica che Macie ha rilevato informazioni personali sensibili in un oggetto S3. Le informazioni possono essere informazioni sanitarie personali (PHI), informazioni di identificazione personale (PII) o una combinazione delle due. Per questo tipo di ritrovamento, Macie determina la gravità in base al tipo e al numero di ricorrenze delle informazioni personali rilevate da Macie nell'oggetto.

La tabella seguente indica i livelli di gravità che Macie assegna ai dati sensibili rilevati che segnalano le occorrenze di PHI in un oggetto S3.

Tipo di dati sensibili	1 occorrenza	2—99 occorrenze	100 o più occorrenze
Numero di registrazione della Drug Enforcement Agency (DEA)	Elevata	Elevata	Elevata
Numero di richiesta di assicurazione sanitaria (HICN)	Elevata	Elevata	Elevata
Numero di identificazione medica e assistenza sanitaria	Elevata	Elevata	Elevata
Codice HCPCS (Healthcare Common Procedure Coding System)	Elevata	Elevata	Elevata
Codice nazionale sulle droghe (NDC)	Elevata	Elevata	Elevata
Identificatore nazionale del fornitore (NPI)	Elevata	Elevata	Elevata

Tipo di dati sensibili	1 occorrenza	2—99 occorrenze	100 o più occorrenze
Identificatore univoco del dispositivo (UDI)	Bassa	Media	Elevata

La tabella seguente indica i livelli di gravità che Macie assegna alle rilevazioni di dati sensibili che segnalano le occorrenze di PII in un oggetto S3.

Tipo di dati sensibili	1 occorrenza	2—99 occorrenze	100 o più occorrenze
Data di nascita	Bassa	Media	Elevata
Numero identificativo della patente di guida	Bassa	Media	Elevata
Numero di lista elettorale	Elevata	Elevata	Elevata
Nome completo	Bassa	Media	Elevata
Coordinate GPS (Global Positioning System)	Bassa	Media	Media
Cookie HTTP	Bassa	Media	Elevata
Indirizzo postale	Bassa	Media	Elevata
Numeri di carta d'identità	Elevata	Elevata	Elevata
Numero di previdenza nazionale (NINO)	Elevata	Elevata	Elevata
Numero di passaporto	Media	Elevata	Elevata

Tipo di dati sensibili	1 occorrenza	2—99 occorrenze	100 o più occorrenze
Numero di residenza permanente (Green Card)	Elevata	Elevata	Elevata
Numero di telefono	Bassa	Media	Elevata
Numero della carta di trasporto pubblico	Media	Media	Elevata
Numero di previdenza sociale (SIN)	Elevata	Elevata	Elevata
Numero di previdenza sociale (SSN)	Elevata	Elevata	Elevata
Codice identificativo o numero di riferimento del contribuente*	Elevata	Elevata	Elevata
Numero di identificazione del veicolo (VIN)	Bassa	Bassa	Media

* Le eccezioni sono: i numeri CUIT per le organizzazioni in Argentina (ARGENTINA_ORGANIZATION_TAX_IDENTIFICATION_NUMBER), i numeri NIT per le organizzazioni in Colombia (COLOMBIA_ORGANIZATION_NIT_NUMBER) e i numeri RFC per le organizzazioni in Messico (MEXICO_ORGANIZATION_RFC_NUMBER). Per questi tipi, i livelli di gravità sono: Medio per 1-99 occorrenze e Alto per 100 o più occorrenze.

Se un risultato riporta più tipi di PHI, PII o sia PHI che PII in un oggetto, Macie determina la gravità del risultato calcolando la gravità per ogni tipo, determinando quale tipo produce la gravità più elevata e assegnando tale severità massima al risultato.

Ad esempio, se Macie rileva 10 nomi completi (livello di gravità medio) e 5 numeri di passaporto (livello di gravità alto) in un oggetto, Macie assegna il livello di gravità elevato al risultato.

Analogamente, se Macie rileva 10 nomi completi (livello di gravità medio) e 10 numeri identificativi dell'assicurazione sanitaria (livello di gravità elevato) in un oggetto, Macie assegna il livello di gravità Alto al risultato.

SensitiveData:S3Object/Multiple

A: Il SensitiveData risultato S3Object/Multiple indica che Macie ha rilevato più categorie di dati sensibili in un oggetto S3. I dati sensibili possono essere qualsiasi combinazione di dati relativi a credenziali, informazioni finanziarie, informazioni personali o testo che corrisponda ai criteri di rilevamento di uno o più identificatori di dati personalizzati.

Per questo tipo di rilevamento, Macie determina la gravità calcolando la gravità per ogni tipo di dati sensibili rilevati da Macie (come indicato negli argomenti precedenti), determinando quale tipo produce la gravità più elevata e assegnando tale gravità massima al risultato.

Ad esempio, se Macie rileva 10 nomi completi (livello di gravità medio) e 10 chiavi di accesso AWS segrete (livello di gravità alto) in un oggetto, Macie assegna il livello di gravità Alta al risultato.

Lavorare con i risultati di esempio di Macie

Per esplorare e conoscere i diversi [tipi di risultati](#) che Amazon Macie può generare, puoi creare risultati di esempio. I risultati di esempio utilizzano dati di esempio e valori segnaposto per dimostrare i tipi di informazioni che ogni tipo di risultato potrebbe contenere.

Ad esempio, la ricerca di BucketPublic esempio Policy: IAMUser /S3 contiene dettagli su un bucket fittizio di Amazon Simple Storage Service (Amazon S3). I dettagli della scoperta includono dati di esempio su un attore e un'azione che ha modificato l'elenco di controllo degli accessi (ACL) per il bucket e lo ha reso accessibile al pubblico. Allo stesso modo, il risultato di SensitiveData campione: S3Object/Multiple contiene dettagli su una cartella di lavoro fittizia di Microsoft Excel. I dettagli del risultato includono dati di esempio sui tipi e sulla posizione dei dati sensibili nella cartella di lavoro.

Oltre ad acquisire familiarità con le informazioni che potrebbero contenere diversi tipi di risultati, è possibile utilizzare risultati di esempio per testare l'integrazione con altre applicazioni, servizi e sistemi. A seconda delle [regole di soppressione](#) del tuo account, Macie può pubblicare esempi di risultati su Amazon EventBridge come eventi. I dati di esempio relativi a questi eventi possono aiutarti a sviluppare e testare soluzioni automatizzate per il monitoraggio e l'elaborazione dei risultati. EventBridge A seconda delle [impostazioni di pubblicazione del](#) tuo account, Macie può anche

pubblicare esempi di risultati su AWS Security Hub. Ciò significa che puoi anche utilizzare esempi di risultati per sviluppare e testare soluzioni per valutare i risultati di Macie con Security Hub. Per informazioni sulla pubblicazione dei risultati su questi servizi, consulta [Monitoraggio ed elaborazione dei risultati](#)

Argomenti

- [Creazione di risultati di esempio](#)
- [Revisione dei risultati di esempio](#)
- [Soppressione dei risultati dei campioni](#)

Creazione di risultati di esempio

Puoi creare risultati di esempio utilizzando la console Amazon Macie o l'API Amazon Macie. Se usi la console, Macie genera automaticamente un risultato di esempio per ogni tipo di risultato supportato da Macie. Se utilizzi l'API, puoi creare un campione per ogni tipo o solo per alcuni tipi da te specificati.

Console

Segui questi passaggi per creare risultati di esempio utilizzando la console Amazon Macie.

Per creare risultati di esempio

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione scegli Impostazioni.
3. In Risultati di esempio, scegli Genera risultati di esempio.

API

Per creare risultati di esempio in modo programmatico, utilizza il [CreateSampleFindings](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza facoltativamente il `findingTypes` parametro per specificare solo determinati tipi di risultati di esempio da creare. Per creare automaticamente campioni di tutti i tipi, non includere questo parametro nella richiesta.

Per creare risultati di esempio utilizzando AWS Command Line Interface (AWS CLI), esegui il [create-sample-findings](#) comando. Per creare automaticamente campioni di tutti i tipi di risultati, non

includete il `finding-types` parametro. Per creare campioni solo di determinati tipi di risultati, includete questo parametro e specificate i tipi di risultati di esempio da creare. Per esempio:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/Multiple" "Policy:IAMUser/S3BucketPublic"
```

SensitiveData:S3Object/Multiple Dov'è un tipo di risultato di dati sensibili da creare ed *Policy:IAMUser/S3BucketPublic* è un tipo di risultato politico da creare.

Se il comando viene eseguito correttamente, Macie restituisce una risposta vuota.

Se crei nuovamente risultati di esempio entro 90 giorni, Macie genera un nuovo risultato per ogni tipo di ricerca di dati sensibili che crei. Per quanto riguarda i risultati delle politiche, Macie aggiorna ogni campione esistente incrementando il numero di occorrenze e aggiornando i dettagli su quando si è verificata l'occorrenza successiva.

Revisione dei risultati di esempio

Per aiutarti a identificare i risultati del campione, Amazon Macie imposta il valore per il campo Sample di ogni risultato del campione su True. Inoltre, il nome del bucket S3 interessato è lo stesso per tutti i risultati del campione: `macie-sample-finding-bucket`. Se esamini i risultati di esempio utilizzando le pagine Findings sulla console Amazon Macie, Macie visualizza anche il prefisso `[SAMPLE]` nel campo Tipo di ricerca per ogni risultato di esempio.

Console

Segui questi passaggi per esaminare i risultati di esempio utilizzando la console Amazon Macie.

Per esaminare i risultati di esempio

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Nella pagina Risultati, esegui una delle seguenti operazioni:
 - Nella colonna Tipo di ricerca, individuate i risultati il cui tipo inizia con `[ESEMPIO]`, come mostrato nell'immagine seguente.

☐	Severity ▼	Finding type ▼	Resources affected
☐	High	[SAMPLE] Policy:IAMUser/S3BucketSharedExternally	macie-sample-finding-bucket
☐	High	[SAMPLE] SensitiveData:S3Object/Credentials	macie-sample-finding-bucket/cred
☐	High	[SAMPLE] SensitiveData:S3Object/Financial	macie-sample-finding-bucket/fin
☐	High	[SAMPLE] Policy:IAMUser/S3BucketPublic	macie-sample-finding-bucket
☐	High	[SAMPLE] Policy:IAMUser/S3BucketReplicatedExternally	macie-sample-finding-bucket
☐	High	[SAMPLE] SensitiveData:S3Object/CustomIdentifier	macie-sample-finding-bucket/emp
☐	High	[SAMPLE] Policy:IAMUser/S3BlockPublicAccessDisabled	macie-sample-finding-bucket
☐	High	[SAMPLE] SensitiveData:S3Object/Multiple	macie-sample-finding-bucket/sam
☐	Medium	[SAMPLE] Policy:IAMUser/S3BucketSharedWithCloudFront	macie-sample-finding-bucket
☐	Low	[SAMPLE] Policy:IAMUser/S3BucketEncryptionDisabled	macie-sample-finding-bucket
☐	Low	[SAMPLE] SensitiveData:S3Object/Personal	macie-sample-finding-bucket/pers

- Utilizzando la casella dei criteri di filtro sopra la tabella, filtrate la tabella per visualizzare solo i risultati di esempio. A tale scopo, posiziona il cursore nella casella. Nell'elenco dei campi che appare, scegli Esempio. Quindi scegli True, quindi scegli Applica.

4. Per esaminare i dettagli di un campione specifico, scegliete il risultato. Il pannello dei dettagli mostra le informazioni relative al risultato.

È inoltre possibile scaricare e salvare i dettagli di uno o più risultati di esempio come file JSON. A tale scopo, seleziona la casella di controllo relativa a ogni risultato di esempio che desideri scaricare e salvare. Quindi scegli Esporta (JSON) nel menu Azioni nella parte superiore della pagina Findings. Nella finestra che appare, scegli Scarica. Per descrizioni dettagliate dei campi JSON che un risultato può includere, consulta [Findings](#) in Amazon Macie API Reference.

API

Per esaminare i risultati dei campioni in modo programmatico, utilizza innanzitutto il [ListFindings](#) funzionamento dell'API Amazon Macie per recuperare l'identificatore univoco `findingId()` per ogni risultato di esempio che hai creato. Utilizza quindi l'[GetFindings](#) operazione per recuperare i dettagli di tali risultati.

Quando si invia la `ListFindings` richiesta, è possibile specificare criteri di filtro per includere solo risultati di esempio nei risultati. A tale scopo, aggiungi una condizione di filtro in cui il valore del

sample campo è true. Se utilizzi il AWS CLI, esegui il comando [list-findings](#) e usa il `finding-criteria` parametro per specificare la condizione del filtro. Per esempio:

```
C:\> aws macie2 list-findings --finding-criteria={"criteria":{"sample":{"eq":{"true":true}}}}
```

Se la richiesta ha esito positivo, Macie restituisce un array. `findingIds` L'array elenca l'identificatore univoco per ogni esempio trovato per il tuo account nell'elenco corrente. Regione AWS

[Per recuperare quindi i dettagli dei risultati del campione, specifica questi identificatori univoci in una `GetFindings` richiesta o, per il AWS CLI, quando esegui il comando `get-findings`.](#)

Soppressione dei risultati dei campioni

Come altri risultati, Amazon Macie archivia i risultati dei campioni per 90 giorni. Dopo aver esaminato e sperimentato gli esempi, puoi facoltativamente archivarli [creando una](#) regola di soppressione. In tal caso, i risultati degli esempi non vengono più visualizzati per impostazione predefinita sulla console e il loro stato diventa archiviato.

Per archiviare i risultati dei campioni utilizzando la console Amazon Macie, configura la regola per archiviare i risultati in cui il valore per il campo `Sample` è `True`. Per archiviare i risultati di esempio utilizzando l'API Amazon Macie, configura la regola per archiviare i risultati dove si trova il valore del `sample` campo. `true`

Revisione delle scoperte di Macie utilizzando la console

Amazon Macie monitora l' AWS ambiente e genera risultati relativi alle policy quando rileva potenziali violazioni delle policy o problemi con la sicurezza o la privacy dei bucket generici Amazon Simple Storage Service (Amazon S3). Macie genera risultati su dati sensibili quando rileva dati sensibili in oggetti S3. Macie archivia le tue policy e i risultati relativi ai dati sensibili per 90 giorni.

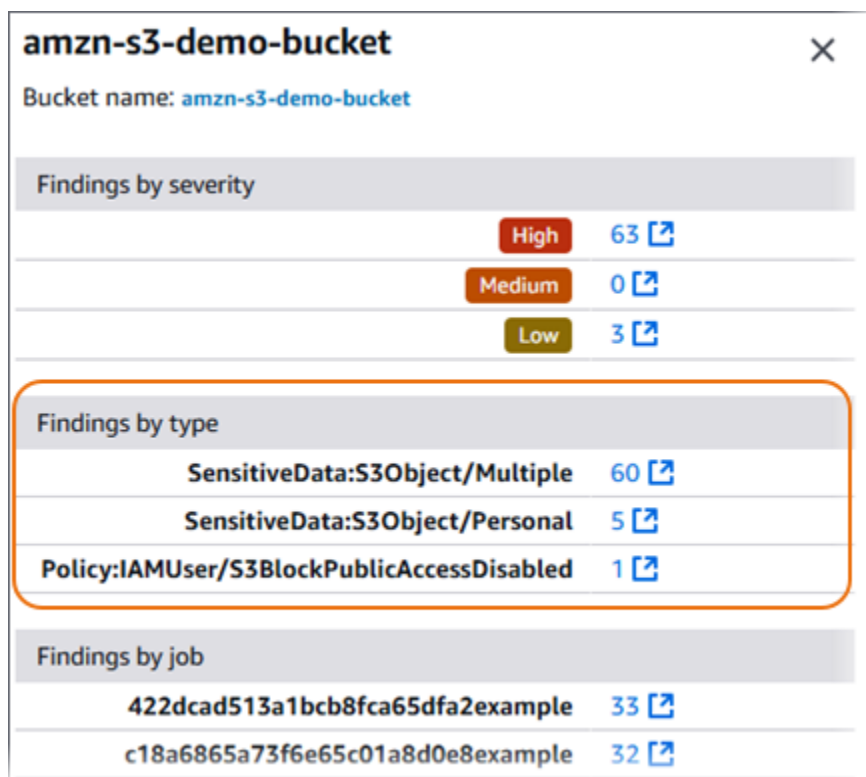
Ogni risultato specifica un [tipo di risultato](#) e un grado di [gravità](#). Ulteriori dettagli includono informazioni sulla risorsa interessata e su quando e come Macie ha riscontrato il problema o sui dati sensibili segnalati dal risultato. La gravità e i dettagli di ogni scoperta variano a seconda del tipo e della natura della scoperta.

Utilizzando la console Amazon Macie, puoi esaminare e analizzare i risultati e accedere ai dettagli dei singoli risultati. Puoi anche esportare uno o più risultati in un file JSON. Per semplificare l'analisi, la console offre diverse opzioni che possono aiutarti a creare visualizzazioni personalizzate dei risultati.

Usa raggruppamenti predefiniti

Utilizza pagine specifiche per esaminare i risultati raggruppati in base a criteri come il bucket S3 interessato, il tipo di ricerca o il processo di rilevamento di dati sensibili. Con queste pagine, puoi esaminare le statistiche aggregate per ogni gruppo, come il conteggio dei risultati per gravità. Puoi anche approfondire i dettagli dei singoli risultati di un gruppo e applicare filtri per affinare l'analisi.

Ad esempio, se raggruppi tutti i risultati per bucket S3 e noti che un determinato bucket presenta una violazione delle policy, puoi determinare rapidamente se sono presenti anche dati sensibili per il bucket. A tale scopo, scegli Per bucket nel riquadro di navigazione (sotto Findings), quindi scegli il bucket. Nel pannello dei dettagli che appare, la sezione Risultati per tipo elenca i tipi di risultati che si applicano al bucket, come mostrato nell'immagine seguente.

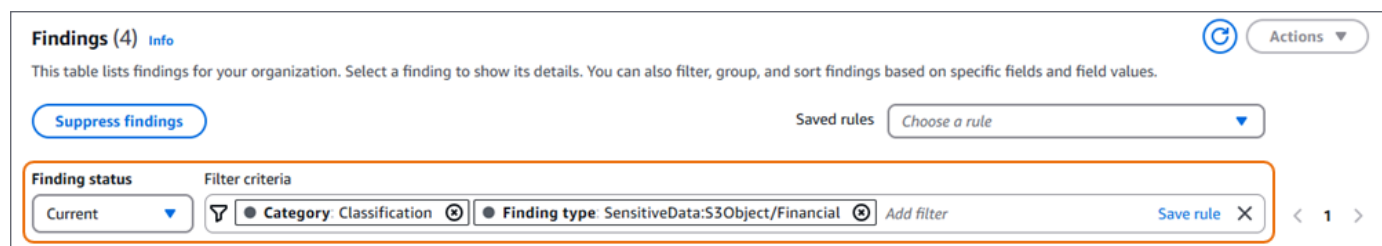


Per esaminare un tipo specifico, scegli il numero corrispondente. Macie visualizza una tabella di tutti i risultati che corrispondono al tipo selezionato e si applicano al bucket S3. Per rifinire i risultati, filtra la tabella.

Crea e applica filtri

Utilizza attributi di ricerca specifici per includere o escludere determinati risultati da una tabella Findings. Un attributo di ricerca è un campo che memorizza dati specifici per un risultato, come il tipo di risultato, la gravità o il nome del bucket S3 interessato. Se si filtra una tabella, è possibile identificare più facilmente i risultati con caratteristiche specifiche. Quindi puoi approfondire i dettagli di tali risultati.

Ad esempio, per esaminare tutti i risultati relativi ai dati sensibili, aggiungi criteri di filtro per il campo Categoria. Per rifinire i risultati e includere solo un tipo specifico di ricerca di dati sensibili, aggiungi criteri di filtro per il campo Tipo di ricerca. Per esempio:



Per rivedere quindi i dettagli di un particolare risultato, scegli il risultato. Il pannello dei dettagli mostra le informazioni relative al risultato.

È inoltre possibile ordinare i risultati in ordine crescente o decrescente in base a determinati campi. A tale scopo, scegli l'intestazione della colonna per il campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna.

Per esaminare i risultati utilizzando la console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti. La pagina Risultati mostra i risultati che Macie ha creato o aggiornato per il tuo account Regione AWS negli ultimi 90 giorni. Per impostazione predefinita, questo non include i risultati che sono stati soppressi da una regola di [soppressione](#).
3. Per analizzare e analizzare i risultati in base a un gruppo logico predefinito, scegli Per bucket, Per tipo o Per processo nel riquadro di navigazione (sotto Risultati). Quindi scegli un elemento nella tabella. Nel pannello dei dettagli, scegli il link relativo al campo su cui eseguire il pivot.
4. Per filtrare i risultati in base a criteri specifici, utilizza le opzioni di filtro sopra la tabella:
 - Per visualizzare i risultati che sono stati soppressi da una regola di soppressione, utilizzate il menu Finding status. Scegliete Tutto per visualizzare sia i risultati soppressi che quelli non

soppressi oppure scegliete Archiviato per visualizzare solo i risultati soppressi. Per nascondere nuovamente i risultati soppressi, scegliete Corrente.

- Per visualizzare solo i risultati che hanno un attributo specifico, utilizzate la casella Criteri di filtro. Posiziona il cursore nella casella e aggiungi una condizione di filtro per l'attributo. Per rifinire ulteriormente i risultati, aggiungi le condizioni per gli attributi aggiuntivi. Per rimuovere quindi una condizione, scegliete l'icona di rimozione della condizione



corrispondente alla condizione da rimuovere.

Per ulteriori informazioni sul filtraggio dei risultati, consulta [Creazione e applicazione di filtri ai risultati di Macie](#).

5. Per ordinare i risultati in base a un campo specifico, scegli l'intestazione di colonna del campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna.
6. Per esaminare i dettagli di un risultato specifico, scegli il risultato. Il pannello dei dettagli mostra le informazioni relative al risultato.

Suggerimenti

Nel pannello dei dettagli, puoi eseguire operazioni di pivot e approfondire determinati campi. Per mostrare i risultati che hanno lo stesso valore per un campo, scegli



nel campo. Scegli



di mostrare i risultati che hanno altri valori per il campo.

Per una ricerca di dati sensibili, puoi anche utilizzare il pannello dei dettagli per esaminare i dati sensibili che Macie ha trovato nell'oggetto S3 interessato:

- Per individuare le occorrenze di un tipo specifico di dati sensibili, scegli il link numerico nel campo relativo a quel tipo di dati. Macie visualizza informazioni (in formato JSON) su dove Macie ha trovato i dati. Per ulteriori informazioni, consulta [Individuazione di dati sensibili](#).
- Per recuperare esempi dei dati sensibili trovati da Macie, scegli Rivedi nel campo Reveal samples. Per ulteriori informazioni, consulta [Recupero di campioni di dati sensibili](#).

- Per passare al risultato della scoperta dei dati sensibili corrispondente, scegli il link nel campo Posizione dettagliata dei risultati. Macie apre la console Amazon S3 e visualizza il file o la cartella che contiene il risultato del rilevamento. Per ulteriori informazioni, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

7. Per scaricare e salvare i dettagli di uno o più risultati come file JSON, seleziona la casella di controllo relativa a ogni risultato da scaricare e salvare. Quindi scegli Esporta (JSON) nel menu Azioni. Nella finestra che appare, scegli Scarica. Per descrizioni dettagliate dei campi JSON che un risultato può includere, consulta [Findings](#) in Amazon Macie API Reference.

In alcuni casi, un risultato potrebbe non includere tutti i dettagli di un bucket S3 interessato. Ciò può verificarsi se si archiviano più di 10.000 bucket in Amazon S3. Macie conserva i dati di inventario completi per soli 10.000 bucket per account, i 10.000 bucket che sono stati creati o modificati più di recente. Per esaminare ulteriori dettagli relativi a un bucket interessato, puoi utilizzare i dati trovati per determinare il nome del bucket, l'ID dell'account del bucket Account AWS che possiede il bucket e di quello che memorizza il bucket. Regione AWS Puoi quindi utilizzare Amazon S3 per esaminare tutti i dettagli del bucket.

Filtrare i risultati di Macie

Per eseguire analisi mirate e analizzare i risultati in modo più efficiente, puoi filtrare i risultati di Amazon Macie. Con i filtri, puoi creare visualizzazioni e query personalizzate per i risultati, che possono aiutarti a identificare e concentrarti sui risultati con caratteristiche specifiche. Usa la console Amazon Macie per filtrare i risultati o inviare query in modo programmatico utilizzando l'API Amazon Macie.

Quando crei un filtro, utilizzi attributi specifici dei risultati per definire criteri per includere o escludere i risultati da una vista o dai risultati delle query. Un attributo di ricerca è un campo che memorizza dati specifici per un risultato, come la gravità, il tipo o il nome del bucket S3 a cui si applica un risultato.

In Macie, un filtro è costituito da una o più condizioni. Ogni condizione, nota anche come criterio, è composta da tre parti:

- Un campo basato su attributi, come Severity o Finding type.
- Un operatore, ad esempio uguale o non uguale.
- Uno o più valori. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti.

Se crei un filtro che desideri riutilizzare, puoi salvarlo come regola di filtro. Una regola di filtro è un insieme di criteri di filtro che crei e salvi per riapplicare quando esamini i risultati sulla console Amazon Macie.

Puoi anche salvare un filtro come regola di soppressione. Una regola di soppressione è un insieme di criteri di filtro creati e salvati per archiviare automaticamente i risultati che corrispondono ai criteri della regola. Per ulteriori informazioni sulle regole di soppressione, vedere. [Eliminazione dei risultati](#)

Argomenti

- [Nozioni di base sul filtraggio dei risultati di Macie](#)
- [Campi per filtrare i risultati di Macie](#)
- [Creazione e applicazione di filtri ai risultati di Macie](#)
- [Definizione delle regole di filtro per i risultati di Macie](#)

Nozioni di base sul filtraggio dei risultati di Macie

Quando filtri i risultati, tieni a mente le seguenti funzionalità e linee guida. Tieni inoltre presente che i risultati filtrati sono limitati ai 90 giorni precedenti e a quelli attuali. Regione AWS Amazon Macie archivia i risultati per soli 90 giorni ciascuno. Regione AWS

Argomenti

- [Utilizzo di più condizioni in un filtro](#)
- [Specificare i valori per i campi](#)
- [Specificare più valori per un campo](#)
- [Utilizzo degli operatori in condizioni](#)

Utilizzo di più condizioni in un filtro

Un filtro può includere una o più condizioni. Ogni condizione, nota anche come criterio, è composta da tre parti:

- Un campo basato su attributi, come Severity o Finding type. Per un elenco dei campi che è possibile utilizzare, vedere. [Campi per filtrare i risultati di Macie](#)
- Un operatore, ad esempio uguale o non uguale. Per un elenco degli operatori che è possibile utilizzare, vedere. [Utilizzo degli operatori in condizioni](#)
- Uno o più valori. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti.

Se un filtro contiene più condizioni, Amazon Macie utilizza la logica AND per unire le condizioni e valutare i criteri di filtro. Ciò significa che un risultato corrisponde ai criteri del filtro solo se corrisponde a tutte le condizioni del filtro.

Ad esempio, se aggiungi una condizione per includere solo i risultati con elevata gravità e aggiungi un'altra condizione per includere solo i risultati relativi ai dati sensibili, Macie restituisce tutti i risultati relativi ai dati sensibili ad alta gravità. In altre parole, Macie esclude tutti i risultati delle politiche e tutti i risultati relativi ai dati sensibili di media e bassa gravità.

È possibile utilizzare un campo solo una volta in un filtro. Tuttavia, è possibile specificare più valori per molti campi.

Ad esempio, se una condizione utilizza il campo Severità per includere solo risultati di gravità elevata, non è possibile utilizzare il campo Severità in un'altra condizione per includere risultati di gravità media o bassa. Specificate invece più valori per la condizione esistente o utilizzate un operatore diverso per la condizione esistente. Ad esempio, per includere tutti i risultati di gravità media e alta, aggiungi una condizione di gravità uguale a media, alta o aggiungi una condizione di gravità non uguale a bassa.

Specificare i valori per i campi

Quando si specifica un valore per un campo, il valore deve essere conforme al tipo di dati sottostante del campo. A seconda del campo, è possibile specificare uno dei seguenti tipi di valori.

Matrice di testo (stringhe)

Specifica un elenco di valori di testo (stringa) per un campo. Ogni stringa è correlata a un valore predefinito o esistente per un campo, ad esempio High per il campo Severity, S3Object/Financial per il campo Finding type o il nome di un bucket S3 SensitiveData per il campo del nome del bucket S3.

Se usi un array, tieni presente quanto segue:

- I valori sono sensibili alle maiuscole.
- Non è possibile specificare valori parziali o utilizzare caratteri jolly nei valori. È necessario specificare un valore completo e valido per il campo.

Ad esempio, per filtrare i risultati per un bucket S3 denominato my-S3-bucket, immettilo **my-S3-bucket** come valore per il campo del nome del bucket S3. Se inserisci qualsiasi altro valore, ad esempio **my-s3-bucket** o, Macie non restituirà i risultati per il **my-S3** bucket.

Per un elenco di valori validi per ogni campo, vedi. [Campi per filtrare i risultati di Macie](#)

È possibile specificare fino a 50 valori in un array. Il modo in cui si specificano i valori dipende dal fatto che si utilizzi la console Amazon Macie o l'API Amazon Macie, come descritto in. [Specificare più valori per un campo](#)

Booleano

Specifica uno dei due valori che si escludono a vicenda per un campo.

Se utilizzi la console Amazon Macie per specificare questo tipo di valore, la console fornisce un elenco di valori tra cui scegliere. Se utilizzi l'API Amazon Macie, specifica `true` o `false` per il valore.

Data/ora (e intervalli di tempo)

Specifica una data e un'ora assolute per un campo. Se si specifica questo tipo di valore, è necessario specificare sia una data che un'ora.

Sulla console Amazon Macie, i valori di data e ora si riferiscono al fuso orario locale e utilizzano la notazione a 24 ore. In tutti gli altri contesti, questi valori sono in formato UTC (Coordinated Universal Time) e ISO 8601 esteso, ad `2020-09-01T14:31:13Z` esempio alle 14:31:13 UTC del 1° settembre 2020.

Se un campo memorizza un valore di data/ora, è possibile utilizzare il campo per definire un intervallo di tempo fisso o relativo. Ad esempio, puoi includere solo i risultati che sono stati creati tra due date e ore specifiche o solo i risultati che sono stati creati prima o dopo una data e un'ora specifiche. Il modo in cui definisci un intervallo di tempo dipende dal fatto che utilizzi la console Amazon Macie o l'API Amazon Macie:

- Sulla console, usa un selettore di date o inserisci il testo direttamente nelle caselle Da e To.
- Con l'API, definisci un intervallo di tempo fisso aggiungendo una condizione che specifichi la prima data e ora dell'intervallo e aggiungi un'altra condizione che specifichi l'ultima data e ora dell'intervallo. Se esegui questa operazione, Macie utilizza la logica AND per unire le condizioni. Per definire un intervallo di tempo relativo, aggiungi una condizione che specifichi la prima o l'ultima data e ora dell'intervallo. Specificate i valori come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. `1604616572653`

Sulla console, gli intervalli di tempo sono inclusi. Con l'API, gli intervalli di tempo possono essere inclusivi o esclusivi, a seconda dell'operatore scelto.

Numero (e intervalli numerici)

Specifica un numero intero lungo per un campo.

Se un campo memorizza un valore numerico, è possibile utilizzare il campo per definire un intervallo numerico fisso o relativo. Ad esempio, puoi includere solo i risultati che riportano 50-90 occorrenze di dati sensibili in un oggetto S3. Il modo in cui definisci un intervallo numerico dipende dal fatto che utilizzi la console Amazon Macie o l'API Amazon Macie:

- Sulla console, usa le caselle Da e A per inserire rispettivamente i numeri più bassi e più alti dell'intervallo.
- Con l'API, definisci un intervallo numerico fisso aggiungendo una condizione che specifichi il numero più basso dell'intervallo e aggiungi un'altra condizione che specifichi il numero più alto dell'intervallo. Se esegui questa operazione, Macie utilizza la logica AND per unire le condizioni. Per definire un intervallo numerico relativo, aggiungi una condizione che specifichi il numero più basso o più alto dell'intervallo.

Sulla console, gli intervalli numerici sono inclusi. Con l'API, gli intervalli numerici possono essere inclusivi o esclusivi, a seconda dell'operatore scelto.

Testo (stringa)

Specificate un singolo valore di testo (stringa) per un campo. La stringa è correlata a un valore predefinito o esistente per un campo, ad esempio, High per il campo Severity, il nome di un bucket S3 per il campo S3 bucket name o l'identificatore univoco per un processo di rilevamento di dati sensibili per il campo Job ID.

Se specificate una singola stringa di testo, tenete presente quanto segue:

- I valori sono sensibili alle maiuscole.
- Non è possibile utilizzare valori parziali o caratteri jolly nei valori. È necessario specificare un valore completo e valido per il campo.

Ad esempio, per filtrare i risultati per un bucket S3 denominato my-S3-bucket, immettilo **my-S3-bucket** come valore per il campo del nome del bucket S3. Se inserisci qualsiasi altro valore, ad esempio **my-s3-bucket** o, Macie non restituirà i risultati per il **my-S3** bucket.

Per un elenco di valori validi per ogni campo, vedi. [Campi per filtrare i risultati di Macie](#)

Specificare più valori per un campo

Con determinati campi e operatori, è possibile specificare più valori per un campo. In tal caso, Amazon Macie utilizza la logica OR per unire i valori e valutare i criteri di filtro. Ciò significa che una ricerca corrisponde ai criteri se contiene uno dei valori del campo.

Ad esempio, se aggiungi una condizione per includere risultati in cui il valore del campo Tipo di ricerca è uguale a: S3 SensitiveData, Object/Financial, SensitiveData:S3Object/Personal Macie restituisce risultati di dati sensibili per gli oggetti S3 che contengono solo informazioni finanziarie e gli oggetti S3 che contengono solo informazioni personali. In altre parole, Macie esclude tutti i risultati delle politiche. Macie esclude anche tutti i dati sensibili rilevati per oggetti che contengono altri tipi di dati sensibili o più tipi di dati sensibili.

L'eccezione è rappresentata dalle condizioni che utilizzano il eqExactMatchoperatore. Per questo operatore, Macie utilizza la logica AND per unire i valori e valutare i criteri di filtro. Ciò significa che una ricerca soddisfa i criteri solo se contiene tutti i valori del campo e solo quei valori per il campo. Per ulteriori informazioni su questo operatore, consulta [Utilizzo degli operatori in condizioni](#).

Il modo in cui si specificano più valori per un campo dipende dal fatto che si utilizzi l'API Amazon Macie o la console Amazon Macie. Con l'API, usi un array che elenca i valori.

Sulla console, in genere si scelgono i valori da un elenco. Tuttavia, per alcuni campi, è necessario aggiungere una condizione distinta per ogni valore. Ad esempio, per includere i risultati relativi ai dati rilevati da Macie utilizzando determinati identificatori di dati personalizzati, procedi come segue:

1. Posiziona il cursore nella casella Criteri di filtro, quindi seleziona il campo Nome identificatore di dati personalizzato. Inserisci il nome di un identificatore di dati personalizzato, quindi scegli Applica.
2. Ripeti il passaggio precedente per ogni identificatore di dati personalizzato aggiuntivo che desideri specificare per il filtro.

Per un elenco dei campi per i quali è necessario eseguire questa operazione, consulta. [Campi per filtrare i risultati di Macie](#)

Utilizzo degli operatori in condizioni

È possibile utilizzare i seguenti tipi di operatori in condizioni individuali.

È uguale a (eq)

Corrisponde a (=) qualsiasi valore specificato per il campo. È possibile utilizzare l'operatore equals con i seguenti tipi di valori: matrice di testo (stringhe), booleano, data/ora, numero e testo (stringa).

Per molti campi, è possibile utilizzare questo operatore e specificare fino a 50 valori per il campo. In tal caso, Amazon Macie utilizza la logica OR per unire i valori. Ciò significa che un risultato corrisponde ai criteri se presenta uno dei valori specificati per il campo.

Per esempio:

- Per includere risultati che segnalano l'occorrenza di informazioni finanziarie, informazioni personali o informazioni sia finanziarie che personali, aggiungi una condizione che utilizzi il campo Categoria di dati sensibili e questo operatore e specifica Informazioni finanziarie e Informazioni personali come valori per il campo.
- Per includere i risultati che riportano le occorrenze dei numeri di carta di credito, degli indirizzi postali o sia dei numeri di carta di credito che degli indirizzi postali, aggiungi una condizione per il campo Tipo di rilevamento dei dati sensibili, utilizza questo operatore e specifica CREDIT_CARD_NUMBER e ADDRESS come valori per il campo.

Se utilizzi l'API Amazon Macie per definire una condizione che utilizza questo operatore con un valore di data/ora, specifica il valore come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. 1604616572653

È uguale alla corrispondenza esatta (eqExactMatch)

Corrisponde esclusivamente a tutti i valori specificati per il campo. È possibile utilizzare l'operatore equals exact match con un set selezionato di campi.

Se si utilizza questo operatore e si specificano più valori per un campo, Macie utilizza la logica AND per unire i valori. Ciò significa che un risultato soddisfa i criteri solo se contiene tutti i valori specificati per il campo e solo quei valori per il campo. È possibile specificare fino a 50 valori per il campo.

Per esempio:

- Per includere risultati che riportano le occorrenze dei numeri di carta di credito e nessun altro tipo di dati sensibili, aggiungi una condizione per il campo Tipo di rilevamento dei dati sensibili, utilizza questo operatore e specifica CREDIT_CARD_NUMBER come unico valore per il campo.
- Per includere risultati che riportino la presenza sia dei numeri di carta di credito che degli indirizzi postali (e nessun altro tipo di dati sensibili), aggiungi una condizione per il campo Tipo

di rilevamento dei dati sensibili, utilizza questo operatore e specifica `CREDIT_CARD_NUMBER` e `ADDRESS` come valori per il campo.

Poiché Macie utilizza la logica AND per unire i valori di un campo, non è possibile utilizzare questo operatore in combinazione con altri operatori per lo stesso campo. In altre parole, se si utilizza l'operatore di corrispondenza esatta con un campo in una condizione, è necessario utilizzarlo in tutte le altre condizioni che utilizzano lo stesso campo.

Come altri operatori, è possibile utilizzare l'operatore di corrispondenza esatta in più di una condizione in un filtro. Se si esegue questa operazione, Macie utilizza la logica AND per unire le condizioni e valutare il filtro. Ciò significa che un risultato corrisponde ai criteri del filtro solo se ha tutti i valori specificati da tutte le condizioni del filtro.

Ad esempio, per includere i risultati creati dopo un certo periodo di tempo, segnalare le occorrenze dei numeri di carta di credito e non segnalare nessun altro tipo di dati sensibili, procedi come segue:

1. Aggiungi una condizione che utilizzi il campo `Creato in`, utilizzi l'operatore maggiore di e specifichi la data e l'ora di inizio del filtro.
2. Aggiungi un'altra condizione che utilizza il campo `Tipo di rilevamento dei dati sensibili`, utilizza l'operatore `equals exact match` e specifica `CREDIT_CARD_NUMBER` come unico valore per il campo.

È possibile utilizzare l'operatore `equals exact match` con i seguenti campi:

- ID identificatore di dati personalizzato () `customDataIdentifiers.detections.arn`
- Nome dell'identificatore di dati personalizzato () `customDataIdentifiers.detections.name`
- Chiave bucket tag S3 () `resourcesAffected.s3Bucket.tags.key`
- valore del tag bucket S3 () `resourcesAffected.s3Bucket.tags.value`
- Chiave del tag dell'oggetto S3 () `resourcesAffected.s3Object.tags.key`
- valore del tag dell'oggetto S3 () `resourcesAffected.s3Object.tags.value`
- Tipo di rilevamento dei dati sensibili () `sensitiveData.detections.type`
- Categoria di dati sensibili (`sensitiveData.category`)

Nell'elenco precedente, il nome tra parentesi utilizza la notazione a punti per indicare il nome del campo nelle rappresentazioni JSON dei risultati e nell'API Amazon Macie.

Maggiore di (gt)

È maggiore di ($>$) il valore specificato per il campo. È possibile utilizzare l'operatore maggiore di con valori numerici e di data/ora.

Ad esempio, per includere solo i risultati che riportano più di 90 occorrenze di dati sensibili in un oggetto S3, aggiungi una condizione che utilizzi il campo Conteggio totale dei dati sensibili e questo operatore e specifica 90 come valore per il campo. Per eseguire questa operazione sulla console Amazon Macie, inserisci **91** nella casella Da, non inserire un valore nella casella A, quindi scegli Applica. I confronti numerici e basati sul tempo sono inclusi nella console.

Se utilizzi l'API Amazon Macie per definire un intervallo di tempo che utilizza questo operatore, devi specificare i valori di data/ora come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. 1604616572653

Maggiore o uguale a (gte)

È maggiore o uguale a ($> =$) il valore specificato per il campo. È possibile utilizzare l'operatore maggiore o uguale a con valori numerici e di data/ora.

Ad esempio, per includere solo i risultati che segnalano 90 o più occorrenze di dati sensibili in un oggetto S3, aggiungi una condizione che utilizzi il campo Conteggio totale dei dati sensibili e questo operatore e specifica 90 come valore per il campo. Per eseguire questa operazione sulla console Amazon Macie, inserisci **90** nella casella Da, non inserire un valore nella casella A, quindi scegli Applica.

Se utilizzi l'API Amazon Macie per definire un intervallo di tempo che utilizza questo operatore, devi specificare i valori di data/ora come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. 1604616572653

Meno di (lt)

È inferiore a ($<$) il valore specificato per il campo. È possibile utilizzare l'operatore less than con valori numerici e di data/ora.

Ad esempio, per includere solo i risultati che riportano meno di 90 occorrenze di dati sensibili in un oggetto S3, aggiungi una condizione che utilizzi il campo Conteggio totale dei dati sensibili e questo operatore e specifica 90 come valore per il campo. Per eseguire questa operazione sulla console Amazon Macie, inserisci **89** nella casella A, non inserire un valore nella casella Da, quindi scegli Applica. I confronti numerici e basati sul tempo sono inclusi nella console.

Se utilizzi l'API Amazon Macie per definire un intervallo di tempo che utilizza questo operatore, devi specificare i valori di data/ora come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. 1604616572653

Minore o uguale a (lte)

È minore o uguale a ($\leq$) il valore specificato per il campo. È possibile utilizzare l'operatore minore o uguale a con valori numerici e di data/ora.

Ad esempio, per includere solo i risultati che riportano 90 o meno occorrenze di dati sensibili in un oggetto S3, aggiungi una condizione che utilizzi il campo Conteggio totale dei dati sensibili e questo operatore e specifica 90 come valore per il campo. Per eseguire questa operazione sulla console Amazon Macie, inserisci **90** nella casella A, non inserire un valore nella casella Da, quindi scegli Applica.

Se utilizzi l'API Amazon Macie per definire un intervallo di tempo che utilizza questo operatore, devi specificare i valori di data/ora come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. 1604616572653

Non è uguale a (neq)

Non corrisponde ($\neq$) a nessun valore specificato per il campo. È possibile utilizzare l'operatore not equals con i seguenti tipi di valori: array di testo (stringhe), booleano, data/ora, numero e testo (stringa).

Per molti campi, è possibile utilizzare questo operatore e specificare fino a 50 valori per il campo. Se lo fai, Macie usa la logica OR per unire i valori. Ciò significa che un risultato corrisponde ai criteri se non ha nessuno dei valori specificati per il campo.

Per esempio:

- Per escludere i risultati che segnalano la presenza di informazioni finanziarie, informazioni personali o informazioni sia finanziarie che personali, aggiungi una condizione che utilizzi il campo Categoria di dati sensibili e questo operatore e specifica Informazioni finanziarie e Informazioni personali come valori per il campo.
- Per escludere i risultati che riportano le occorrenze di numeri di carta di credito, aggiungi una condizione per il campo Tipo di rilevamento dei dati sensibili, utilizza questo operatore e specifica CREDIT_CARD_NUMBER come valore per il campo.
- Per escludere i risultati che segnalano l'occorrenza di numeri di carta di credito, indirizzi postali o sia numeri di carta di credito che indirizzi postali, aggiungi una condizione per il campo Tipo di

rilevamento dei dati sensibili, utilizza questo operatore e specifica CREDIT_CARD_NUMBER e ADDRESS come valori per il campo.

Se utilizzi l'API Amazon Macie per definire una condizione che utilizza questo operatore con un valore di data/ora, specifica il valore come timestamp Unix in millisecondi, ad esempio per le 22:49:32 UTC del 5 novembre 2020. 1604616572653

Campi per filtrare i risultati di Macie

Per aiutarti ad analizzare i risultati in modo più efficiente, la console Amazon Macie e l'API Amazon Macie forniscono l'accesso a diversi set di campi per filtrare i risultati:

- **Campi comuni:** questi campi memorizzano dati che si applicano a qualsiasi tipo di risultato. Sono correlati agli attributi comuni dei risultati, come la gravità, il tipo di risultato e l'ID del risultato.
- **Campi di risorse interessati:** questi campi memorizzano i dati sulle risorse a cui si applica un risultato, come il nome, i tag e le impostazioni di crittografia per un bucket o oggetto S3 interessato.
- **Campi per i risultati delle politiche:** questi campi memorizzano i dati specifici dei risultati delle politiche, come l'azione che ha prodotto un risultato e l'entità che ha eseguito l'azione.
- **Campi per l'individuazione di dati sensibili:** questi campi memorizzano dati specifici relativi ai dati sensibili, come la categoria e i tipi di dati sensibili che Macie ha trovato in un oggetto S3 interessato.

Un filtro può utilizzare una combinazione di campi di uno qualsiasi dei set precedenti. Gli argomenti di questa sezione elencano e descrivono i singoli campi di ogni set. Per ulteriori dettagli su questi campi, incluse eventuali relazioni tra i campi, consulta [Findings](#) in the Amazon Macie API Reference.

Argomenti

- [Campi comuni](#)
- [Campi di risorse interessati](#)
- [Campi per i risultati delle politiche](#)
- [Campi per il rilevamento di dati sensibili](#)

Campi comuni

La tabella seguente elenca e descrive i campi che puoi utilizzare per filtrare i risultati in base agli attributi di ricerca comuni. Questi campi memorizzano dati che si applicano a qualsiasi tipo di ricerca.

Nella tabella, la colonna Campo indica il nome del campo sulla console Amazon Macie. La colonna del campo JSON utilizza la notazione a punti per indicare il nome del campo nelle rappresentazioni JSON dei risultati e nell'API Amazon Macie. La colonna Descrizione fornisce una breve descrizione dei dati archiviati nel campo e indica eventuali requisiti per i valori del filtro. La tabella viene ordinata in ordine alfabetico crescente per campo e quindi per campo JSON.

Campo	Campo JSON	Descrizione
ID dell'account*	accountId	L'identificatore univoco a Account AWS cui si riferisce il risultato. Si tratta in genere dell'account proprietario della risorsa interessata.
—	archived	Un valore booleano che specifica se il risultato è stato soppresso (archiviato automaticamente) da una regola di soppressione. Per utilizzare questo campo in un filtro sulla console, scegliete un'opzione nel menu di stato della ricerca: Archiviato (solo soppresso), Corrente (solo non soppresso) o Tutto (sia soppresso che non soppresso).
Categoria	category	La categoria del risultato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Nell'API, i valori validi sono: CLASSIFICATION , per la ricerca di dati

Campo	Campo JSON	Descrizione
		sensibili e, POLICY, per una ricerca di policy.
—	count	Il numero totale di occorrenze del risultato. Per i rilevamenti di dati sensibili, questo valore è sempre 1. Tutti i dati sensibili rilevati sono considerati unici. Questo campo non è disponibile come opzione di filtro sulla console. Con l'API, puoi utilizzare questo campo per definire un intervallo numerico per un filtro.
Creato in	createdAt	La data e l'ora in cui Macie ha creato il ritrovamento. È possibile utilizzare questo campo per definire un intervallo di tempo per un filtro.
ID di trovazione*	id	L'identificatore univoco del risultato. Si tratta di una stringa casuale che Macie genera e assegna a un risultato al momento della creazione del risultato.

Campo	Campo JSON	Descrizione
Tipo di trovamento*	type	Il tipo di risultato, ad esempio, o. SensitiveData:S3Object/PersonalPolicy:IAMUser/S3BucketPublic La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi nell'API, consulta FindingType Amazon Macie API Reference.
Regione	region	Il risultato Regione AWS in cui Macie ha creato il risultato, ad esempio o. us-east-1 central-1
Project N.E.M.O.	sample	Un valore booleano che specifica se il risultato è un risultato di esempio. Un risultato di esempio è un risultato che utilizza dati di esempio e valori segnaposto per dimostrare cosa potrebbe contenere un risultato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro.

Campo	Campo JSON	Descrizione
Gravità	severity.description	La rappresentazione qualitativa della gravità del risultato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Nell'API, i valori validi sono: LowMedium, eHigh.
Ora aggiornamento	updatedAt	La data e l'ora dell'ultimo aggiornamento del risultato . Per quanto riguarda i dati sensibili, questo valore è uguale al valore del campo Creato in. Tutti i dati sensibili rilevati sono considerati nuovi (unici). È possibile utilizzare questo campo per definire un intervallo di tempo per un filtro.

* Per specificare più valori per questo campo sulla console, aggiungi una condizione che utilizzi il campo e specifichi un valore distinto per il filtro, quindi ripeti il passaggio per ogni valore aggiuntivo. Per eseguire questa operazione con l'API, utilizza un array che elenchi i valori da utilizzare per il filtro.

Campi di risorse interessati

Le tabelle seguenti elencano e descrivono i campi che è possibile utilizzare per filtrare i risultati in base al tipo di risorsa a cui si applica un risultato: un [bucket S3](#) o un oggetto [S3](#).

Bucket S3

Questa tabella elenca e descrive i campi che è possibile utilizzare per filtrare i risultati in base alle caratteristiche del bucket S3 a cui si applica un risultato.

Nella tabella, la colonna Campo indica il nome del campo sulla console Amazon Macie. La colonna del campo JSON utilizza la notazione a punti per indicare il nome del campo nelle rappresentazioni JSON dei risultati e nell'API Amazon Macie. (I nomi di campo JSON più lunghi utilizzano la sequenza di caratteri di nuova riga () per migliorare la leggibilità.) \n La colonna Descrizione fornisce una breve descrizione dei dati archiviati nel campo e indica eventuali requisiti per i valori del filtro. La tabella viene ordinata in ordine alfabetico crescente per campo e quindi per campo JSON.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3Bucket.createdAt</code>	La data e l'ora in cui è stato creato il bucket interessato o le ultime modifiche, come le modifiche alla politica del bucket, sono state apportate al bucket interessato. Questo campo non è disponibile come opzione di filtro sulla console. Con l'API, puoi utilizzare questo campo per definire un intervallo di tempo per un filtro.
Crittografia predefinita del bucket S3	<code>resourcesAffected.s3Bucket.\n defaultServerSideEncryption.encryptionType</code>	L'algoritmo di crittografia lato server utilizzato di default per crittografare gli oggetti aggiunti al bucket interessato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi per l'API, consulta Encryptio nType Amazon Macie API Reference.

Campo	Campo JSON	Descrizione
ID chiave KMS di crittografia con bucket S3*	<code>resourcesAffected.s3Bucket.\n</code> <code>defaultServerSideEncryption.kmsMasterKeyId</code>	L'Amazon Resource Name (ARN) o l'identificatore univoco (key ID) per il AWS KMS key che viene utilizzato di default per crittografare gli oggetti che vengono aggiunti al bucket interessato.
Crittografia del bucket S3 richiesta dalla policy del bucket	<code>resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads</code>	Specifica se la policy del bucket per il bucket interessato richiede la crittografia degli oggetti sul lato server quando gli oggetti vengono aggiunti al bucket. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi per l'API, consulta S3Bucket nell'Amazon Macie API Reference.
Nome del bucket S3*	<code>resourcesAffected.s3Bucket.name</code>	Il nome completo del bucket interessato.
Nome visualizzato del proprietario del bucket S3*	<code>resourcesAffected.s3Bucket.owner.displayName</code>	Il nome visualizzato dell' AWS utente proprietario del bucket interessato.

Campo	Campo JSON	Descrizione
Autorizzazione di accesso pubblico al bucket S3	<code>resourcesAffected.s3Bucket.publicAccess.effectivePermission</code>	Specifica se il bucket interessato è accessibile pubblicamente in base a una combinazione di impostazioni di autorizzazione che si applicano al bucket. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi per l'API, consulta BucketPublicAccess Amazon Macie API Reference.
—	<code>resourcesAffected.s3Bucket.publicAccess.\n</code> <code>permissionConfiguration.accountLevelPermissions.\n</code> <code>blockPublicAccess.blockPublicAcls</code>	Un valore booleano che specifica se Amazon S3 blocca le liste di controllo degli accessi pubblici (ACLs) per il bucket interessato e gli oggetti in esso contenuti. Si tratta di un'impostazione di accesso pubblico a blocco a livello di account per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.accountLevelPermissions.</code> <code>blockPublicAccess.blockPublicPolicy</code>	Un valore booleano che specifica se Amazon S3 blocca le policy dei bucket pubblici per il bucket interessato. Si tratta di un'impostazione di accesso pubblico a blocco a livello di account per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.accountLevelPermissions.</code> <code>blockPublicAccess.ignorePublicAcls</code>	Un valore booleano che specifica se Amazon S3 ignora il pubblico ACLs per il bucket interessato e gli oggetti nel bucket. Si tratta di un'impostazione di accesso pubblico a blocco a livello di account per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.accountLevelPermissions.</code> <code>blockPublicAccess.restrictPublicBuckets</code>	Un valore booleano che specifica se Amazon S3 limita le politiche dei bucket pubblici per il bucket interessato. Si tratta di un'impostazione di accesso pubblico a blocco a livello di account per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>accessControlList.allowsPublicReadAccess</code>	Un valore booleano che specifica se l'ACL a livello di bucket per il bucket interessato concede al pubblico le autorizzazioni di accesso in lettura per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>accessControlList.allowsPublicWriteAccess</code>	Un valore booleano che specifica se l'ACL a livello di bucket per il bucket interessato concede al pubblico le autorizzazioni di accesso in scrittura per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>blockPublicAccess.blockPublicAcls</code>	Un valore booleano che specifica se Amazon S3 blocca il pubblico ACLs per il bucket interessato e gli oggetti nel bucket. Si tratta di un'impostazione di accesso pubblico a blocchi a livello di bucket per un bucket. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>blockPublicAccess.blockPublicPolicy</code>	Un valore booleano che specifica se Amazon S3 blocca le policy dei bucket pubblici per il bucket interessato. Si tratta di un'impostazione di accesso pubblico a blocchi a livello di bucket per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>blockPublicAccess.ignorePublicAcls</code>	Un valore booleano che specifica se Amazon S3 ignora il pubblico ACLs per il bucket interessato e gli oggetti nel bucket. Si tratta di un'impostazione di accesso pubblico a blocco a livello di bucket per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>blockPublicAccess.restrictPublicBuckets</code>	Un valore booleano che specifica se Amazon S3 limita le politiche dei bucket pubblici per il bucket interessato. Si tratta di un'impostazione di accesso pubblico a blocco a livello di bucket per il bucket. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>bucketPolicy.allowPublicReadAccess</code>	Un valore booleano che specifica se la politica del bucket interessato consente al pubblico in generale di avere accesso in lettura al bucket. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>resourcesAffected.s3Bucket.publicAccess.</code> <code>permissionConfiguration.bucketLevelPermissions.</code> <code>bucketPolicy.allowPublicWriteAccess</code>	Un valore booleano che specifica se la politica del bucket interessato consente al pubblico in generale di avere accesso in scrittura al bucket. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
Chiave bucket tag S3*	<code>resourcesAffected.s3Bucket.tags.key</code>	Una chiave tag associata al bucket interessato.
Valore del tag bucket S3*	<code>resourcesAffected.s3Bucket.tags.value</code>	Un valore di tag associato al bucket interessato.

* Per specificare più valori per questo campo sulla console, aggiungi una condizione che utilizzi il campo e specifichi un valore distinto per il filtro, quindi ripeti il passaggio per ogni valore aggiuntivo. Per eseguire questa operazione con l'API, utilizza un array che elenchi i valori da utilizzare per il filtro.

Oggetto S3

Questa tabella elenca e descrive i campi che è possibile utilizzare per filtrare i risultati in base alle caratteristiche dell'oggetto S3 a cui si applica un risultato.

Nella tabella, la colonna Campo indica il nome del campo sulla console Amazon Macie. La colonna del campo JSON utilizza la notazione a punti per indicare il nome del campo nelle rappresentazioni JSON dei risultati e nell'API Amazon Macie. (I nomi di campo JSON più lunghi utilizzano la sequenza di caratteri di nuova riga (`\n`) per migliorare la leggibilità.) `\n` La colonna Descrizione fornisce una breve descrizione dei dati archiviati nel campo e indica eventuali requisiti per i valori del filtro. La tabella viene ordinata in ordine alfabetico crescente per campo e quindi per campo JSON.

Campo	Campo JSON	Descrizione
ID della chiave KMS di crittografia degli oggetti S3*	<code>resourcesAffected.s3object.\nserverSideEncryption.kmsMasterKeyId</code>	L'Amazon Resource Name (ARN) o l'identificatore univoco (ID chiave) per il AWS KMS key che è stato utilizzato per crittografare l'oggetto interessato.
Tipo di crittografia degli oggetti S3	<code>resourcesAffected.s3object.\n</code>	

Campo	Campo JSON	Descrizione
	<code>serverSideEncryption.encryptedType</code>	L'algoritmo di crittografia lato server utilizzato per crittografare l'oggetto interessato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi per l'API, consulta EncryptionType Amazon Macie API Reference.
—	<code>resourcesAffected.s3object.extension</code>	L'estensione del nome di file dell'oggetto interessato. Per gli oggetti che non hanno un'estensione del nome di file, specificate "" come valore per il filtro. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>resourcesAffected.s3object.lastModified</code>	La data e l'ora in cui l'oggetto interessato è stato creato o modificato l'ultima volta, a seconda di quale data sia più recente. Questo campo non è disponibile come opzione di filtro sulla console. Con l'API, puoi utilizzare questo campo per definire un intervallo di tempo per un filtro.
Chiave dell'oggetto S3*	<code>resourcesAffected.s3object.key</code>	Il nome completo (chiave) dell'oggetto interessato, incluso il prefisso dell'oggetto, se applicabile.
—	<code>resourcesAffected.s3object.path</code>	Il percorso completo dell'oggetto interessato, incluso il nome del bucket interessato e il nome dell'oggetto (chiave). Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
Accesso pubblico agli oggetti S3	<code>resourcesAffected.s3object.publicAccess</code>	Un valore booleano che specifica se l'oggetto interessato è accessibile pubblicamente in base a una combinazione di impostazioni di autorizzazione che si applicano all'oggetto. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro.
Chiave del tag dell'oggetto S3*	<code>resourcesAffected.s3object.tags.key</code>	Una chiave di tag associata all'oggetto interessato.
Valore del tag dell'oggetto S3*	<code>resourcesAffected.s3object.tags.value</code>	Un valore di tag associato all'oggetto interessato.

* Per specificare più valori per questo campo sulla console, aggiungi una condizione che utilizza il campo e specifica un valore distinto per il filtro, quindi ripeti il passaggio per ogni valore aggiuntivo. Per eseguire questa operazione con l'API, utilizza un array che elenchi i valori da utilizzare per il filtro.

Campi per i risultati delle politiche

La tabella seguente elenca e descrive i campi che è possibile utilizzare per filtrare i risultati delle politiche. Questi campi memorizzano dati specifici relativi ai risultati delle politiche.

Nella tabella, la colonna Campo indica il nome del campo sulla console Amazon Macie. La colonna del campo JSON utilizza la notazione a punti per indicare il nome del campo nelle rappresentazioni JSON dei risultati e nell'API Amazon Macie. (I nomi di campo JSON più lunghi utilizzano la sequenza di caratteri di nuova riga (`\n`) per migliorare la leggibilità.)
La colonna Descrizione fornisce una breve descrizione dei dati archiviati nel campo e indica eventuali requisiti per i valori del filtro. La tabella viene ordinata in ordine alfabetico crescente per campo e quindi per campo JSON.

Campo	Campo JSON	Descrizione
Tipo di operazione	<code>policyDetails.action.actionType</code>	Il tipo di azione che ha prodotto il risultato. L'unico valore valido per questo campo è <code>AWS_API_CALL</code> .
Nome della chiamata API*	<code>policyDetails.action.apiCallDetails.api</code>	Il nome dell'operazione che è stata richiamata più di recente e che ha prodotto il risultato.
Nome del servizio API*	<code>policyDetails.action.apiCallDetails.apiServiceName</code>	L'URL di Servizio AWS che fornisce l'operazione che è stata richiamata e che ha prodotto il risultato, ad esempio. <code>s3.amazonaws.com</code>
—	<code>policyDetails.action.apiCallDetails.firstSeen</code>	La prima data e ora in cui un'operazione è stata richiamata e ha prodotto il risultato. Questo campo non è disponibile come opzione di filtro sulla console. Con l'API, puoi utilizzare questo campo per definire un intervallo di tempo per un filtro.
—	<code>policyDetails.action.apiCallDetails.lastSeen</code>	La data e l'ora più recenti in cui l'operazione specificata (nome della chiamata API <code>oapi</code>) è stata richiamata e ha prodotto il risultato. Questo campo non è disponibile come opzione di filtro sulla

Campo	Campo JSON	Descrizione
		console. Con l'API, puoi utilizzare questo campo per definire un intervallo di tempo per un filtro.
—	<code>policyDetails.actor.domainDetails.domainName</code>	Il nome di dominio del dispositivo utilizzato per eseguire l'azione. Questo campo non è disponibile come opzione di filtro sulla console.
Città IP*	<code>policyDetails.actor.ipAddressDetails.ipCity.name</code>	Il nome della città di origine dell'indirizzo IP del dispositivo utilizzato per eseguire l'azione.
Paese IP*	<code>policyDetails.actor.ipAddressDetails.ipCountry.name</code>	Il nome del paese di origine dell'indirizzo IP del dispositivo utilizzato per eseguire l'azione, ad esempio. United States
—	<code>policyDetails.actor.ipAddressDetails.ipOwner.asn</code>	L'Autonomous System Number (ASN) del sistema autonomo che includeva l'indirizzo IP del dispositivo utilizzato per eseguire l'azione. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
Proprietario dell'IP, ASN, org*	<code>policyDetails.actor.ipAddressDetails.ipOwner.asnOrg</code>	L'identificatore dell'organizzazione associato all'ASN per il sistema autonomo che includeva l'indirizzo IP del dispositivo utilizzato per eseguire l'azione.
ISP del proprietario dell'IP*	<code>policyDetails.actor.ipAddressDetails.ipOwner.isp</code>	Il nome del provider di servizi Internet (ISP) proprietario dell'indirizzo IP del dispositivo utilizzato per eseguire l'azione.
Indirizzo IP V4*	<code>policyDetails.actor.ipAddressDetails.ipAddressV4</code>	L'indirizzo del protocollo Internet versione 4 (IPv4) del dispositivo utilizzato per eseguire l'azione.
—	<code>policyDetails.actor.userIdentity.\nassumedRole.accessKeyId</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il AssumeRole funzionamento dell' AWS STS API, l'ID della chiave di AWS accesso che identifica le credenziali. Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
Identità dell'utente, ruolo assunto, id dell'account*	<code>policyDetails.actor.userIdentity.\n</code> <code>assumedRole.accountId</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il AssumeRole funzionamento dell' AWS STS API, l'identificatore univoco del proprietario dell' Account AWS entità utilizzata per ottenere le credenziali.
L'identità dell'utente ha assunto il ruolo principal id*	<code>policyDetails.actor.userIdentity.\n</code> <code>assumedRole.principalId</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il AssumeRole funzionamento dell' AWS STS API, l'identificatore univoco dell'entità utilizzato per ottenere le credenziali.
Identità utente: sessione di ruolo assunta ARN*	<code>policyDetails.actor.userIdentity.\n</code> <code>assumedRole.arn</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il AssumeRole funzionamento dell' AWS STS API, l'Amazon Resource Name (ARN) dell'account di origine, dell'utente IAM o del ruolo utilizzato per ottenere le credenziali.

Campo	Campo JSON	Descrizione
—	<code>policyDetails.actor.userIdentity.\n</code> <code>assumedRole.sessionContext.sessionIssuer.type</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il AssumeRole funzionamento dell' AWS STS API, l'origine delle credenziali di sicurezza temporanee, ad esempio, o. Root IAMUser Role Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>policyDetails.actor.userIdentity.\n</code> <code>assumedRole.sessionContext.sessionIssuer.userName</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il AssumeRole funzionamento dell' AWS STS API, il nome o l'alias dell'utente o del ruolo che ha emesso la sessione. Nota che questo valore è nullo se le credenziali sono state ottenute da un account root che non dispone di un alias. Questo campo non è disponibile come opzione di filtro sulla console.
Identità utente, AWS account, id*	<code>policyDetails.actor.userIdentity.\n</code> <code>awsAccount.accountId</code>	Per un'azione eseguita utilizzando le credenziali di un'altra Account AWS, l'identificatore univoco dell'account.

Campo	Campo JSON	Descrizione
ID principale dell' AWS account di identità utente*	<code>policyDetails.actor.userIdentity.\nawsAccount.principalId</code>	Per un'azione eseguita utilizzando le credenziali di un'altra Account AWS, l'identificatore univoco dell'entità che ha eseguito l'azione.
AWS Servizio di identità utente richiamato da	<code>policyDetails.actor.userIdentity.\nawsService.invokedBy</code>	Per un'azione eseguita da un account che appartiene a un Servizio AWS, il nome del servizio.
—	<code>policyDetails.actor.userIdentity.\nfederatedUser.accessKeyId</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il <code>GetFederationToken</code> funzionamento dell' AWS STS API, l'ID della chiave di AWS accesso che identifica le credenziali. Questo campo non è disponibile come opzione di filtro sulla console.
Sessione federata con identità utente ARN*	<code>policyDetails.actor.userIdentity.\nfederatedUser.arn</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il <code>GetFederationToken</code> funzionamento dell' AWS STS API, l'ARN dell'entità utilizzata per ottenere le credenziali.

Campo	Campo JSON	Descrizione
Identità utente, ID dell'account utente federato*	<code>policyDetails.actor.userIdentity.\n</code> <code>federatedUser.accountId</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il <code>GetFederationToken</code> funzionamento dell' AWS STS API, l'identificatore univoco del proprietario dell' Account AWS entità utilizzata per ottenere le credenziali.
Identità utente, ID principale dell'utente federato*	<code>policyDetails.actor.userIdentity.\n</code> <code>federatedUser.principalId</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il <code>GetFederationToken</code> funzionamento dell' AWS STS API, l'identificatore univoco dell'entità utilizzato per ottenere le credenziali.
—	<code>policyDetails.actor.userIdentity.\n</code> <code>federatedUser.sessionContext.sessionIssuer.type</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il <code>GetFederationToken</code> funzionamento dell' AWS STS API, l'origine delle credenziali di sicurezza temporanee, ad esempio, o. <code>Root IAMUser Role</code> Questo campo non è disponibile come opzione di filtro sulla console.

Campo	Campo JSON	Descrizione
—	<code>policyDetails.actor.userIdentity.\n</code> <code>federatedUser.sessionContext.sessionIssuer.userName</code>	Per un'azione eseguita con credenziali di sicurezza temporanee ottenute utilizzando il <code>GetFederationToken</code> funzionamento dell' AWS STS API, il nome o l'alias dell'utente o del ruolo che ha emesso la sessione. Nota che questo valore è nullo se le credenziali sono state ottenute da un account root che non dispone di un alias. Questo campo non è disponibile come opzione di filtro sulla console.
Identità utente, ID dell'account IAM*	<code>policyDetails.actor.userIdentity.\n</code> <code>iamUser.accountId</code>	Per un'azione eseguita utilizzando le credenziali di un utente IAM, l'identificatore univoco associato all'utente IAM Account AWS che ha eseguito l'azione.
Identità utente, ID principale IAM*	<code>policyDetails.actor.userIdentity.\n</code> <code>iamUser.principalId</code>	Per un'azione eseguita utilizzando le credenziali di un utente IAM, l'identificatore univoco dell'utente IAM che ha eseguito l'azione.
Identità utente, nome utente IAM*	<code>policyDetails.actor.userIdentity.\n</code> <code>iamUser.userName</code>	Per un'azione eseguita utilizzando le credenziali di un utente IAM, il nome utente dell'utente IAM che ha eseguito l'azione.

Campo	Campo JSON	Descrizione
Identità dell'utente, ID dell'account root*	<code>policyDetails.actor.userIdentity.\nroot.accountId</code>	Per un'azione eseguita utilizzando le credenziali del tuo Account AWS, l'identificatore univoco dell'account.
Identità utente, root principal id*	<code>policyDetails.actor.userIdentity.\nroot.principalId</code>	Per un'azione eseguita utilizzando le credenziali dell'utente Account AWS, l'identificatore univoco dell'entità che ha eseguito l'azione.
Tipo di identità utente	<code>policyDetails.actor.userIdentity.type</code>	Il tipo di entità che ha eseguito l'azione che ha prodotto il risultato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi per l'API, consulta UserIdentityType Amazon Macie API Reference.

* Per specificare più valori per questo campo sulla console, aggiungi una condizione che utilizzi il campo e specifichi un valore distinto per il filtro, quindi ripeti il passaggio per ogni valore aggiuntivo. Per eseguire questa operazione con l'API, utilizza un array che elenchi i valori da utilizzare per il filtro.

Campi per il rilevamento di dati sensibili

La tabella seguente elenca e descrive i campi che è possibile utilizzare per filtrare i risultati di dati sensibili. Questi campi memorizzano dati specifici per i risultati relativi ai dati sensibili.

Nella tabella, la colonna Campo indica il nome del campo sulla console Amazon Macie. La colonna del campo JSON utilizza la notazione a punti per indicare il nome del campo nelle rappresentazioni JSON dei risultati e nell'API Amazon Macie. (I nomi di campo JSON più lunghi utilizzano la sequenza

di caratteri di nuova riga () per migliorare la leggibilità.) \n La colonna Descrizione fornisce una breve descrizione dei dati archiviati nel campo e indica eventuali requisiti per i valori del filtro. La tabella viene ordinata in ordine alfabetico crescente per campo e quindi per campo JSON.

Campo	Campo JSON	Descrizione
ID identificatore di dati personalizzato*	classificationDetails.result.\n customDataIdentifiers.detections.arn	L'identificatore univoco dell'identificatore di dati personalizzato che ha rilevato i dati e prodotto il risultato.
Nome dell'identificatore di dati personalizzato*	classificationDetails.result.\n customDataIdentifiers.detections.name	Il nome dell'identificatore di dati personalizzato che ha rilevato i dati e prodotto il risultato.
Numero totale degli identificatori di dati personalizzati	classificationDetails.result.\n customDataIdentifiers.detections.count	Il numero totale di occorrenze dei dati rilevate da identificatori di dati personalizzati e che hanno prodotto il risultato. È possibile utilizzare questo campo per definire un intervallo numerico per un filtro.
Job ID*	classificationDetails.jobId	L'identificatore univoco del processo di rilevamento dei dati sensibili che ha prodotto il risultato.
Tipo di origine	classificationDetails.originType	Come Macie ha trovato i dati sensibili che hanno prodotto la scoperta: AUTOMATED_SENSITIVE_DATA_DISCOVERY o SENSITIVE_DATA_DISCOVERY_JOB .

Campo	Campo JSON	Descrizione
—	<code>classificationDetails.result.mimeType</code>	Il tipo di contenuto, in formato MIME, a cui si applica il risultato, ad esempio per un file CSV o <code>text/csv</code> per un file Adobe Portable Document Format. Questo campo non è disponibile come opzione di filtro sulla console.
—	<code>classificationDetails.result.sizeClassified</code>	La dimensione totale di archiviazione, in byte, dell'oggetto S3 a cui si applica il risultato. Questo campo non è disponibile come opzione di filtro sulla console. Con l'API, puoi utilizzare questo campo per definire un intervallo numerico per un filtro.

Campo	Campo JSON	Descrizione
Codice di stato del risultato*	<code>classificationDetails.result.status.code</code>	Lo stato del risultato. I valori validi sono: • COMPLETE— Macie ha completato l'analisi dell'oggetto. • PARTIAL— Macie ha analizzato solo un sottoinsieme dei dati nell'oggetto. Ad esempio, l'oggetto è un file di archivio che contiene file in un formato non supportato. • SKIPPED— Macie non è stata in grado di analizzare e l'oggetto. Ad esempio, l'oggetto è un file in formato errato.
Categoria di dati sensibili	<code>classificationDetails.result.sensitiveData.category</code>	La categoria di dati sensibili che sono stati rilevati e che hanno prodotto il risultato. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Nell'API, i valori validi sono: CREDENTIALS, FINANCIAL_INFORMATION, ePERSONAL_INFORMATION.

Campo	Campo JSON	Descrizione
Tipo di rilevamento dei dati sensibili	<code>classificationDetails.result.\n</code> <code>sensitiveData.detections.type</code>	Il tipo di dati sensibili che sono stati rilevati e che hanno prodotto il risultato. Si tratta dell'identificatore univoco dell'identificatore di dati gestito che ha rilevato i dati. La console fornisce un elenco di valori tra cui scegliere quando si aggiunge questo campo a un filtro. Per un elenco di valori validi sia per la console che per l'API, consulta Riferimento rapido: identificatori di dati gestiti per tipo.
Conteggio totale dei dati sensibili	<code>classificationDetails.result.\n</code> <code>sensitiveData.detections.count</code>	Il numero totale di ricorrenze e del tipo di dati sensibili rilevati e che hanno prodotto il risultato. È possibile utilizzare questo campo per definire un intervallo numerico per un filtro.

* Per specificare più valori per questo campo sulla console, aggiungi una condizione che utilizzi il campo e specifichi un valore distinto per il filtro, quindi ripeti il passaggio per ogni valore aggiuntivo. Per eseguire questa operazione con l'API, utilizza un array che elenchi i valori da utilizzare per il filtro.

Creazione e applicazione di filtri ai risultati di Macie

Per identificare e concentrarti sui risultati con caratteristiche specifiche, puoi filtrare i risultati sulla console Amazon Macie e nelle query inviate a livello di codice utilizzando l'API Amazon Macie. Quando crei un filtro, utilizzi attributi specifici dei risultati per definire criteri per includere o escludere i

risultati da una vista o dai risultati delle query. Un attributo di ricerca è un campo che memorizza dati specifici per un risultato, come la gravità, il tipo o il nome della risorsa a cui si applica un risultato.

In Macie, un filtro è costituito da una o più condizioni. Ogni condizione, nota anche come criterio, è composta da tre parti:

- Un campo basato su attributi, come Severity o Finding type.
- Un operatore, ad esempio uguale o non uguale.
- Uno o più valori. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti.

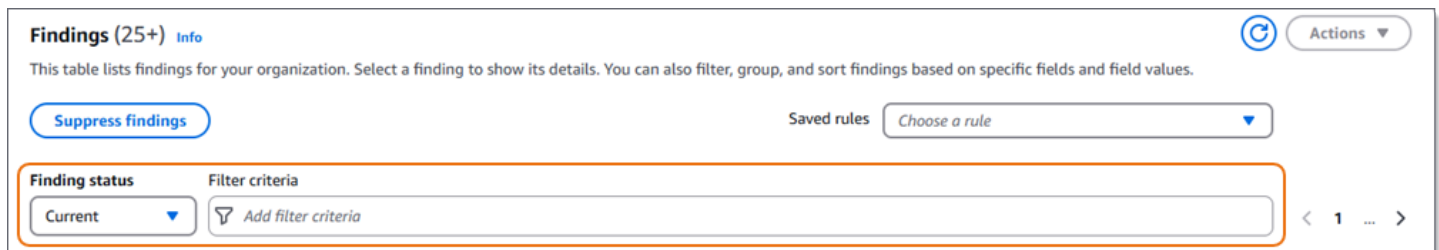
Il modo in cui definisci e applichi le condizioni di filtro dipende dal fatto che utilizzi la console Amazon Macie o l'API Amazon Macie.

Argomenti

- [Filtrare i risultati utilizzando la console Amazon Macie](#)
- [Filtraggio dei risultati in modo programmatico con l'API Amazon Macie](#)

Filtrare i risultati utilizzando la console Amazon Macie

Se utilizzi la console Amazon Macie per filtrare i risultati, Macie offre opzioni per aiutarti a scegliere campi, operatori e valori per condizioni individuali. Puoi accedere a queste opzioni utilizzando le impostazioni dei filtri nelle pagine Findings, come mostrato nell'immagine seguente.



Utilizzando il menu Finding status, è possibile specificare se includere i risultati che sono stati soppressi (archiviati automaticamente) da una regola di [soppressione](#). Utilizzando la casella Criteri di filtro, è possibile inserire le condizioni di filtro.

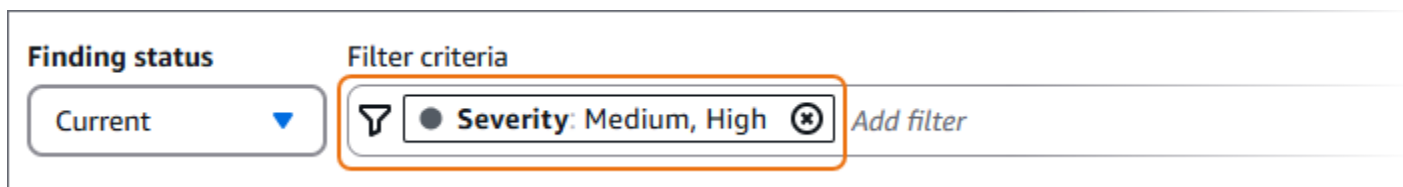
Quando posizionate il cursore nella casella Criteri di filtro, Macie visualizza un elenco di campi che è possibile utilizzare nelle condizioni di filtro. I campi sono organizzati per categorie logiche. Ad esempio, la categoria Campi comuni include campi che si applicano a qualsiasi tipo di ricerca e la

categoria Campi di classificazione include campi che si applicano solo ai risultati di dati sensibili. I campi sono ordinati alfabeticamente all'interno di ogni categoria.

Per aggiungere una condizione, inizia scegliendo un campo dall'elenco. Per trovare un campo, sfoglia l'elenco completo o inserisci parte del nome del campo per restringere l'elenco dei campi.

A seconda del campo scelto, Macie mostra diverse opzioni. Le opzioni riflettono il tipo e la natura del campo scelto. Ad esempio, se scegli il campo Severità, Macie visualizza un elenco di valori tra cui scegliere: Basso, Medio e Alto. Se scegli il campo del nome del bucket S3, Macie visualizza una casella di testo in cui puoi inserire il nome del bucket. Qualunque campo tu scelga, Macie ti guida attraverso i passaggi per aggiungere una condizione che includa le impostazioni richieste per il campo.

Dopo aver aggiunto una condizione, Macie applica i criteri relativi alla condizione e aggiunge la condizione a un token di filtro nella casella Criteri del filtro, come mostrato nell'immagine seguente.



The screenshot shows the 'Filter criteria' section of the Macie console. On the left, there is a 'Finding status' dropdown menu currently set to 'Current'. To its right is the 'Filter criteria' section, which is highlighted with an orange border. Inside this section, there is a filter token for 'Severity: Medium, High'. The token includes a radio button that is selected for 'Medium, High' and another radio button for 'Low' which is unselected. To the right of the filter token is a button labeled 'Add filter'.

In questo esempio, la condizione è configurata per includere tutti i risultati di gravità media e alta e per escludere tutti i risultati di bassa gravità. Restituisce risultati in cui il valore del campo Severità è uguale a Medio o Alto.

Tip

Per molti campi, è possibile modificare l'operatore di una condizione da uguale a non uguale scegliendo l'icona uguale



nel token di filtro relativo alla condizione. Se lo fai, Macie cambia l'operatore in not equals e visualizza l'icona not equals () nel token.



Per passare nuovamente all'operatore equals, scegli l'icona not equals.

Man mano che aggiungi altre condizioni, Macie applica i relativi criteri e li aggiunge ai token nella casella Filtra criteri. Puoi fare riferimento al riquadro in qualsiasi momento per determinare quali criteri hai applicato. Per rimuovere una condizione, scegli l'icona di rimozione della condizione



nel token della condizione.

Per filtrare i risultati utilizzando la console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. (Facoltativo) Per esaminare e analizzare prima i risultati in base a un gruppo logico predefinito, scegli Per bucket, Per tipo o Per processo nel pannello di navigazione (sotto Risultati). Quindi scegli un elemento nella tabella. Nel pannello dei dettagli, scegli il link relativo al campo su cui eseguire il pivot.
4. (Facoltativo) Per visualizzare i risultati che sono stati soppressi da una [regola di soppressione](#), modifica l'impostazione dello stato del filtro. Scegliete Archiviato per visualizzare solo i risultati soppressi oppure scegliete Tutti per visualizzare sia i risultati soppressi che quelli non soppressi. Per nascondere i risultati soppressi, scegliete Corrente.
5. Per aggiungere una condizione di filtro:
 - a. Posiziona il cursore nella casella Criteri del filtro, quindi scegli il campo da utilizzare per la condizione. Per informazioni sui campi che puoi utilizzare, consulta [Campi per filtrare i risultati di Macie](#).
 - b. Immettere il tipo di valore appropriato per il campo. Per informazioni dettagliate sui diversi tipi di valori, vedere [Specificare i valori per i campi](#).

Matrice di testo (stringhe)

Per questo tipo di valore, Macie fornisce spesso un elenco di valori tra cui scegliere. In tal caso, selezionate ogni valore che desiderate utilizzare nella condizione.

Se Macie non fornisce un elenco di valori, inserisci un valore completo e valido per il campo. Per specificare valori aggiuntivi per il campo, scegli Applica, quindi aggiungi un'altra condizione per ogni valore aggiuntivo.

Nota che i valori distinguono tra maiuscole e minuscole. Inoltre, non è possibile utilizzare valori parziali o caratteri jolly nei valori. Ad esempio, per filtrare i risultati per un bucket S3 denominato my-S3-bucket, inseriscilo **my-S3-bucket** come valore per il campo del nome del bucket S3. Se inserisci qualsiasi altro valore, ad esempio **my-s3-bucket** o, Macie non restituirà i risultati per il **my-S3** bucket.

Booleano

Per questo tipo di valore, Macie fornisce un elenco di valori tra cui scegliere. Seleziona il valore che desideri utilizzare nella condizione.

Data/ora (intervalli di tempo)

Per questo tipo di valore, utilizzate le caselle Da e A per definire un intervallo di tempo inclusivo:

- Per definire un intervallo di tempo fisso, utilizzate le caselle Da e A per specificare rispettivamente la prima data e ora e l'ultima data e ora dell'intervallo.
- Per definire un intervallo di tempo relativo che inizi in una determinata data e ora e termini nell'ora corrente, immettete la data e l'ora di inizio nelle caselle Da ed eliminate il testo nelle caselle To.
- Per definire un intervallo di tempo relativo che termini con una determinata data e ora, inserite la data e l'ora di fine nelle caselle A ed eliminate il testo nelle caselle Da.

Tieni presente che i valori temporali utilizzano la notazione a 24 ore. Se si utilizza il selettore di date per scegliere le date, è possibile rifinire i valori inserendo il testo direttamente nelle caselle Da e A.

Numero (intervalli numerici)

Per questo tipo di valore, utilizzate le caselle Da e A per inserire uno o più numeri interi che definiscono un intervallo numerico inclusivo, fisso o relativo.

Valori di testo (stringa)

Per questo tipo di valore, inserisci un valore completo e valido per il campo.

Nota che i valori fanno distinzione tra maiuscole e minuscole. Inoltre, non è possibile utilizzare valori parziali o caratteri jolly nei valori. Ad esempio, per filtrare i risultati per un bucket S3 denominato my-S3-bucket, inseriscilo **my-S3-bucket** come valore per il campo del nome del bucket S3. Se inserisci qualsiasi altro valore, ad esempio **my-s3-bucket** o, Macie non restituirà i risultati per il **my-S3** bucket.

- c. Quando hai finito di aggiungere i valori per il campo, scegli Applica. Macie applica i criteri di filtro e aggiunge la condizione a un token di filtro nella casella Criteri di filtro.

6. Ripeti il passaggio 5 per ogni condizione aggiuntiva che desideri aggiungere.

7. Per rimuovere una condizione, scegli l'icona di rimozione della condizione



)

nel token del filtro relativo alla condizione.

8. Per modificare una condizione, rimuovi la condizione scegliendo l'icona di rimozione della condizione



)

nel token del filtro relativo alla condizione. Quindi ripeti il passaggio 5 per aggiungere una condizione con le impostazioni corrette.

Tip

Se desideri utilizzare nuovamente questo set di condizioni in un secondo momento, puoi salvare il set come regola di filtro. A tale scopo, scegli Salva regola nella casella Criteri di filtro. Quindi inserisci un nome e, facoltativamente, una descrizione per la regola. Al termine, scegli Salva.

Filtraggio dei risultati in modo programmatico con l'API Amazon Macie

Per filtrare i risultati in modo programmatico, specifica i criteri di filtro nelle query inviate utilizzando [ListFindings](#) o il [GetFindingStatistics](#) funzionamento dell'API Amazon Macie. L'[ListFindings](#) operazione restituisce una serie di risultati IDs, un ID per ogni risultato che corrisponde ai criteri di filtro. L'[GetFindingStatistics](#) operazione restituisce dati statistici aggregati su tutti i risultati che corrispondono ai criteri di filtro, raggruppati in base a un campo specificato nella richiesta.

Tieni presente che le [GetFindingStatistics](#) operazioni [ListFindings](#) and sono diverse dalle operazioni utilizzate per [sopprimere](#) i risultati. A differenza delle operazioni di soppressione, che specificano anche criteri di filtro, le [GetFindingStatistics](#) operazioni [ListFindings](#) and interrogano solo i dati dei risultati. Non eseguono alcuna azione sui risultati che soddisfano i criteri di filtro. Per eliminare i risultati, utilizza il [CreateFindingsFilter](#) funzionamento dell'API Amazon Macie.

Per specificare i criteri di filtro in una query, includi una mappa delle condizioni di filtro nella richiesta. Per ogni condizione, specificate un campo, un operatore e uno o più valori per il campo. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti. Per informazioni sui campi, gli operatori e i tipi di valori che è possibile utilizzare in una condizione, vedere [Campi per filtrare i risultati di Macie](#) [Utilizzo degli operatori in condizioni](#), e [Specificare i valori per i campi](#).

Gli esempi seguenti mostrano come specificare i criteri di filtro nelle query inviate utilizzando [AWS Command Line Interface \(AWS CLI\)](#). Puoi farlo anche utilizzando la versione corrente di un altro strumento a riga di AWS comando o di un AWS SDK oppure inviando richieste HTTPS direttamente a Macie. Per informazioni sugli AWS strumenti e SDKs, consulta [Tools to Build on](#). AWS

Esempi

- [Esempio 1: filtra i risultati in base alla gravità](#)
- [Esempio 2: filtra i risultati in base alla categoria di dati sensibili](#)
- [Esempio 3: filtra i risultati in base a un intervallo di tempo fisso](#)
- [Esempio 4: filtra i risultati in base allo stato di soppressione](#)
- [Esempio 5: filtra i risultati in base a più campi e tipi di valori](#)

Negli esempi viene utilizzato il comando [list-finding](#). Se un esempio viene eseguito correttamente, Macie restituisce un array. `findingIds` L'array elenca l'identificatore univoco per ogni risultato che corrisponde ai criteri di filtro, come illustrato nell'esempio seguente.

```
{
  "findingIds": [
    "1f1c2d74db5d8caa76859ec52example",
    "6cfa9ac820dd6d55cad30d851example",
    "702a6fd8750e567d1a3a63138example",
    "826e94e2a820312f9f964cf60example",
    "274511c3fdcd87010a19a3a42example"
  ]
}
```

Se nessun risultato corrisponde ai criteri di filtro, Macie restituisce un array vuoto `findingIds`.

```
{
  "findingIds": []
}
```

Esempio 1: filtra i risultati in base alla gravità

Questo esempio recupera i risultati IDs per tutti i risultati di gravità elevata e media nella versione corrente. Regione AWS

Per Linux, macOS o Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={"criterion\":
{"severity.description\":{"eq\":["High\","Medium\"]}}}
```

Dove:

- *severity.description* specifica il nome JSON del campo Severity.
- *eq* specifica l'operatore equals.
- *High* e *Medium* sono una matrice di valori enumerati per il campo Severità.

Esempio 2: filtra i risultati in base alla categoria di dati sensibili

Questo esempio recupera i risultati di tutti i dati sensibili rilevati nella regione corrente e riporta le occorrenze di informazioni finanziarie (e nessun'altra categoria di dati sensibili) negli oggetti S3. IDs

Per Linux, macOS o Unix, utilizzando il carattere di continuazione di riga con barra rovesciata (\) per migliorare la leggibilità:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Per Microsoft Windows, utilizzando il carattere di continuazione di riga con cursore (^) per migliorare la leggibilità:

```
C:\> aws macie2 list-findings ^
--finding-criteria={"criterion\":
{"classificationDetails.result.sensitiveData.category\":{"eqExactMatch\":
{"FINANCIAL_INFORMATION\"]}}}
```

Dove:

- *classificationDetails.result.sensitiveData.category* specifica il nome JSON del campo Categoria di dati sensibili.

- *eqExactMatch* specifica l'operatore equals Exact Match.
- *FINANCIAL_INFORMATION* è un valore enumerato per il campo Categoria di dati sensibili.

Esempio 3: filtra i risultati in base a un intervallo di tempo fisso

Questo esempio recupera i risultati IDs per tutti i risultati che si trovano nella regione corrente e sono stati creati tra le 07:00 UTC del 5 ottobre 2020 e le 07:00 UTC del 5 novembre 2020 (incluse).

Per Linux, macOS o Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":{"gte":"1601881200000","lte":"1604559600000"}}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={"criterion":{"createdAt":{"gte":"1601881200000","lte":"1604559600000"}}}
```

Dove:

- *createdAt* specifica il nome JSON del campo Created at.
- *gte* specifica l'operatore maggiore o uguale a.
- *1601881200000* è la prima data e ora (come timestamp Unix in millisecondi) nell'intervallo di tempo.
- *lte* specifica l'operatore minore o uguale a.
- *1604559600000* è l'ultima data e ora (come timestamp Unix in millisecondi) nell'intervallo di tempo.

Esempio 4: filtra i risultati in base allo stato di soppressione

Questo esempio recupera i risultati IDs per tutti i risultati che si trovano nella regione corrente e che sono stati soppressi (archiviati automaticamente) da una regola di soppressione.

Per Linux, macOS o Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":["true"]}}}'
```

Per Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={"criterion":{"archived":{"eq":["true"]}}}
```

Dove:

- *archived* specifica il nome JSON del campo Archiviato.
- *eq* specifica l'operatore equals.
- *true* è un valore booleano per il campo Archiviato.

Esempio 5: filtra i risultati in base a più campi e tipi di valori

Questo esempio recupera i risultati di tutti i dati sensibili che si trovano nella regione corrente e soddisfano i seguenti criteri: sono stati creati tra le 07:00 UTC del 5 ottobre 2020 e le 07:00 UTC del 5 novembre 2020 (esclusivamente); segnala le occorrenze di dati finanziari e nessun'altra categoria di dati sensibili negli oggetti S3; e non sono stati soppressi (archiviati automaticamente) da una regola di soppressione. IDs

Per Linux, macOS o Unix, utilizzando il carattere di continuazione di riga con barra rovesciata (\) per migliorare la leggibilità:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":"1601881200000","lt":"1604559600000"},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Per Microsoft Windows, utilizzando il carattere di continuazione di riga con cursore (^) per migliorare la leggibilità:

```
C:\> aws macie2 list-findings ^
--finding-criteria={"criterion":{"createdAt":{"gt":"1601881200000,
\"lt\":\"1604559600000\"},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

Dove:

- *createdAt* specifica il nome JSON del campo Created at e:
- *gt* specifica l'operatore maggiore o uguale a.

- **1601881200000** è la prima data e ora (come timestamp Unix in millisecondi) nell'intervallo di tempo.
- **lt** specifica l'operatore minore o uguale a.
- **1604559600000** è l'ultima data e ora (come timestamp Unix in millisecondi) nell'intervallo di tempo.
- **classificationDetails.result.sensitiveData.category** specifica il nome JSON del campo della categoria di dati sensibili e:
 - **eqExactMatch** specifica l'operatore equals Exact Match.
 - **FINANCIAL_INFORMATION** è un valore enumerato per il campo.
- **archived** specifica il nome JSON del campo Archiviato e:
 - **eq** specifica l'operatore equals.
 - **false** è un valore booleano per il campo.

Definizione delle regole di filtro per i risultati di Macie

Per eseguire un'analisi coerente dei risultati, puoi creare e applicare regole di filtro. Una regola di filtro è un insieme di criteri di filtro che crei e salvi per riutilizzarli quando esamini i risultati sulla console Amazon Macie. Le regole di filtro possono aiutarti a eseguire analisi ripetute e coerenti di risultati con caratteristiche specifiche. Ad esempio, è possibile creare una regola di filtro per analizzare tutti i dati sensibili ad alta gravità che riportano tipi specifici di dati sensibili. Puoi creare un'altra regola di filtro per analizzare tutti i risultati delle policy ad alta severità per i bucket Amazon Simple Storage Service (Amazon S3) che memorizzano oggetti non crittografati.

Quando crei una regola di filtro, utilizzi attributi specifici dei risultati per definire criteri per includere o escludere i risultati da una vista. Un attributo di ricerca è un campo che memorizza dati specifici per un risultato, come la gravità, il tipo o il nome del bucket S3 a cui si applica un risultato. È inoltre necessario specificare un nome e, facoltativamente, una descrizione della regola. Per analizzare quindi i risultati che corrispondono ai criteri della regola, scegli la regola. Macie applica i criteri della regola e visualizza solo i risultati che corrispondono ai criteri. Macie visualizza anche i criteri per aiutarti a determinare quali criteri ha applicato.

Nota che le regole di filtro sono diverse dalle regole di soppressione. Una regola di soppressione è un insieme di criteri di filtro creati e salvati per archiviare automaticamente i risultati che corrispondono ai criteri della regola. Sebbene entrambi i tipi di regole memorizzino e applichino criteri di filtro, una regola di filtro non esegue alcuna azione sui risultati che soddisfano i criteri della regola. Invece, una

regola di filtro determina solo quali risultati vengono visualizzati sulla console dopo l'applicazione della regola. Per informazioni sulle regole di soppressione, vedere [Eliminazione dei risultati](#).

Argomenti

- [Creazione di una regola di filtro per i risultati di Macie](#)
- [Applicazione di una regola di filtro ai risultati di Macie](#)
- [Modifica di una regola di filtro per i risultati di Macie](#)
- [Eliminazione di una regola di filtro per i risultati di Macie](#)

Creazione di una regola di filtro per i risultati di Macie

Una regola di filtro è un insieme di criteri di filtro che crei e salvi per riutilizzarli quando esamini i risultati sulla console Amazon Macie. Le regole di filtro possono aiutarti a eseguire analisi ripetute e coerenti di risultati con caratteristiche specifiche. Ad esempio, potresti creare una regola di filtro per analizzare tutti i dati sensibili ad alta gravità che segnalano le occorrenze di dati sensibili, in particolare i bucket Amazon Simple Storage Service (Amazon S3). Puoi quindi applicare quella regola di filtro ogni volta che desideri identificare e analizzare i risultati che presentano le caratteristiche specificate.

Quando si crea una regola di filtro, si specificano i criteri di filtro, un nome e, facoltativamente, una descrizione della regola. Per i criteri di filtro, si utilizzano attributi specifici dei risultati per specificare se includere o escludere i risultati da una vista. Un attributo di ricerca è un campo che memorizza dati specifici per un risultato, come la gravità, il tipo o il nome della risorsa a cui si applica un risultato. I criteri di filtro sono costituiti da una o più condizioni. Ogni condizione, nota anche come criterio, è composta da tre parti:

- Un campo basato su attributi, come Severity o Finding type.
- Un operatore, ad esempio uguale o non uguale.
- Uno o più valori. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti.

Dopo aver creato e salvato una regola di filtro, puoi applicarne i criteri di filtro scegliendo la regola. Macie utilizza quindi i criteri per determinare quali risultati visualizzare. Macie visualizza anche i criteri per aiutarti a determinare quali criteri hai applicato.

Nota che le regole di filtro sono diverse dalle regole di soppressione. Una regola di soppressione è un insieme di criteri di filtro creati e salvati per archiviare automaticamente i risultati che corrispondono ai criteri della regola. Sebbene entrambi i tipi di regole memorizzino e applichino criteri di filtro, una

regola di filtro non esegue alcuna azione sui risultati che soddisfano i criteri della regola. Invece, una regola di filtro determina solo quali risultati vengono visualizzati sulla console dopo l'applicazione della regola. Per informazioni sulle regole di soppressione, vedere [Eliminazione dei risultati](#).

Per creare una regola di filtro per i risultati

Puoi creare una regola di filtro utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per creare una regola di filtro utilizzando la console Amazon Macie.

Per creare una regola di filtro

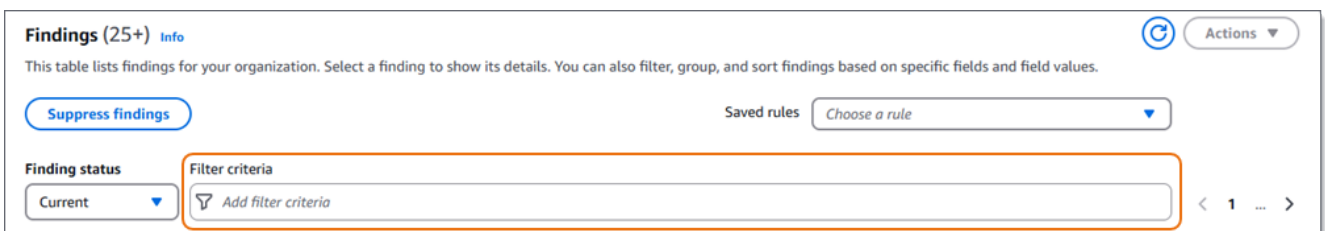
1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.

Tip

Per utilizzare una regola di filtro esistente come punto di partenza, scegli la regola dall'elenco Regole salvate.

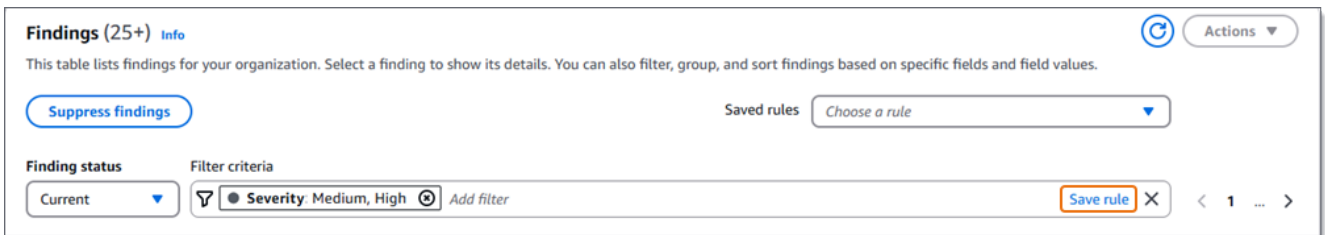
È inoltre possibile semplificare la creazione di una regola impostando innanzitutto i risultati in base a un gruppo logico predefinito e analizzando i risultati in base a un gruppo logico predefinito. In questo caso, Macie crea e applica automaticamente le condizioni di filtro appropriate, che possono essere un utile punto di partenza per creare una regola. Per fare ciò, scegli Per bucket, Per tipo o Per lavoro nel riquadro di navigazione (sotto Risultati). Quindi scegli un elemento nella tabella. Nel pannello dei dettagli, scegli il link relativo al campo su cui eseguire il pivot.

3. Nella casella Criteri di filtro, aggiungi le condizioni che definiscono i criteri di filtro per la regola.



Per informazioni su come aggiungere condizioni di filtro, consulta [Creazione e applicazione di filtri ai risultati di Macie](#).

- Al termine della definizione dei criteri di filtro per la regola, scegli **Salva regola** nella casella **Criteri di filtro**.



- In **Regola di filtro**, inserisci un nome e, facoltativamente, una descrizione della regola.
- Seleziona **Salva**.

API

Per creare una regola di filtro a livello di codice, utilizza il [CreateFindingsFilter](#) funzionamento dell'API Amazon Macie e specifica i valori appropriati per i parametri richiesti:

- Per il `action` parametro, specifica `N00P` in modo che Macie non sopprima (archivi automaticamente) i risultati che corrispondono ai criteri della regola.
- Per il `criterion` parametro, specifica una mappa di condizioni che definiscono i criteri di filtro per la regola.

Nella mappa, ogni condizione deve specificare un campo, un operatore e uno o più valori per il campo. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti. Per informazioni sui campi, gli operatori e i tipi di valori che è possibile utilizzare in una condizione, vedere: [Campi per filtrare i risultati di Macie](#), [Utilizzo degli operatori in condizioni](#), e [Specificare i valori per i campi](#).

Per creare una regola di filtro utilizzando AWS Command Line Interface (AWS CLI), esegui il [create-findings-filter](#) comando e specifica i valori appropriati per i parametri richiesti. Gli esempi seguenti creano una regola di filtro che restituisce tutti i dati sensibili rilevati nella versione corrente Regione AWS e riporta le occorrenze di informazioni personali (e nessun'altra categoria di dati sensibili) negli oggetti S3.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 create-findings-filter \
```

```
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={"criterion\":
{"classificationDetails.result.sensitiveData.category\":{"eqExactMatch\":
["PERSONAL_INFORMATION\"]}}}
```

Dove:

- *my_filter_rule* è il nome personalizzato per la regola.
- *criterion* è una mappa delle condizioni di filtro per la regola:
 - *classificationDetails.result.sensitiveData.category* è il nome JSON del campo della categoria di dati sensibili.
 - *eqExactMatch* specifica l'operatore equals exact match.
 - *PERSONAL_INFORMATION* è un valore enumerato per il campo Categoria di dati sensibili.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-aa2f-4940-b347-d1451example",
  "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

arn è l'Amazon Resource Name (ARN) della regola di filtro che è stata creata e *id* l'identificatore univoco della regola.

Per ulteriori esempi di criteri di filtro, consulta [Filtraggio dei risultati in modo programmatico con l'API Amazon Macie](#)

Applicazione di una regola di filtro ai risultati di Macie

Quando applichi una regola di filtro, Amazon Macie utilizza i criteri della regola per determinare quali risultati includere o escludere dalla visualizzazione dei risultati sulla console. Macie visualizza anche i criteri per aiutarti a determinare quali criteri hai applicato.

Tip

Sebbene le regole di filtro siano progettate per l'uso con la console Amazon Macie, puoi utilizzare i criteri di una regola per interrogare i dati dei risultati in modo programmatico con l'API Amazon Macie. A tale scopo, recupera i criteri di filtro per la regola, quindi aggiungi i criteri alla tua query. Per recuperare i criteri, utilizzare l'[GetFindingsFilter](#) operazione. Per identificare quindi i risultati che corrispondono ai criteri, utilizzate l'[ListFindings](#) operazione e specificate i criteri nella query. Per informazioni sulla specificazione dei criteri di filtro in una query, vedere [Creazione e applicazione di filtri ai risultati di Macie](#).

Per applicare una regola di filtro ai risultati

Segui questi passaggi per filtrare i risultati sulla console Amazon Macie applicando una regola di filtro.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Nell'elenco Regole salvate, scegli la regola di filtro che desideri applicare. Macie applica i criteri della regola e li visualizza nella casella Filtra criteri.
4. Per rifinire i criteri, utilizzate la casella Filtro criteri per aggiungere o rimuovere le condizioni di filtro. In tal caso, le modifiche non influiranno sulle impostazioni della regola. Macie salva le modifiche solo se le salvi esplicitamente come nuova regola.
5. Per applicare una regola di filtro diversa, ripeti il passaggio 3.

Dopo aver applicato una regola di filtro, puoi rimuovere rapidamente tutti i relativi criteri di filtro dalla tua visualizzazione. A tale scopo, scegli la X nella casella Criteri di filtro.

Modifica di una regola di filtro per i risultati di Macie

Dopo aver creato una regola di filtro, puoi perfezionarne i criteri e modificare altre impostazioni per la regola. Una regola di filtro è un insieme di criteri di filtro che crei e salvi per riutilizzarli quando esamini

i risultati sulla console Amazon Macie. Le regole di filtro possono aiutarti a eseguire analisi ripetute e coerenti di risultati con caratteristiche specifiche. Ogni regola è composta da un insieme di criteri di filtro, un nome e, facoltativamente, una descrizione.

Oltre a modificare i criteri di filtro o altre impostazioni di una regola, è possibile assegnare tag a una regola. Un tag è un'etichetta che definisci e assegni a determinati tipi di AWS risorse. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

Per modificare una regola di filtro per i risultati

Per assegnare tag o modificare le impostazioni di una regola di filtro, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per assegnare tag o modificare le impostazioni di una regola di filtro utilizzando la console Amazon Macie.

Per modificare una regola di filtro

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Nell'elenco delle regole salvate, scegli l'icona di modifica



accanto alla regola di filtro che desideri modificare o a cui assegnare i tag.

4. Effettua una delle seguenti operazioni:
 - Per modificare i criteri di filtro della regola, utilizza la casella Criteri di filtro. Nella casella, inserite le condizioni per i criteri desiderati. Per scoprire come, consulta [Creazione e applicazione di filtri ai risultati di Macie](#).
 - Per modificare il nome della regola, inserisci un nuovo nome nella casella Nome sotto Regola di filtro.
 - Per modificare la descrizione della regola, inserisci una nuova descrizione nella casella Descrizione sotto Regola di filtro.
 - Per assegnare tag alla regola, scegli Gestisci tag in Regola di filtro. Quindi aggiungi, rivedi e modifica i tag secondo necessità. Una regola può avere fino a 50 tag.

5. Una volta completate le modifiche, scegliere Save (Salva).

API

Per modificare una regola di filtro a livello di codice, utilizza il [UpdateFindingsFilter](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza i parametri supportati per specificare un nuovo valore per ogni impostazione che desideri modificare.

Per il `id` parametro, specifica l'identificatore univoco della regola da modificare. Puoi ottenere questo identificatore utilizzando l'[ListFindingsFilter](#) operazione per recuperare un elenco di regole di filtro e soppressione per il tuo account. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il [list-findings-filters](#) comando per recuperare questo elenco.

Per modificare una regola di filtro utilizzando il AWS CLI, esegui il [update-findings-filter](#) comando e utilizza i parametri supportati per specificare un nuovo valore per ogni impostazione che desideri modificare. Ad esempio, il comando seguente modifica il nome di una regola di filtro esistente.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --name personal_information_only
```

Dove:

- *9b2b4508-aa2f-4940-b347-d1451example* è l'identificatore univoco della regola.
- *personal_information_only* è il nuovo nome della regola.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-aa2f-4940-b347-d1451example",
  "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

`arn` è l'Amazon Resource Name (ARN) della regola che è stata modificata e `id` l'identificatore univoco della regola.

Analogamente, l'esempio seguente converte una regola di [soppressione in una regola](#) di filtro modificando il valore del parametro da `action ARCHIVE NOOP`

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --  
action NOOP
```

Dove:

- **8a1c3508-aa2f-4940-b347-d1451example** è l'identificatore univoco della regola.
- **NOOP** è la nuova azione che Macie deve eseguire sui risultati che soddisfano i criteri della regola: non eseguire alcuna azione (non sopprimere i risultati).

Se il comando viene eseguito correttamente, si ottiene un output simile al seguente:

```
{  
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-  
aa2f-4940-b347-d1451example",  
  "id": "8a1c3508-aa2f-4940-b347-d1451example"  
}
```

`arn` è l'Amazon Resource Name (ARN) della regola che è stata modificata e `id` l'identificatore univoco della regola.

Eliminazione di una regola di filtro per i risultati di Macie

Se crei una regola di filtro, puoi eliminarla in qualsiasi momento. Una regola di filtro è un insieme di criteri di filtro che crei e salvi per riutilizzarli quando esamini i risultati sulla console Amazon Macie. Se elimini una regola di filtro, la modifica non influisce sui risultati che corrispondono ai criteri della regola. Una regola di filtro determina solo quali risultati vengono visualizzati sulla console dopo l'applicazione della regola.

Per eliminare una regola di filtro per i risultati

Puoi eliminare una regola di filtro utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per eliminare una regola di filtro utilizzando la console Amazon Macie.

Per eliminare una regola di filtro

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>

2. Nel riquadro di navigazione, seleziona Esiti.
3. Nell'elenco delle regole salvate, scegli l'icona di modifica  accanto alla regola di filtro che desideri eliminare.
4. In Regola di filtro, scegli Elimina.

API

Per eliminare una regola di filtro a livello di codice, utilizza il [DeleteFindingsFilter](#) funzionamento dell'API Amazon Macie. Per il `id` parametro, specifica l'identificatore univoco per la regola di filtro da eliminare. Puoi ottenere questo identificatore utilizzando l'[ListFindingsFilter](#) operazione per recuperare un elenco di regole di filtro e soppressione per il tuo account. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il [list-findings-filters](#) comando per recuperare questo elenco.

Per eliminare una regola di filtro utilizzando il AWS CLI, esegui il [delete-findings-filter](#) comando. Per esempio:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

9b2b4508-aa2f-4940-b347-d1451example Dov'è l'identificatore univoco della regola di filtro da eliminare.

Se il comando viene eseguito correttamente, Macie restituisce una risposta HTTP 200 vuota. Altrimenti, Macie restituisce una risposta HTTP 4xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Analisi dei dati sensibili con i risultati di Macie

Quando esegui processi di rilevamento di dati sensibili o Amazon Macie esegue il rilevamento automatico di dati sensibili, Macie acquisisce i dettagli sulla posizione di ogni occorrenza di dati sensibili che trova negli oggetti Amazon Simple Storage Service (Amazon S3). Ciò include i dati sensibili che Macie rileva utilizzando identificatori di [dati gestiti e i dati che corrispondono ai criteri degli identificatori](#) di [dati personalizzati](#) che configuri per un job o Macie per l'utilizzo.

Con i dati sensibili rilevati, puoi esaminare questi dettagli per un massimo di 15 occorrenze di dati sensibili che Macie trova nei singoli oggetti S3. I dettagli forniscono informazioni sull'ampiezza delle

categorie e dei tipi di dati sensibili che specifici bucket e oggetti S3 potrebbero contenere. Possono aiutarti a localizzare le singole occorrenze di dati sensibili negli oggetti e a determinare se eseguire un'indagine più approfondita su bucket e oggetti specifici.

Per ulteriori informazioni, puoi facoltativamente configurare e utilizzare Macie per recuperare campioni di dati sensibili che Macie riporta nei singoli risultati. Gli esempi possono aiutarti a verificare la natura dei dati sensibili trovati da Macie. Possono anche aiutarti a personalizzare l'indagine su un bucket e un oggetto S3 interessati. Se scegli di recuperare campioni di dati sensibili per un risultato, Macie utilizza i dati del risultato per individuare da 1 a 10 occorrenze di ogni tipo di dato sensibile riportato dal risultato. Macie estrae quindi le occorrenze di dati sensibili dall'oggetto interessato e visualizza i dati affinché tu possa esaminarli.

Se un oggetto S3 contiene molte occorrenze di dati sensibili, una scoperta può anche aiutarti a navigare verso il corrispondente risultato della scoperta dei dati sensibili. A differenza di un rilevamento di dati sensibili, un risultato di rilevamento di dati sensibili fornisce dati dettagliati sulla posizione per un massimo di 1.000 occorrenze di ogni tipo di dati sensibili che Macie trova in un oggetto. Macie utilizza lo stesso schema per i dati sulla posizione nelle rilevazioni di dati sensibili e nei risultati della scoperta di dati sensibili. Per ulteriori informazioni sui risultati della scoperta di dati sensibili, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

Gli argomenti di questa sezione spiegano come individuare e, facoltativamente, recuperare le occorrenze di dati sensibili segnalati dai rilevamenti di dati sensibili. Spiegano inoltre lo schema utilizzato da Macie per segnalare la posizione delle singole occorrenze di dati sensibili rilevati da Macie.

Argomenti

- [Individuazione dei dati sensibili con i risultati di Macie](#)
- [Recupero di campioni di dati sensibili con i risultati di Macie](#)
- [Schema per la segnalazione della posizione dei dati sensibili](#)

Individuazione dei dati sensibili con i risultati di Macie

Quando esegui processi di rilevamento di dati sensibili o Amazon Macie esegue il rilevamento automatico di dati sensibili, Macie esegue un'ispezione approfondita della versione più recente di ogni oggetto Amazon Simple Storage Service (Amazon S3) che analizza. Per ogni esecuzione di lavoro o ciclo di analisi, Macie utilizza anche un algoritmo di ricerca approfondito per compilare i risultati risultanti con dettagli sulla posizione di occorrenze specifiche di dati sensibili che Macie trova negli

oggetti S3. Queste occorrenze forniscono informazioni sulle categorie e sui tipi di dati sensibili che un bucket e un oggetto S3 interessati potrebbero contenere. I dettagli possono aiutarti a individuare le singole occorrenze di dati sensibili negli oggetti e a determinare se eseguire un'indagine più approfondita su bucket e oggetti specifici.

Con i dati sensibili rilevati, puoi determinare la posizione di ben 15 occorrenze di dati sensibili che Macie ha trovato in un oggetto S3 interessato. Ciò include i dati sensibili rilevati da Macie utilizzando [identificatori di dati gestiti](#) e i dati che corrispondono ai criteri degli [identificatori di dati personalizzati che hai configurato per un job](#) o Macie per l'utilizzo.

Una ricerca di dati sensibili può fornire dettagli come:

- Il numero di colonna e di riga per una cella o un campo in una cartella di lavoro di Microsoft Excel, un file CSV o un file TSV.
- Il percorso di un campo o di una matrice in un file JSON o JSON Lines.
- Il numero di riga di una riga in un file di testo non binario diverso da un file CSV, JSON, JSON Lines o TSV, ad esempio un file HTML, TXT o XML.
- Il numero di pagina di una pagina in un file Adobe Portable Document Format (PDF).
- L'indice dei record e il percorso di un campo in un record in un contenitore di oggetti Apache Avro o in un file Apache Parquet.

Puoi accedere a questi dettagli utilizzando la console Amazon Macie o l'API Amazon Macie. Puoi anche accedere a questi dettagli nei risultati che Macie pubblica ad altri Servizi AWS, sia Amazon EventBridge che AWS Security Hub. Per maggiori informazioni sulle strutture JSON utilizzate da Macie per riportare questi dettagli, consulta [Schema per la segnalazione della posizione dei dati sensibili](#). Per informazioni su come accedere ai dettagli dei risultati che Macie pubblica ad altri, consulta [Servizi AWS Monitoraggio ed elaborazione dei risultati](#).

Se un oggetto S3 contiene molte occorrenze di dati sensibili, puoi anche utilizzare un risultato per accedere al corrispondente risultato della scoperta di dati sensibili. A differenza di un rilevamento di dati sensibili, un risultato di rilevamento di dati sensibili fornisce dati dettagliati sulla posizione per un massimo di 1.000 occorrenze di ogni tipo di dati sensibili che Macie ha trovato in un oggetto. Se un oggetto S3 è un file di archivio, ad esempio un file.tar o.zip, ciò include le occorrenze di dati sensibili nei singoli file che Macie ha estratto dall'archivio. (Macie non include queste informazioni nelle rilevazioni di dati sensibili.) Per ulteriori informazioni sui risultati della scoperta di dati sensibili, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#). Macie utilizza lo

stesso schema per i dati sulla posizione nelle rilevazioni di dati sensibili e nei risultati della scoperta di dati sensibili.

Per individuare i dati sensibili con i risultati

Per individuare le occorrenze di dati sensibili segnalati da un risultato, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Per eseguire questa operazione a livello di codice, usa l'operazione [GetFindings](#). Se un risultato include dettagli sulla posizione di una o più occorrenze di un tipo specifico di dati sensibili, `occurrences` gli oggetti del risultato forniscono tali dettagli. Per ulteriori informazioni, consulta [Schema per la segnalazione della posizione dei dati sensibili](#).

Per individuare le occorrenze di dati sensibili utilizzando la console, segui questi passaggi.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.

 Tip

Puoi visualizzare rapidamente tutti i risultati di un particolare processo di rilevamento di dati sensibili. A tale scopo, scegli Lavori nel riquadro di navigazione, quindi scegli il nome del lavoro. Nella parte superiore del pannello dei dettagli, scegli Mostra risultati, quindi scegli Mostra risultati.

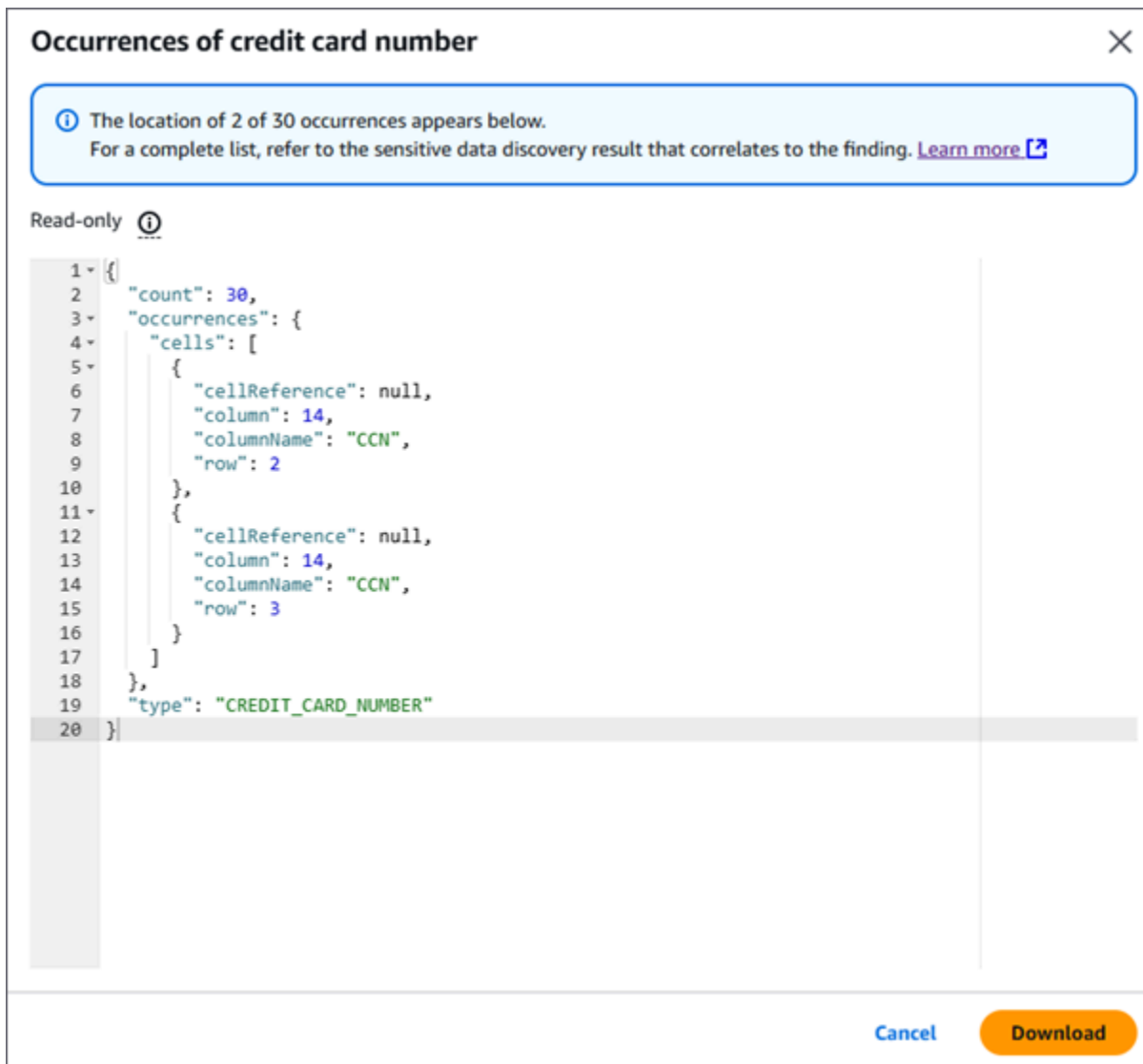
3. Nella pagina Risultati, scegli il risultato relativo ai dati sensibili che desideri individuare. Il pannello dei dettagli mostra le informazioni relative al risultato.
4. Nel pannello dei dettagli, scorri fino alla sezione Dati sensibili. Questa sezione fornisce informazioni sulle categorie e sui tipi di dati sensibili che Macie ha trovato nell'oggetto S3 interessato. Indica anche il numero di occorrenze di ogni tipo di dati sensibili rilevati da Macie.

Ad esempio, l'immagine seguente mostra alcuni dettagli di una scoperta che riporta 30 occorrenze di numeri di carte di credito, 20 occorrenze di nomi e 29 occorrenze di numeri di previdenza sociale degli Stati Uniti.

Financial information		
Credit card number	30	+ -
Personal information		
Name	20	+ -
Usa social security number	29	+ -

Se la scoperta include dettagli sulla posizione di una o più occorrenze di un tipo specifico di dati sensibili, il numero di occorrenze è un collegamento. Scegli il link per mostrare i dettagli. Macie apre una nuova finestra e visualizza i dettagli in formato JSON.

Ad esempio, l'immagine seguente mostra la posizione di due occorrenze di numeri di carta di credito in un oggetto S3 interessato.



Per salvare i dettagli come file JSON, scegli Scarica, quindi specifica un nome e una posizione per il file.

5. Per salvare tutti i dettagli del risultato come file JSON, scegli l'identificatore del risultato (Finding ID) nella parte superiore del pannello dei dettagli. Macie apre una nuova finestra e visualizza tutti i dettagli in formato JSON. Scegli Scarica, quindi specifica un nome e una posizione per il file.

Per accedere ai dettagli sulla posizione di ben 1.000 occorrenze di ogni tipo di dati sensibili nell'oggetto interessato, fate riferimento al corrispondente risultato della scoperta dei dati sensibili relativo al risultato. A tale scopo, scorrete fino all'inizio della sezione Dettagli del pannello. Quindi scegli il link nel campo Posizione dettagliata dei risultati. Macie apre la console Amazon S3 e visualizza il file o la cartella che contiene il risultato del rilevamento corrispondente.

Recupero di campioni di dati sensibili con i risultati di Macie

Per verificare la natura dei dati sensibili che Amazon Macie riporta nei risultati, puoi facoltativamente configurare e utilizzare Macie per recuperare e rivelare campioni di dati sensibili segnalati da singoli risultati. [Ciò include i dati sensibili che Macie rileva utilizzando identificatori di dati gestiti e i dati che corrispondono ai criteri degli identificatori di dati personalizzati.](#) Gli esempi possono aiutarti a personalizzare l'indagine su un oggetto e un bucket Amazon Simple Storage Service (Amazon S3) interessati.

Se recuperi e riveli campioni di dati sensibili per scopi di ricerca, Macie esegue le seguenti attività generali:

1. [Verifica che il risultato specifichi la posizione delle singole occorrenze di dati sensibili e la posizione del corrispondente risultato della scoperta di dati sensibili.](#)
2. Valuta il risultato del rilevamento dei dati sensibili corrispondente, verificando la validità dei metadati per l'oggetto S3 interessato e i dati sulla posizione per rilevare eventuali occorrenze di dati sensibili nell'oggetto.
3. Utilizzando i dati nel risultato del rilevamento dei dati sensibili, individua le prime 1-10 occorrenze di dati sensibili riportate dal risultato ed estrae i primi 1-128 caratteri di ogni occorrenza dall'oggetto S3 interessato. Se il risultato riporta più tipi di dati sensibili, Macie lo fa per un massimo di 100 tipi.
4. Crittografa i dati estratti con una chiave AWS Key Management Service (AWS KMS) specificata dall'utente.
5. Memorizza temporaneamente i dati crittografati in una cache e visualizza i dati per consentirne la revisione. I dati vengono crittografati in ogni momento, sia in transito che a riposo.
6. Subito dopo l'estrazione e la crittografia, elimina definitivamente i dati dalla cache, a meno che non sia temporaneamente necessaria una conservazione aggiuntiva per risolvere un problema operativo.

Se scegli di recuperare e rivelare campioni di dati sensibili da ritrovare, Macie ripete queste operazioni per localizzarli, estrarli, crittografarli, archivarli e infine eliminarli.

Macie non utilizza il [ruolo collegato al servizio Macie per il tuo account per eseguire](#) queste attività. Invece, usi la tua identità AWS Identity and Access Management (IAM) o consenti a Macie di assumere un ruolo IAM nel tuo account. Puoi recuperare e rivelare campioni di dati sensibili a scopo di ricerca se tu o il ruolo avete il permesso di accedere alle risorse e ai dati necessari ed eseguire le azioni richieste. [Tutte le azioni richieste vengono registrate. AWS CloudTrail](#)

Important

Ti consigliamo di limitare l'accesso a questa funzionalità utilizzando [policy IAM personalizzate](#). Per un ulteriore controllo degli accessi, ti consigliamo di creare anche uno strumento dedicato alla AWS KMS key crittografia dei campioni di dati sensibili che vengono recuperati e di limitare l'uso della chiave solo ai responsabili che devono essere autorizzati a recuperare e rivelare campioni di dati sensibili.

Per consigli ed esempi di politiche che potresti utilizzare per controllare l'accesso a questa funzionalità, consulta il seguente post sul blog sulla AWS sicurezza: [Come usare Amazon Macie per visualizzare in anteprima i dati sensibili nei bucket S3](#).

Gli argomenti di questa sezione spiegano come configurare e usare Macie per recuperare e rivelare campioni di dati sensibili da analizzare. Puoi eseguire queste attività in tutte le aree in Regioni AWS cui Macie è attualmente disponibile, ad eccezione delle regioni di Asia Pacifico (Osaka) e Israele (Tel Aviv).

Argomenti

- [Opzioni di configurazione per il recupero di campioni di dati sensibili con Macie](#)
- [Configurazione di Macie per recuperare campioni di dati sensibili](#)
- [Recupero di campioni di dati sensibili per una scoperta di Macie](#)

Opzioni di configurazione per il recupero di campioni di dati sensibili con Macie

Facoltativamente, puoi configurare e utilizzare Amazon Macie per recuperare e rivelare campioni di dati sensibili che Macie riporta nei singoli risultati. Se recuperi e riveli campioni di dati sensibili per una ricerca, Macie utilizza i dati nel corrispondente [risultato della scoperta dei dati sensibili](#) per individuare le occorrenze di dati sensibili nell'oggetto Amazon Simple Storage Service (Amazon S3) interessato. Macie estrae quindi campioni di tali occorrenze dall'oggetto interessato. Macie crittografa i dati estratti con una chiave AWS Key Management Service (AWS KMS) specificata dall'utente, archivia temporaneamente i dati crittografati in una cache e restituisce i dati nei risultati per la ricerca. Subito dopo l'estrazione e la crittografia, Macie elimina definitivamente i dati dalla cache, a meno che non sia temporaneamente necessaria una conservazione aggiuntiva per risolvere un problema operativo.

Macie non utilizza il [ruolo collegato al servizio Macie](#) per l'account per individuare, recuperare, crittografare o rivelare campioni di dati sensibili per gli oggetti S3 interessati. Macie utilizza invece le

impostazioni e le risorse che configuri per il tuo account. Quando configuri le impostazioni in Macie, specifichi come accedere agli oggetti S3 interessati. È inoltre necessario specificare quale utilizzare AWS KMS key per crittografare i campioni. Puoi configurare le impostazioni in tutte le aree in Regioni AWS cui Macie è attualmente disponibile, ad eccezione delle regioni Asia Pacifico (Osaka) e Israele (Tel Aviv).

Per accedere agli oggetti S3 interessati e recuperare campioni di dati sensibili da essi, hai due opzioni. Puoi configurare Macie per utilizzare le credenziali utente AWS Identity and Access Management (IAM) o assumere un ruolo IAM:

- **Usa le credenziali utente IAM:** con questa opzione, ogni utente del tuo account utilizza la propria identità IAM individuale per individuare, recuperare, crittografare e rivelare gli esempi. Ciò significa che un utente può recuperare e rivelare campioni di dati sensibili a fini di ricerca se è autorizzato ad accedere alle risorse e ai dati necessari ed eseguire le azioni richieste.
- **Assumi un ruolo IAM:** con questa opzione, crei un ruolo IAM che delega l'accesso a Macie. Ti assicuri inoltre che le politiche di fiducia e autorizzazioni per il ruolo soddisfino tutti i requisiti necessari per l'assunzione del ruolo da parte di Macie. Macie assume quindi il ruolo quando un utente del tuo account sceglie di individuare, recuperare, crittografare e rivelare campioni di dati sensibili a scopo di ricerca.

Puoi utilizzare entrambe le configurazioni con qualsiasi tipo di account Macie: l'account amministratore Macie delegato per un'organizzazione, un account membro Macie in un'organizzazione o un account Macie autonomo.

Nei seguenti argomenti vengono illustrate le opzioni, i requisiti e le considerazioni che possono aiutarti a determinare come configurare le impostazioni e le risorse per il tuo account. Ciò include le politiche di fiducia e autorizzazioni da collegare a un ruolo IAM. Per ulteriori consigli ed esempi di politiche che potresti utilizzare per recuperare e rivelare campioni di dati sensibili, consulta il seguente post sul blog sulla AWS sicurezza: [Come usare Amazon Macie per visualizzare in anteprima i dati sensibili nei bucket S3](#).

Argomenti

- [Determinazione del metodo di accesso da utilizzare](#)
- [Utilizzo delle credenziali utente IAM per accedere agli oggetti S3 interessati](#)
- [Assumendo un ruolo IAM per accedere agli oggetti S3 interessati](#)
- [Configurazione di un ruolo IAM per accedere agli oggetti S3 interessati](#)
- [Decrittografia degli oggetti S3 interessati](#)

Determinazione del metodo di accesso da utilizzare

Nel determinare la configurazione migliore per il proprio AWS ambiente, una considerazione fondamentale è se l'ambiente include più account Amazon Macie gestiti centralmente come organizzazione. Se sei l'amministratore Macie delegato di un'organizzazione, la configurazione di Macie per l'assunzione di un ruolo IAM può semplificare il recupero di campioni di dati sensibili dagli oggetti S3 interessati per gli account dell'organizzazione. Con questo approccio, crei un ruolo IAM nel tuo account amministratore. Inoltre, crei un ruolo IAM in ogni account membro applicabile. Il ruolo nel tuo account amministratore delega l'accesso a Macie. Il ruolo in un account membro delega l'accesso tra account diversi al ruolo nel tuo account amministratore. Se implementato, puoi quindi utilizzare il concatenamento dei ruoli per accedere agli oggetti S3 interessati per i tuoi account membro.

Considera anche chi ha accesso diretto ai singoli risultati per impostazione predefinita. Per recuperare e rivelare campioni di dati sensibili relativi a un risultato, un utente deve prima avere accesso al risultato:

- **Lavori di rilevamento di dati sensibili:** solo l'account che crea un lavoro può accedere ai risultati prodotti dal lavoro. Se disponi di un account amministratore Macie, puoi configurare un job per analizzare gli oggetti nei bucket S3 per qualsiasi account della tua organizzazione. Pertanto, i tuoi lavori possono produrre risultati per gli oggetti contenuti nei bucket di proprietà dei tuoi account membro. Se disponi di un account membro o di un account Macie autonomo, puoi configurare un processo per analizzare gli oggetti solo nei bucket di proprietà del tuo account.
- **Rilevamento automatico dei dati sensibili:** solo l'account amministratore di Macie può accedere ai risultati prodotti dal rilevamento automatico per gli account della propria organizzazione. Gli account dei membri non possono accedere a questi risultati. Se disponi di un account Macie indipendente, puoi accedere ai risultati che il rilevamento automatico produce solo per il tuo account.

Se prevedi di accedere agli oggetti S3 interessati utilizzando un ruolo IAM, considera anche quanto segue:

- Per individuare le occorrenze di dati sensibili in un oggetto, il risultato della scoperta dei dati sensibili corrispondente a un risultato deve essere archiviato in un oggetto S3 firmato da Macie con un Message Authentication Code (HMAC) basato su Hash. AWS KMS key Macie deve essere in grado di verificare l'integrità e l'autenticità del risultato della scoperta dei dati sensibili. Altrimenti, Macie non assumerà il ruolo di IAM per recuperare campioni di dati sensibili. Si tratta di una barriera aggiuntiva per limitare l'accesso ai dati negli oggetti S3 per un account.

- Per recuperare campioni di dati sensibili da un oggetto crittografato e gestito da un cliente AWS KMS key, è necessario consentire al ruolo IAM di decrittografare i dati con la chiave. Più specificamente, la policy della chiave deve consentire al ruolo di eseguire l'azione. `kms:Decrypt`. Per altri tipi di crittografia lato server, non sono necessarie autorizzazioni o risorse aggiuntive per decrittografare un oggetto interessato. Per ulteriori informazioni, consulta [Decrittografia degli oggetti S3 interessati](#).
- Per recuperare campioni di dati sensibili da un oggetto per un altro account, devi attualmente essere l'amministratore Macie delegato per l'account nell'elenco applicabile. Regione AWS Inoltre:
 - Macie deve essere attualmente abilitato per l'account membro nella regione applicabile.
 - L'account membro deve avere un ruolo IAM che delega l'accesso tra account diversi a un ruolo IAM nell'account amministratore di Macie. Il nome del ruolo deve essere lo stesso nell'account amministratore Macie e nell'account membro.
 - La politica di fiducia per il ruolo IAM nell'account membro deve includere una condizione che specifichi l'ID esterno corretto per la configurazione. Questo ID è una stringa alfanumerica unica che Macie genera automaticamente dopo aver configurato le impostazioni per l'account amministratore Macie. Per informazioni sull'utilizzo di policy di trust esterne IDs, consulta [Accesso ai contenuti di Account AWS proprietà di terze parti nella Guida](#) per l'utente AWS Identity and Access Management
- Se il ruolo IAM nell'account membro soddisfa tutti i requisiti di Macie, non è necessario che l'account membro configuri e abiliti le impostazioni di Macie per recuperare campioni di dati sensibili dagli oggetti relativi all'account. Macie utilizza solo le impostazioni e il ruolo IAM nell'account amministratore Macie e il ruolo IAM nell'account membro.

 Tip

Se il tuo account fa parte di un'organizzazione di grandi dimensioni, prendi in considerazione l'utilizzo di un AWS CloudFormation modello e di un set di stack per fornire e gestire i ruoli IAM per gli account dei membri della tua organizzazione. Per informazioni sulla creazione e l'utilizzo di modelli e set di stack, consulta la Guida per [l'AWS CloudFormation utente](#).

Per esaminare e, facoltativamente, scaricare un CloudFormation modello che possa fungere da punto di partenza, puoi utilizzare la console Amazon Macie. Nel pannello di navigazione della console, in Impostazioni, scegli Reveal samples. Scegli Modifica, quindi scegli Visualizza le autorizzazioni e il CloudFormation modello del ruolo del membro.

Gli argomenti successivi di questa sezione forniscono dettagli e considerazioni aggiuntivi per ogni tipo di configurazione. Per i ruoli IAM, ciò include le politiche di fiducia e autorizzazioni da associare a un ruolo. Se non sei sicuro del tipo di configurazione migliore per il tuo ambiente, chiedi assistenza AWS all'amministratore.

Utilizzo delle credenziali utente IAM per accedere agli oggetti S3 interessati

Se configuri Amazon Macie per recuperare campioni di dati sensibili utilizzando le credenziali utente IAM, ogni utente del tuo account Macie utilizza la propria identità IAM per individuare, recuperare, crittografare e rivelare campioni per singoli risultati. Ciò significa che un utente può recuperare e rivelare campioni di dati sensibili per verificare se la sua identità IAM è autorizzata ad accedere alle risorse e ai dati necessari ed eseguire le azioni necessarie. [Tutte le azioni richieste vengono registrate. AWS CloudTrail](#)

Per recuperare e rivelare campioni di dati sensibili per un particolare risultato, a un utente deve essere consentito di accedere ai seguenti dati e risorse: il risultato, il corrispondente risultato della scoperta dei dati sensibili, il bucket S3 interessato e l'oggetto S3 interessato. È inoltre necessario consentire loro di utilizzare AWS KMS key quello che è stato utilizzato per crittografare l'oggetto interessato, se applicabile, e AWS KMS key quello che Macie è stato configurato per utilizzare per crittografare campioni di dati sensibili. Se alcune policy IAM, policy di risorse o altre impostazioni di autorizzazione negano l'accesso richiesto, l'utente non sarà in grado di recuperare e rivelare gli esempi del risultato.

Per configurare questo tipo di configurazione, completa le seguenti attività generali:

1. Verifica di aver configurato un repository per i risultati del rilevamento dei dati sensibili.
2. Configuralo AWS KMS key da utilizzare per la crittografia di campioni di dati sensibili.
3. Verifica le tue autorizzazioni per configurare le impostazioni in Macie.
4. Configura e abilita le impostazioni in Macie.

Per informazioni sull'esecuzione di queste attività, consulta [Configurazione di Macie per recuperare campioni di dati sensibili](#).

Assumendo un ruolo IAM per accedere agli oggetti S3 interessati

Per configurare Amazon Macie per recuperare campioni di dati sensibili assumendo un ruolo IAM, inizia creando un ruolo IAM che deleghi l'accesso ad Amazon Macie. Assicurati che le politiche di fiducia e autorizzazioni per il ruolo soddisfino tutti i requisiti necessari per l'assunzione del

ruolo da parte di Macie. Quando un utente del tuo account Macie sceglie quindi di recuperare e rivelare campioni di dati sensibili per una ricerca, Macie si assume il ruolo di recuperare i campioni dall'oggetto S3 interessato. Macie assume il ruolo solo quando un utente sceglie di recuperare e rivelare i campioni per un risultato. Per assumere il ruolo, Macie utilizza il [AssumeRole](#) funzionamento dell'API (). AWS Security Token Service AWS STS Tutte le azioni richieste vengono [registrate](#). AWS CloudTrail

Per recuperare e rivelare campioni di dati sensibili relativi a un particolare risultato, a un utente deve essere consentito di accedere al risultato della scoperta, al corrispondente risultato della scoperta dei dati sensibili e ai dati configurati da Macie per crittografare i campioni di dati sensibili. AWS KMS key Il ruolo IAM deve consentire a Macie di accedere al bucket S3 e all'oggetto S3 interessato. Il ruolo deve inoltre essere autorizzato a utilizzare AWS KMS key ciò che è stato utilizzato per crittografare l'oggetto interessato, se applicabile. Se le politiche IAM, le politiche delle risorse o altre impostazioni di autorizzazione negano l'accesso richiesto, l'utente non sarà in grado di recuperare e rivelare gli esempi del risultato.

Per configurare questo tipo di configurazione, completa le seguenti attività generali. Se disponi di un account membro in un'organizzazione, collabora con l'amministratore di Macie per determinare se e come configurare le impostazioni e le risorse per il tuo account.

1. Definisci quanto segue:

- Il nome del ruolo IAM che vuoi che Macie assuma. Se il tuo account fa parte di un'organizzazione, questo nome deve essere lo stesso per l'account amministratore Macie delegato e per ogni account membro applicabile dell'organizzazione. In caso contrario, l'amministratore Macie non sarà in grado di accedere agli oggetti S3 interessati per un account membro applicabile.
- Il nome della policy di autorizzazione IAM da allegare al ruolo IAM. Se il tuo account fa parte di un'organizzazione, ti consigliamo di utilizzare lo stesso nome di policy per ogni account membro applicabile nell'organizzazione. Questo può semplificare il provisioning e la gestione del ruolo negli account dei membri.

2. Verifica di aver configurato un repository per i risultati del rilevamento dei dati sensibili.

3. Configuralo AWS KMS key da utilizzare per la crittografia di campioni di dati sensibili.

4. Verifica le tue autorizzazioni per la creazione di ruoli IAM e la configurazione delle impostazioni in Macie.

5. Se sei l'amministratore Macie delegato di un'organizzazione o hai un account Macie autonomo:

- a. Crea e configura il ruolo IAM per il tuo account. Assicurati che le politiche di fiducia e autorizzazioni per il ruolo soddisfino tutti i requisiti necessari per l'assunzione del ruolo da parte di Macie. Per informazioni dettagliate su questi requisiti, consulta l'argomento [successivo](#).
 - b. Configura e abilita le impostazioni in Macie. Macie genera quindi un ID esterno per la configurazione. Se sei l'amministratore Macie di un'organizzazione, prendi nota di questo ID. La politica di fiducia per il ruolo IAM in ciascuno degli account membro applicabili deve specificare questo ID.
6. Se disponi di un account membro in un'organizzazione:
- a. Chiedi all'amministratore di Macie l'ID esterno da specificare nella policy di fiducia per il ruolo IAM nel tuo account. Verifica anche il nome del ruolo IAM e la politica di autorizzazione da creare.
 - b. Crea e configura il ruolo IAM per il tuo account. Assicurati che le politiche di fiducia e autorizzazioni per il ruolo soddisfino tutti i requisiti per l'assunzione del ruolo da parte dell'amministratore Macie. Per informazioni dettagliate su questi requisiti, consulta l'argomento [successivo](#).
 - c. (Facoltativo) Se desideri recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati per il tuo account, configura e abilita le impostazioni in Macie. Se vuoi che Macie assuma un ruolo IAM per recuperare gli esempi, inizia creando e configurando un ruolo IAM aggiuntivo nel tuo account. Assicurati che le politiche di fiducia e autorizzazioni per questo ruolo aggiuntivo soddisfino tutti i requisiti necessari affinché Macie possa assumere il ruolo. Quindi configura le impostazioni in Macie e specifica il nome di questo ruolo aggiuntivo. Per informazioni dettagliate sui requisiti politici per il ruolo, consulta l'[argomento successivo](#).

Per informazioni sull'esecuzione di queste attività, vedere [Configurazione di Macie per recuperare campioni di dati sensibili](#).

Configurazione di un ruolo IAM per accedere agli oggetti S3 interessati

Per accedere agli oggetti S3 interessati utilizzando un ruolo IAM, inizia creando e configurando un ruolo che deleghi l'accesso ad Amazon Macie. Assicurati che le politiche di fiducia e autorizzazioni per il ruolo soddisfino tutti i requisiti necessari per l'assunzione del ruolo da parte di Macie. Il modo in cui esegui questa operazione dipende dal tipo di account Macie che possiedi.

Le sezioni seguenti forniscono dettagli sulle politiche di fiducia e autorizzazioni da associare al ruolo IAM per ogni tipo di account Macie. Scegli la sezione relativa al tipo di account che possiedi.

 Note

Se disponi di un account membro in un'organizzazione, potresti dover creare e configurare due ruoli IAM per il tuo account:

- Per consentire all'amministratore Macie di recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati per il tuo account, crea e configura un ruolo che l'account dell'amministratore possa assumere. Per questi dettagli, scegli la sezione Account membro Macie.
- Per recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati per il tuo account, crea e configura un ruolo che Macie possa assumere. Per questi dettagli, scegli la sezione Account Macie standalone.

Prima di creare e configurare uno dei ruoli IAM, collabora con l'amministratore di Macie per determinare la configurazione appropriata per il tuo account.

Per informazioni dettagliate sull'utilizzo di IAM per creare il ruolo, consulta [Creazione di un ruolo utilizzando politiche di fiducia personalizzate](#) nella Guida per l'AWS Identity and Access Management utente.

Account amministratore Macie

Se sei l'amministratore Macie delegato di un'organizzazione, inizia utilizzando l'editor delle politiche IAM per creare la politica di autorizzazione per il ruolo IAM. La politica dovrebbe essere la seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RetrieveS3Objects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    },
    {
```

```

        "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
        "Effect": "Allow",
        "Action": [
            "sts:AssumeRole"
        ],
        "Resource": "arn:aws:iam::*:role/IAMRoleName"
    }
}

```

IAMRoleName Dov'è il nome del ruolo IAM che Macie deve assumere quando recupera campioni di dati sensibili dagli oggetti S3 interessati per gli account dell'organizzazione. Sostituisci questo valore con il nome del ruolo che stai creando per il tuo account e che intendi creare per gli account membro applicabili nella tua organizzazione. Questo nome deve essere lo stesso per il tuo account amministratore Macie e per ogni account membro applicabile.

Note

Nella precedente politica di autorizzazione, l'elemento della prima istruzione utilizza un carattere jolly (*). Ciò consente a un'entità IAM collegata di recuperare oggetti da tutti i bucket S3 di proprietà dell'organizzazione. Per consentire questo accesso solo per bucket specifici, sostituisci il carattere jolly con l'Amazon Resource Name (ARN) di ogni bucket. Ad esempio, per consentire l'accesso solo agli oggetti in un bucket denominato amzn-s3-demo-bucket1, cambia l'elemento in:

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
```

Puoi anche limitare l'accesso agli oggetti in bucket S3 specifici per singoli account. Per fare ciò, specifica il bucket ARNs nell'elemento della politica di autorizzazione per il ruolo IAM in ogni account applicabile. Per ulteriori informazioni ed esempi, consulta [IAM JSON Policy elements: Resource](#) in the AWS Identity and Access Management User Guide.

Dopo aver creato la politica di autorizzazione per il ruolo IAM, crea e configura il ruolo. Se lo fai utilizzando la console IAM, scegli Custom trust policy come tipo di entità affidabile per il ruolo. Per la policy di fiducia che definisce le entità attendibili per il ruolo, specifica quanto segue.

```

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

```



```

        "Sid": "AllowMacieReveal",
        "Effect": "Allow",
        "Principal": {
            "Service": "reveal-samples.macie.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
        }
    }
]
}

```

accountID Dov'è l'ID dell'account per il tuo Account AWS. Sostituisci questo valore con l'ID del tuo account a 12 cifre.

Nella precedente politica di fiducia:

- L'Elemento **Principal** specifica il servizio principale che Macie utilizza per recuperare campioni di dati sensibili dagli oggetti S3 interessati, `reveal-samples.macie.amazonaws.com`
- L'Elemento **Action** specifica l'azione che il responsabile del servizio è autorizzato a eseguire, il [AssumeRole](#) funzionamento dell'API (). AWS Security Token Service AWS STS
- L'Elemento **Condition** definisce una condizione che utilizza la chiave di contesto [aws:SourceAccount](#) global condition. Questa condizione determina quale account può eseguire l'azione specificata. In questo caso, consente a Macie di assumere il ruolo solo per l'account specificato (*accountID*). Questa condizione aiuta a evitare che Macie venga usato come [agente confuso](#) durante le transazioni con AWS STS

Dopo aver definito la politica di fiducia per il ruolo IAM, collega la politica di autorizzazione al ruolo. Questa dovrebbe essere la politica di autorizzazioni che hai creato prima di iniziare a creare il ruolo. Quindi completa i passaggi rimanenti in IAM per completare la creazione e la configurazione del ruolo. Al termine, [configura e abilita le impostazioni in Macie](#).

Account membro Macie

Se disponi di un account membro Macie e desideri consentire al tuo amministratore Macie di recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati per il tuo account, inizia chiedendo all'amministratore Macie le seguenti informazioni:

- Il nome del ruolo IAM da creare. Il nome deve essere lo stesso per il tuo account e per l'account amministratore Macie della tua organizzazione.
- Il nome della policy di autorizzazione IAM da allegare al ruolo.
- L'ID esterno da specificare nella politica di fiducia per il ruolo. Questo ID deve essere l'ID esterno generato da Macie per la configurazione dell'amministratore di Macie.

Dopo aver ricevuto queste informazioni, utilizza l'editor delle politiche IAM per creare la politica di autorizzazione per il ruolo. La politica dovrebbe essere la seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RetrieveS3Objects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La politica di autorizzazione precedente consente a un'entità IAM collegata di recuperare oggetti da tutti i bucket S3 del tuo account. Questo perché l'elemento della policy utilizza un carattere jolly (*). Per consentire questo accesso solo per bucket specifici, sostituisci il carattere jolly con l'Amazon Resource Name (ARN) di ogni bucket. Ad esempio, per consentire l'accesso solo agli oggetti in un bucket denominato amzn-s3-demo-bucket2, cambia l'elemento in:

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket2/*"
```

Per ulteriori informazioni ed esempi, consulta [IAM JSON Policy elements: Resource](#) in the AWS Identity and Access Management User Guide.

Dopo aver creato la politica di autorizzazione per il ruolo IAM, crea il ruolo. Se crei il ruolo utilizzando la console IAM, scegli Custom trust policy come tipo di entità affidabile per il ruolo. Per la politica di fiducia che definisce le entità attendibili per il ruolo, specifica quanto segue.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "externalID",
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

Nella politica precedente, sostituisci i valori segnaposto con i valori corretti per il tuo AWS ambiente, dove:

- *administratorAccountID* è l'ID dell'account a 12 cifre per l'account dell'amministratore di Macie.
- *IAMRoleName* è il nome del ruolo IAM nell'account dell'amministratore di Macie. Dovrebbe essere il nome che hai ricevuto dall'amministratore di Macie.
- *externalID* è l'ID esterno che hai ricevuto dall'amministratore di Macie.

In generale, la politica di fiducia consente all'amministratore Macie di assumere il ruolo di recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati per il tuo account. L'Principale elemento specifica l'ARN di un ruolo IAM nell'account dell'amministratore di Macie. Questo è il ruolo che l'amministratore Macie utilizza per recuperare e rivelare campioni di dati sensibili per gli account della tua organizzazione. Il Condition blocco definisce due condizioni che determinano ulteriormente chi può assumere il ruolo:

- La prima condizione specifica un ID esterno univoco per la configurazione dell'organizzazione. Per ulteriori informazioni sugli elementi esterni IDs, consulta [Accesso ai dati Account AWS di proprietà di terzi](#) nella Guida per l'AWS Identity and Access Management utente.

- La seconda condizione utilizza la chiave di contesto della condizione globale [aws: PrincipalOrgID](#). Il valore della chiave è una variabile dinamica che rappresenta l'identificatore univoco di un'organizzazione in AWS Organizations (`${aws:ResourceOrgID}`). La condizione limita l'accesso solo agli account che fanno parte della stessa organizzazione in AWS Organizations. Se sei entrato a far parte della tua organizzazione accettando un invito su Macie, rimuovi questa condizione dalla politica.

Dopo aver definito la politica di fiducia per il ruolo IAM, collega la politica di autorizzazione al ruolo. Questa dovrebbe essere la politica di autorizzazioni che hai creato prima di iniziare a creare il ruolo. Quindi completa i passaggi rimanenti in IAM per completare la creazione e la configurazione del ruolo. Non configurate né inserite le impostazioni per il ruolo in Macie.

Account Macie autonomo

Se disponi di un account Macie indipendente o di un account membro Macie e desideri recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati per il tuo account, inizia a utilizzare l'editor delle politiche di IAM per creare la politica di autorizzazione per il ruolo IAM. La politica dovrebbe essere la seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RetrieveS3Objects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Nella precedente politica di autorizzazione, l'`Resource` elemento utilizza un carattere jolly (*). Ciò consente a un'entità IAM collegata di recuperare oggetti da tutti i bucket S3 del tuo account. Per consentire questo accesso solo per bucket specifici, sostituisci il carattere jolly con l'Amazon Resource Name (ARN) di ogni bucket. Ad esempio, per consentire l'accesso solo agli oggetti in un bucket denominato `amzn-s3-demo-bucket3`, cambia l'elemento in:

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket3/*"
```

Per ulteriori informazioni ed esempi, consulta [IAM JSON Policy elements: Resource](#) in the AWS Identity and Access Management User Guide.

Dopo aver creato la politica di autorizzazione per il ruolo IAM, crea il ruolo. Se crei il ruolo utilizzando la console IAM, scegli Custom trust policy come tipo di entità affidabile per il ruolo. Per la politica di fiducia che definisce le entità attendibili per il ruolo, specifica quanto segue.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMacieReveal",
      "Effect": "Allow",
      "Principal": {
        "Service": "reveal-samples.macie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        }
      }
    }
  ]
}
```

accountID Dov'è l'ID dell'account per il tuo Account AWS. Sostituisci questo valore con l'ID del tuo account a 12 cifre.

Nella precedente politica di fiducia:

- L'elemento **Principal** specifica il servizio principale che Macie utilizza per recuperare e rivelare campioni di dati sensibili dagli oggetti S3 interessati, `reveal-samples.macie.amazonaws.com`
- L'elemento **Action** specifica l'azione che il responsabile del servizio è autorizzato a eseguire, il funzionamento dell'[AssumeRole](#) API (). AWS Security Token Service AWS STS
- L'elemento **Condition** definisce una condizione che utilizza la chiave di contesto [aws:SourceAccount](#) global condition. Questa condizione determina quale account può eseguire l'azione specificata. Consente a Macie di assumere il ruolo solo per l'account specificato (*accountID*).

Questa condizione aiuta a evitare che Macie venga usato come [agente confuso](#) durante le transazioni con. AWS STS

Dopo aver definito la politica di fiducia per il ruolo IAM, collega la politica di autorizzazione al ruolo. Questa dovrebbe essere la politica di autorizzazioni che hai creato prima di iniziare a creare il ruolo. Quindi completa i passaggi rimanenti in IAM per completare la creazione e la configurazione del ruolo. Al termine, [configura e abilita le impostazioni in Macie](#).

Decrittografia degli oggetti S3 interessati

Amazon S3 supporta diverse opzioni di crittografia per oggetti S3. Per la maggior parte di queste opzioni, non sono necessarie risorse o autorizzazioni aggiuntive affinché un utente o un ruolo IAM possa decrittografare e recuperare campioni di dati sensibili da un oggetto interessato. Questo è il caso di un oggetto crittografato utilizzando la crittografia lato server con una chiave gestita Amazon S3 o una chiave gestita. AWS AWS KMS key

Tuttavia, se un oggetto S3 è crittografato con un oggetto gestito dal cliente AWS KMS key, sono necessarie autorizzazioni aggiuntive per decrittografare e recuperare campioni di dati sensibili dall'oggetto. Più specificamente, la policy chiave per la chiave KMS deve consentire all'utente o al ruolo IAM di eseguire l'azione. kms :Decrypt In caso contrario, si verifica un errore e Amazon Macie non recupera alcun campione dall'oggetto. Per sapere come fornire questo accesso a un utente IAM, consulta [l'accesso e le autorizzazioni delle chiavi KMS](#) nella Guida per gli sviluppatori.AWS Key Management Service

Il modo in cui fornire questo accesso per un ruolo IAM dipende dal fatto che l'account proprietario possieda AWS KMS key anche il ruolo:

- Se lo stesso account possiede la chiave KMS e il ruolo, un utente dell'account deve aggiornare la politica della chiave.
- Se un account possiede la chiave KMS e un altro account possiede il ruolo, un utente dell'account che possiede la chiave deve consentire l'accesso alla chiave da più account.

Questo argomento descrive come eseguire queste attività per un ruolo IAM che hai creato per recuperare campioni di dati sensibili dagli oggetti S3. Fornisce inoltre esempi per entrambi gli scenari. Per informazioni su come consentire l'accesso ai servizi gestiti dal cliente AWS KMS keys per altri scenari, consulta [l'accesso e le autorizzazioni con chiave KMS nella Guida](#) per gli AWS Key Management Service sviluppatori.

Consentire l'accesso dello stesso account a una chiave gestita dal cliente

Se lo stesso account possiede AWS KMS key sia il ruolo che quello IAM, un utente dell'account deve aggiungere una dichiarazione alla policy della chiave. L'istruzione aggiuntiva deve consentire al ruolo IAM di decrittografare i dati utilizzando la chiave. Per informazioni dettagliate sull'aggiornamento di una policy chiave, consulta [Changing a key policy](#) nella AWS Key Management Service Developer Guide.

Nella dichiarazione:

- L'Principal elemento deve specificare l'Amazon Resource Name (ARN) del ruolo IAM.
- L'Action array deve specificare l'`kms:Decrypt` azione. Questa è l'unica AWS KMS azione che il ruolo IAM deve essere autorizzato a eseguire per decrittografare un oggetto crittografato con la chiave.

Di seguito è riportato un esempio dell'istruzione da aggiungere alla politica per una chiave KMS.

```
{
  "Sid": "Allow the Macie reveal role to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Nell'esempio precedente:

- Il `AWS` campo nell'Principal elemento specifica l'ARN del ruolo IAM nell'account. Consente al ruolo di eseguire l'azione specificata dalla dichiarazione politica. *123456789012* è un esempio di ID di account. Sostituisci questo valore con l'ID dell'account che possiede il ruolo e la chiave KMS. *IAMRoleName* è un nome di esempio. Sostituisci questo valore con il nome del ruolo IAM nell'account.
- L'Action array specifica l'azione che il ruolo IAM può eseguire utilizzando la chiave KMS: decrittografare il testo cifrato crittografato con la chiave.

La posizione in cui si aggiunge questa dichiarazione a una politica chiave dipende dalla struttura e dagli elementi attualmente contenuti nella politica. Quando aggiungete l'istruzione, assicuratevi che la sintassi sia valida. Le politiche chiave utilizzano il formato JSON. Ciò significa che è necessario aggiungere anche una virgola prima o dopo l'istruzione, a seconda di dove si aggiunge l'istruzione alla politica.

Consentire l'accesso tra più account a una chiave gestita dal cliente

Se un account possiede il AWS KMS key (proprietario della chiave) e un altro account possiede il ruolo IAM (proprietario del ruolo), il proprietario della chiave deve fornire al proprietario del ruolo l'accesso alla chiave da più account. Un modo per farlo è utilizzare una sovvenzione. Una sovvenzione è uno strumento politico che consente ai AWS committenti di utilizzare le chiavi KMS nelle operazioni crittografiche se le condizioni specificate dalla concessione sono soddisfatte. Per maggiori informazioni sulle sovvenzioni, consulta [Grants nella AWS KMS](#) Developer Guide. AWS Key Management Service

Con questo approccio, il proprietario della chiave si assicura innanzitutto che la politica della chiave consenta al proprietario del ruolo di creare una concessione per la chiave. Il proprietario del ruolo crea quindi una concessione per la chiave. La concessione delega le autorizzazioni pertinenti al ruolo IAM nel loro account. Consente al ruolo di decrittografare gli oggetti S3 crittografati con la chiave.

Fase 1: Aggiornare la politica chiave

Nella policy chiave, il proprietario della chiave deve assicurarsi che la policy includa una dichiarazione che consenta al proprietario del ruolo di creare una sovvenzione per il ruolo IAM nel proprio account (del proprietario del ruolo). In questa dichiarazione, l'Principal elemento deve specificare l'ARN dell'account del proprietario del ruolo. L'Action array deve specificare l'kms:CreateGrant azione. Un Condition blocco può filtrare l'accesso all'azione specificata. Di seguito è riportato un esempio di questa dichiarazione nella politica per una chiave KMS.

```
{
  "Sid": "Allow a role in an account to create a grant",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:CreateGrant"
  ],
  "Resource": "*",
```



```
"Condition": {
  "StringEquals": {
    "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
  },
  "ForAllValues:StringEquals": {
    "kms:GrantOperations": "Decrypt"
  }
}
```

Nell'esempio precedente:

- Il AWS campo nell'Principale elemento specifica l'ARN dell'account del proprietario del ruolo. Consente all'account di eseguire l'azione specificata dalla dichiarazione politica. **111122223333** è un esempio di ID di account. Sostituisci questo valore con l'ID dell'account del proprietario del ruolo.
- L'Action array specifica l'azione che il proprietario del ruolo è autorizzato a eseguire sulla chiave KMS: creare una concessione per la chiave.
- Il Condition blocco utilizza [gli operatori di condizione](#) e le seguenti chiavi di condizione per filtrare l'accesso all'azione che il proprietario del ruolo è autorizzato a eseguire sulla chiave KMS:
 - [kms: GranteePrincipal](#) — Questa condizione consente al proprietario del ruolo di creare una concessione solo per il beneficiario principale specificato, che è l'ARN del ruolo IAM nel proprio account. In quell'ARN, **111122223333** c'è un esempio di ID account. Sostituisci questo valore con l'ID dell'account del proprietario del ruolo. *IAMRoleName* è un nome di esempio. Sostituisci questo valore con il nome del ruolo IAM nell'account del proprietario del ruolo.
 - [kms: GrantOperations](#) — Questa condizione consente al proprietario del ruolo di creare una concessione solo per delegare l'autorizzazione a eseguire l' AWS KMS Decrittazione (decrittografare il testo cifrato crittografato con la chiave). Impedisce al proprietario del ruolo di creare concessioni che delegano le autorizzazioni per eseguire altre azioni sulla chiave KMS. L'Decrittazione è l'unica AWS KMS azione che il ruolo IAM deve essere autorizzato a eseguire per decrittografare un oggetto crittografato con la chiave.

Il punto in cui il proprietario della chiave aggiunge questa dichiarazione alla policy chiave dipende dalla struttura e dagli elementi attualmente contenuti nella policy. Quando il proprietario della chiave aggiunge l'istruzione, deve assicurarsi che la sintassi sia valida. Le politiche chiave utilizzano il formato JSON. Ciò significa che il proprietario della chiave deve aggiungere anche una virgola prima o dopo l'istruzione, a seconda di dove aggiunge l'istruzione alla politica. Per informazioni dettagliate

sull'aggiornamento di una politica chiave, consulta [Modifica di una politica chiave](#) nella Guida per gli AWS Key Management Service sviluppatori.

Fase 2: Creare una sovvenzione

Dopo che il proprietario della chiave ha aggiornato la politica chiave secondo necessità, il proprietario del ruolo crea una concessione per la chiave. La concessione delega le autorizzazioni pertinenti al ruolo IAM nel loro account (del proprietario del ruolo). Prima che il proprietario del ruolo crei la concessione, deve verificare di essere autorizzato a eseguire l'azione `kms:CreateGrant`. Questa azione consente loro di aggiungere una sovvenzione a una sovvenzione esistente gestita dal cliente AWS KMS key.

Per creare la concessione, il proprietario del ruolo può utilizzare il [CreateGrant](#) funzionamento dell'AWS Key Management Service API. Quando il proprietario del ruolo crea la concessione, deve specificare i seguenti valori per i parametri richiesti:

- **KeyId**— L'ARN della chiave KMS. Per l'accesso da più account a una chiave KMS, questo valore deve essere un ARN. Non può essere un ID chiave.
- **GranteePrincipal**— L'ARN del ruolo IAM nel loro account. Questo valore dovrebbe essere `arn:aws:iam::111122223333:role/IAMRoleName:111122223333` dov'è l'ID dell'account del proprietario del ruolo e `IAMRoleName` il nome del ruolo.
- **Operations**— L'azione AWS KMS di decrittografia (`Decrypt`). Questa è l'unica AWS KMS azione che il ruolo IAM deve essere autorizzato a eseguire per decrittografare un oggetto crittografato con la chiave KMS.

Se il proprietario del ruolo utilizza AWS Command Line Interface (AWS CLI), può eseguire il comando [create-grant per creare](#) la concessione. L'esempio seguente mostra come. L'esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws kms create-grant ^  
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^  
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^  
--operations "Decrypt"
```

Dove:

- `key-id` specifica l'ARN della chiave KMS a cui applicare la concessione.

- `grantee-principalspecifica` l'ARN del ruolo IAM a cui è consentito eseguire l'azione specificata dalla concessione. Questo valore deve corrispondere all'ARN specificato dalla `kms:GranteePrincipal` condizione nella politica chiave.
- `operationsspecifica` l'azione che la concessione consente al principale specificato di eseguire: decrittografare il testo cifrato crittografato con la chiave.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{
  "GrantToken": "<grant token>",
  "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Dove `GrantToken` è una stringa univoca, non segreta, a lunghezza variabile e con codifica in base64 che rappresenta la concessione creata e ne rappresenta l'identificatore univoco. `GrantId`

Configurazione di Macie per recuperare campioni di dati sensibili

Facoltativamente, puoi configurare e utilizzare Amazon Macie per recuperare e rivelare campioni di dati sensibili che Macie riporta nei singoli risultati. Gli esempi possono aiutarti a verificare la natura dei dati sensibili trovati da Macie. Possono anche aiutarti a personalizzare l'indagine su un oggetto e un bucket Amazon Simple Storage Service (Amazon S3) interessati. Puoi recuperare e rivelare campioni di dati sensibili in tutte le regioni in Regioni AWS cui Macie è attualmente disponibile, ad eccezione delle regioni di Asia Pacifico (Osaka) e Israele (Tel Aviv).

Quando recuperi e riveli campioni di dati sensibili per una ricerca, Macie utilizza i dati contenuti nel corrispondente risultato della scoperta dei dati sensibili per individuare le occorrenze di dati sensibili nell'oggetto S3 interessato. Macie estrae quindi campioni di tali occorrenze dall'oggetto interessato. Macie crittografa i dati estratti con una chiave AWS Key Management Service (AWS KMS) specificata dall'utente, archivia temporaneamente i dati crittografati in una cache e restituisce i dati nei risultati per la ricerca. Subito dopo l'estrazione e la crittografia, Macie elimina definitivamente i dati dalla cache, a meno che non sia temporaneamente necessaria una conservazione aggiuntiva per risolvere un problema operativo.

Per recuperare e rivelare campioni di dati sensibili per i risultati, devi prima configurare e abilitare le impostazioni per il tuo account Macie. Devi anche configurare le risorse di supporto e le autorizzazioni per il tuo account. Gli argomenti di questa sezione ti guidano nel processo di

configurazione di Macie per recuperare e rivelare campioni di dati sensibili e nella gestione dello stato della configurazione del tuo account.

Argomenti

- [Prima di iniziare](#)
- [Configurazione e attivazione delle impostazioni di Macie](#)
- [Disabilitazione delle impostazioni di Macie](#)

Tip

Per consigli ed esempi di politiche che potresti utilizzare per controllare l'accesso a questa funzionalità, consulta il seguente post sul blog sulla AWS sicurezza: [Come usare Amazon Macie per visualizzare in anteprima i dati sensibili nei bucket S3](#).

Prima di iniziare

Prima di configurare Amazon Macie per recuperare e rivelare campioni di dati sensibili per i risultati, completa le seguenti attività per assicurarti di disporre delle risorse e delle autorizzazioni necessarie.

Attività

- [Passaggio 1: configura un archivio per i risultati della scoperta di dati sensibili](#)
- [Fase 2: Determinare come accedere agli oggetti S3 interessati](#)
- [Fase 3: Configurare un AWS KMS key](#)
- [Passaggio 4: verifica le tue autorizzazioni](#)

Queste attività sono facoltative se hai già configurato Macie per recuperare e rivelare campioni di dati sensibili e desideri modificare solo le impostazioni di configurazione.

Passaggio 1: configura un archivio per i risultati della scoperta di dati sensibili

Quando recuperi e riveli campioni di dati sensibili per una ricerca, Macie utilizza i dati del corrispondente risultato di rilevamento dei dati sensibili per individuare le occorrenze di dati sensibili nell'oggetto S3 interessato. Pertanto, è importante verificare di aver configurato un repository per i risultati del rilevamento dei dati sensibili. Altrimenti, Macie non sarà in grado di individuare campioni di dati sensibili che desideri recuperare e rivelare.

Per determinare se hai configurato questo repository per il tuo account, puoi utilizzare la console Amazon Macie: scegli Discovery results (in Impostazioni) nel pannello di navigazione. Per eseguire questa operazione a livello di codice, utilizza il [GetClassificationExportConfiguration](#) funzionamento dell'API Amazon Macie. Per ulteriori informazioni sui risultati della scoperta di dati sensibili e su come configurare questo repository, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#)

Fase 2: Determinare come accedere agli oggetti S3 interessati

Per accedere agli oggetti S3 interessati e recuperare campioni di dati sensibili da essi, hai due opzioni. Puoi configurare Macie per utilizzare le tue credenziali utente AWS Identity and Access Management (IAM). Oppure puoi configurare Macie in modo che assuma un ruolo IAM che deleghi l'accesso a Macie. Puoi utilizzare entrambe le configurazioni con qualsiasi tipo di account Macie: l'account amministratore Macie delegato per un'organizzazione, un account membro Macie in un'organizzazione o un account Macie autonomo. Prima di configurare le impostazioni in Macie, stabilisci quale metodo di accesso desideri utilizzare. Per informazioni dettagliate sulle opzioni e i requisiti di ciascun metodo, consulta [Opzioni di configurazione per il recupero dei campioni](#).

Se prevedi di utilizzare un ruolo IAM, crea e configura il ruolo prima di configurare le impostazioni in Macie. Assicurati inoltre che le politiche di fiducia e autorizzazioni per il ruolo soddisfino tutti i requisiti necessari per l'assunzione del ruolo da parte di Macie. Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, collabora con l'amministratore Macie per determinare innanzitutto se e come configurare il ruolo per il tuo account.

Fase 3: Configurare un AWS KMS key

Quando recuperi e riveli campioni di dati sensibili per una ricerca, Macie li crittografa con una chiave AWS Key Management Service (AWS KMS) specificata dall'utente. Pertanto, è necessario determinare quale AWS KMS key utilizzare per crittografare i campioni. La chiave può essere una chiave KMS esistente del tuo account o una chiave KMS esistente di proprietà di un altro account. Se desideri utilizzare una chiave di proprietà di un altro account, ottieni l'Amazon Resource Name (ARN) della chiave. Dovrai specificare questo ARN quando accedi alle impostazioni di configurazione in Macie.

La chiave KMS deve essere una chiave di crittografia simmetrica gestita dal cliente. Inoltre, deve essere una chiave a regione singola abilitata nello stesso account Regione AWS Macie. La chiave KMS può trovarsi in un archivio di chiavi esterno. Tuttavia, la chiave potrebbe quindi essere più lenta e meno affidabile di una chiave gestita interamente all'interno. AWS KMS Se la latenza o un

problema di disponibilità impediscono a Macie di crittografare i campioni di dati sensibili che desideri recuperare e rivelare, si verifica un errore e Macie non restituisce alcun campione per la ricerca.

Inoltre, la policy chiave per la chiave deve consentire ai responsabili appropriati (ruoli IAM, utenti IAM o Account AWS) di eseguire le seguenti azioni:

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

 Important

Come ulteriore livello di controllo degli accessi, ti consigliamo di creare una chiave KMS dedicata per la crittografia dei campioni di dati sensibili che vengono recuperati e di limitare l'uso della chiave solo ai principali che devono essere autorizzati a recuperare e rivelare campioni di dati sensibili. Se a un utente non è consentito eseguire le azioni precedenti per la chiave, Macie respinge la richiesta di recuperare e rivelare campioni di dati sensibili. Macie non restituisce alcun campione per la scoperta.

Per informazioni sulla creazione e la configurazione delle chiavi KMS, consulta [Create a KMS key](#) nella Developer Guide.AWS Key Management Service Per informazioni sull'utilizzo delle politiche chiave per gestire l'accesso alle chiavi KMS, consulta le [politiche chiave AWS KMS nella](#) Guida per gli sviluppatori.AWS Key Management Service

Passaggio 4: verifica le tue autorizzazioni

Prima di configurare le impostazioni in Macie, verifica anche di disporre delle autorizzazioni necessarie. Per verificare le tue autorizzazioni, utilizza AWS Identity and Access Management (IAM) per esaminare le policy IAM allegate alla tua identità IAM. Quindi confronta le informazioni contenute in tali policy con il seguente elenco di azioni che devi essere autorizzato a eseguire.

Amazon Macie

Per Macie, verifica di avere il permesso di eseguire le seguenti azioni:

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

La prima azione ti consente di accedere al tuo account Macie. La seconda azione consente di modificare le impostazioni di configurazione per il recupero e la visualizzazione di campioni di dati sensibili. Ciò include l'attivazione e la disabilitazione della configurazione per l'account.

Facoltativamente, verifica che anche tu sia autorizzato a eseguire l'azione `macie2:GetRevealConfiguration`. Questa azione ti consente di recuperare le impostazioni di configurazione correnti e lo stato attuale della configurazione per il tuo account.

AWS KMS

Se prevedi di utilizzare la console Amazon Macie per accedere alle impostazioni di configurazione, verifica anche di essere autorizzato a eseguire le seguenti AWS Key Management Service (AWS KMS) azioni:

- `kms:DescribeKey`
- `kms:ListAliases`

Queste azioni ti consentono di recuperare informazioni AWS KMS keys relative al tuo account. È quindi possibile scegliere uno di questi tasti quando si accede alle impostazioni.

IAM

Se prevedi di configurare Macie per assumere un ruolo IAM per recuperare e rivelare campioni di dati sensibili, verifica anche di essere autorizzato a eseguire la seguente azione IAM:

`iam:PassRole` Questa azione ti consente di passare il ruolo a Macie, che a sua volta consente a Macie di assumere il ruolo. Quando inserisci le impostazioni di configurazione per il tuo account, Macie può anche verificare che il ruolo esista nel tuo account e sia configurato correttamente.

Se non sei autorizzato a eseguire le azioni richieste, chiedi assistenza AWS all'amministratore.

Configurazione e attivazione delle impostazioni di Macie

Dopo aver verificato di disporre delle risorse e delle autorizzazioni necessarie, puoi configurare le impostazioni in Amazon Macie e abilitare la configurazione per il tuo account.

Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, tieni presente quanto segue prima di configurare o modificare successivamente le impostazioni del tuo account:

- Se hai un account membro, collabora con l'amministratore di Macie per determinare se e come configurare le impostazioni per il tuo account. L'amministratore di Macie può aiutarti a determinare le impostazioni di configurazione corrette per il tuo account.

- Se disponi di un account amministratore Macie e modifichi le impostazioni per l'accesso agli oggetti S3 interessati, le modifiche potrebbero influire su altri account e risorse dell'organizzazione. Ciò dipende dal fatto che Macie sia attualmente configurato per assumere un ruolo AWS Identity and Access Management (IAM) per recuperare campioni di dati sensibili. Se lo è e riconfigurate Macie per utilizzare le credenziali utente IAM, Macie elimina definitivamente le impostazioni esistenti per il ruolo IAM, ovvero il nome del ruolo e l'ID esterno per la configurazione. Se successivamente la tua organizzazione sceglie di utilizzare nuovamente i ruoli IAM, dovrai specificare un nuovo ID esterno nella politica di fiducia per il ruolo in ogni account membro applicabile.

Per dettagli sulle opzioni di configurazione e sui requisiti per entrambi i tipi di account, consulta [Opzioni di configurazione per il recupero dei campioni](#).

Per configurare le impostazioni in Macie e abilitare la configurazione per il tuo account, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per configurare e abilitare le impostazioni utilizzando la console Amazon Macie.

Per configurare e abilitare le impostazioni di Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri configurare e consenti a Macie di recuperare e rivelare campioni di dati sensibili.
3. Nel pannello di navigazione, in Impostazioni, scegli Reveal samples.
4. Nella sezione Settings (Impostazioni), scegli Edit (Modifica).
5. In Stato, scegli Abilitato.
6. In Access, specifica il metodo di accesso e le impostazioni che desideri utilizzare per recuperare campioni di dati sensibili dagli oggetti S3 interessati:
 - Per utilizzare un ruolo IAM che delega l'accesso a Macie, scegli Assumi un ruolo IAM. Se scegli questa opzione, Macie recupera gli esempi assumendo il ruolo IAM che hai creato e configurato nel tuo Account AWS. Nella casella Nome ruolo, inserisci il nome del ruolo.

- Per utilizzare le credenziali dell'utente IAM che richiede gli esempi, scegli Usa credenziali utente IAM. Se scegli questa opzione, ogni utente del tuo account utilizza la propria identità IAM individuale per recuperare gli esempi.
7. In Crittografia, specifica AWS KMS key quello che desideri utilizzare per crittografare i campioni di dati sensibili che vengono recuperati:
- Per utilizzare una chiave KMS del tuo account, scegli Seleziona una chiave dal tuo account. Quindi, nell'AWS KMS keyelenco, scegli la chiave da usare. L'elenco mostra le chiavi KMS di crittografia simmetrica esistenti per il tuo account.
 - Per utilizzare una chiave KMS di proprietà di un altro account, scegli Inserisci l'ARN di una chiave di un altro account. Quindi, nella casella AWS KMS key ARN, inserisci l'Amazon Resource Name (ARN) della chiave da utilizzare, ad esempio. **arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab**
8. Quando hai finito di inserire le impostazioni, scegli Salva.

Macie verifica le impostazioni e verifica che siano corrette. Se hai configurato Macie per assumere un ruolo IAM, Macie verifica anche che il ruolo esista nel tuo account e che le politiche di fiducia e autorizzazioni siano configurate correttamente. Se c'è un problema, Macie visualizza un messaggio che descrive il problema.

Per risolvere un problema relativo a AWS KMS key, fai riferimento ai requisiti nell'[argomento precedente](#) e specifica una chiave KMS che soddisfi i requisiti. Per risolvere un problema relativo al ruolo IAM, inizia verificando di aver inserito il nome del ruolo corretto. Se il nome è corretto, assicurati che le politiche del ruolo soddisfino tutti i requisiti necessari affinché Macie possa assumere il ruolo. Per questi dettagli, vedi [Configurazione di un ruolo IAM per accedere agli oggetti S3 interessati](#). Dopo aver risolto eventuali problemi, puoi salvare e abilitare le impostazioni.

 Note

Se sei l'amministratore Macie di un'organizzazione e hai configurato Macie per assumere un ruolo IAM, Macie genera e visualizza un ID esterno dopo aver salvato le impostazioni del tuo account. Annota questo ID. La politica di fiducia per il ruolo IAM in ciascuno degli account membro applicabili deve specificare questo ID. Altrimenti, non sarai in grado di recuperare campioni di dati sensibili dagli oggetti S3 di proprietà degli account.

API

Per configurare e abilitare le impostazioni a livello di codice, utilizza il [UpdateRevealConfiguration](#) funzionamento dell'API Amazon Macie. Nella richiesta, specifica i valori appropriati per i parametri supportati:

- Per i `retrievalConfiguration` parametri, specifica il metodo di accesso e le impostazioni che desideri utilizzare per recuperare campioni di dati sensibili dagli oggetti S3 interessati:
 - Per assumere un ruolo IAM che deleghi l'accesso a Macie, specifica il `retrievalMode` parametro e specifica il nome del ruolo `ASSUME_ROLE` per il parametro. `roleName` Se specifichi queste impostazioni, Macie recupera gli esempi assumendo il ruolo IAM che hai creato e configurato nel tuo Account AWS
 - Per utilizzare le credenziali dell'utente IAM che richiede gli esempi, specifica `CALLER_CREDENTIALS` il parametro. `retrievalMode` Se specifichi questa impostazione, ogni utente del tuo account utilizza la propria identità IAM individuale per recuperare gli esempi.

Important

Se non specificate valori per questi parametri, Macie imposta il metodo di accesso (`retrievalMode`) su. `CALLER_CREDENTIALS` Se Macie è attualmente configurato per utilizzare un ruolo IAM per recuperare gli esempi, Macie elimina anche in modo permanente il nome del ruolo corrente e l'ID esterno per la configurazione. Per mantenere queste impostazioni per una configurazione esistente, includi i `retrievalConfiguration` parametri nella richiesta e specifica le impostazioni correnti per tali parametri. Per recuperare le impostazioni correnti, usa l'[GetRevealConfiguration](#) operazione o, se stai usando il AWS Command Line Interface (AWS CLI), esegui il [get-reveal-configuration](#) comando.

- Per il `kmsKeyId` parametro, specifica AWS KMS key quello che desideri utilizzare per crittografare i campioni di dati sensibili che vengono recuperati:
 - Per utilizzare una chiave KMS dal tuo account, specifica l'Amazon Resource Name (ARN), l'ID o l'alias per la chiave. Se specifichi un alias, includi il prefisso, ad esempio. `alias/exampleAlias`
 - Per utilizzare una chiave KMS di proprietà di un altro account, specifica l'ARN della chiave, ad esempio. `arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`

Oppure specifica l'ARN dell'alias per la chiave, ad esempio. `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`

- Per il status parametro, specifica di abilitare la configurazione ENABLED per il tuo account Macie.

Nella richiesta, assicurati inoltre di specificare Regione AWS in che modo desideri abilitare e utilizzare la configurazione.

Per configurare e abilitare le impostazioni utilizzando il AWS CLI, esegui il [update-reveal-configuration](#) comando e specifica i valori appropriati per i parametri supportati. Ad esempio, se utilizzi Microsoft Windows, esegui il comando seguente: AWS CLI

```
C:\> aws macie2 update-reveal-configuration ^  
--region us-east-1 ^  
--configuration={"kmsKeyId\":"arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias","\  
status\":"ENABLED\"} ^  
--retrievalConfiguration={"retrievalMode\":"ASSUME_ROLE","\  
MacieRevealRole\"}  
^
```

Dove:

- *us-east-1* è la regione in cui abilitare e utilizzare la configurazione. In questo esempio, la regione degli Stati Uniti orientali (Virginia settentrionale).
- *arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias* è l'ARN dell'alias da utilizzare. AWS KMS key In questo esempio, la chiave è di proprietà di un altro account.
- ENABLED è lo stato della configurazione.
- *ASSUME_ROLE* è il metodo di accesso da utilizzare. In questo esempio, assumiamo il ruolo IAM specificato.
- *MacieRevealRole* è il nome del ruolo IAM che Macie deve assumere durante il recupero di campioni di dati sensibili.

L'esempio precedente utilizza il carattere di continuazione di riga con accento circonflesso (^) per migliorare la leggibilità.

Quando invii la richiesta, Macie verifica le impostazioni. Se hai configurato Macie per assumere un ruolo IAM, Macie verifica anche che il ruolo esista nel tuo account e che le politiche di fiducia e autorizzazioni siano configurate correttamente. Se c'è un problema, la tua richiesta fallisce

e Macie restituisce un messaggio che descrive il problema. Per risolvere un problema con il AWS KMS key, fai riferimento ai requisiti nell'[argomento precedente](#) e specifica una chiave KMS che soddisfi i requisiti. Per risolvere un problema relativo al ruolo IAM, inizia verificando di aver specificato il nome del ruolo corretto. Se il nome è corretto, assicurati che le politiche del ruolo soddisfino tutti i requisiti necessari affinché Macie possa assumere il ruolo. Per questi dettagli, vedi [Configurazione di un ruolo IAM per accedere agli oggetti S3 interessati](#). Dopo aver risolto il problema, invia nuovamente la richiesta.

Se la richiesta ha esito positivo, Macie abilita la configurazione del tuo account nella regione specificata e riceverai un output simile al seguente.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

Dove `kmsKeyId` specifica AWS KMS key da usare per crittografare i campioni di dati sensibili che vengono recuperati ed `status` è lo stato della configurazione per il tuo account Macie. I `retrievalConfiguration` valori specificano il metodo di accesso e le impostazioni da utilizzare per il recupero dei campioni.

Note

Se sei l'amministratore Macie di un'organizzazione e hai configurato Macie per assumere un ruolo IAM, annota l'ID esterno (`externalId`) nella risposta. La politica di fiducia per il ruolo IAM in ciascuno degli account membro applicabili deve specificare questo ID. Altrimenti, non sarai in grado di recuperare campioni di dati sensibili dagli oggetti S3 interessati di proprietà degli account.

Per verificare successivamente le impostazioni o lo stato della configurazione del tuo account, usa l'[GetRevealConfiguration](#) operazione o, per il AWS CLI, esegui il comando. [get-reveal-configuration](#)

Disabilitazione delle impostazioni di Macie

Puoi disabilitare le impostazioni di configurazione per il tuo account Amazon Macie in qualsiasi momento. Se disabiliti la configurazione, Macie mantiene l'impostazione che specifica quale utilizzare AWS KMS key per crittografare i campioni di dati sensibili che vengono recuperati. Macie elimina definitivamente le impostazioni di accesso di Amazon S3 per la configurazione.

Warning

Quando disabiliti le impostazioni di configurazione per il tuo account Macie, elimini definitivamente anche le impostazioni correnti che specificano come accedere agli oggetti S3 interessati. Se Macie è attualmente configurato per accedere agli oggetti interessati assumendo un ruolo AWS Identity and Access Management (IAM), ciò include: il nome del ruolo e l'ID esterno generato da Macie per la configurazione. Queste impostazioni non possono essere recuperate dopo essere state eliminate.

Per disabilitare le impostazioni di configurazione per il tuo account Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per disabilitare le impostazioni di configurazione per il tuo account utilizzando la console Amazon Macie.

Per disabilitare le impostazioni di Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri disabilitare le impostazioni di configurazione per il tuo account Macie.
3. Nel pannello di navigazione, in Impostazioni, scegli Reveal samples.
4. Nella sezione Settings (Impostazioni), scegli Edit (Modifica).
5. Per Stato, scegli Disabilita.

6. Seleziona Salva.

API

Per disabilitare le impostazioni di configurazione a livello di codice, utilizza il [UpdateRevealConfiguration](#) funzionamento dell'API Amazon Macie. Nella richiesta, assicurati di specificare il campo Regione AWS in cui desideri disabilitare la configurazione. Per il parametro status, specifica DISABLED.

Per disabilitare le impostazioni di configurazione utilizzando AWS Command Line Interface (AWS CLI), esegui il [update-reveal-configuration](#) comando. Utilizzate il region parametro per specificare la regione in cui desiderate disabilitare la configurazione. Per il parametro status, specifica DISABLED. Ad esempio, se utilizzi Microsoft Windows, esegui il comando seguente: AWS CLI

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --  
configuration={"status\":\"DISABLED\"}
```

Dove:

- **us-east-1** è la regione in cui disattivare la configurazione. In questo esempio, la regione degli Stati Uniti orientali (Virginia settentrionale).
- DISABLED è il nuovo stato della configurazione.

Se la richiesta ha esito positivo, Macie disabilita la configurazione del tuo account nella regione specificata e ricevi un output simile al seguente.

```
{  
  "configuration": {  
    "status": "DISABLED"  
  }  
}
```

statusDov'è il nuovo stato della configurazione del tuo account Macie.

Se Macie è stato configurato per assumere un ruolo IAM per recuperare campioni di dati sensibili, puoi facoltativamente eliminare il ruolo e la politica di autorizzazione del ruolo. Macie non elimina queste risorse quando disabiliti le impostazioni di configurazione per il tuo account. Inoltre, Macie non utilizza queste risorse per eseguire altre attività per il tuo account. Per eliminare il ruolo e la

relativa politica di autorizzazione, puoi utilizzare la console IAM o l'API IAM. Per ulteriori informazioni, consulta [Eliminazione dei ruoli nella Guida](#) per l'AWS Identity and Access Management utente.

Recupero di campioni di dati sensibili per una scoperta di Macie

Utilizzando Amazon Macie, puoi recuperare e rivelare campioni di dati sensibili che Macie riporta nelle singole rilevazioni di dati sensibili. [Ciò include i dati sensibili che Macie rileva utilizzando identificatori di dati gestiti e i dati che corrispondono ai criteri degli identificatori di dati personalizzati.](#)

Gli esempi possono aiutarti a verificare la natura dei dati sensibili trovati da Macie. Possono anche aiutarti a personalizzare l'indagine su un oggetto e un bucket Amazon Simple Storage Service (Amazon S3) interessati. Puoi recuperare e rivelare campioni di dati sensibili in tutte le regioni in Regioni AWS cui Macie è attualmente disponibile, ad eccezione delle regioni di Asia Pacifico (Osaka) e Israele (Tel Aviv).

Se recuperi e riveli campioni di dati sensibili per un risultato, Macie utilizza i dati contenuti nel corrispondente risultato della [scoperta di dati sensibili per individuare le prime 1-10 occorrenze di dati sensibili segnalate dal risultato](#). Macie estrae quindi i primi 1-128 caratteri di ogni occorrenza dall'oggetto S3 interessato. Se un risultato riporta più tipi di dati sensibili, Macie lo fa per un massimo di 100 tipi di dati sensibili segnalati dal risultato.

Quando Macie estrae dati sensibili da un oggetto S3 interessato, Macie crittografa i dati con una chiave AWS Key Management Service (AWS KMS) specificata dall'utente, archivia temporaneamente i dati crittografati in una cache e restituisce i dati nei risultati per la ricerca. Subito dopo l'estrazione e la crittografia, Macie elimina definitivamente i dati dalla cache, a meno che non sia temporaneamente necessaria una conservazione aggiuntiva per risolvere un problema operativo.

Se scegli di recuperare e rivelare campioni di dati sensibili per un nuovo ritrovamento, Macie ripete il processo per localizzare, estrarre, crittografare, archiviare e infine eliminare i campioni.

Per una dimostrazione di come recuperare e rivelare campioni di dati sensibili utilizzando la console Amazon Macie, guarda il seguente video: [Recupero e rivelazione di campioni di dati sensibili con Amazon Macie](#).

Argomenti

- [Prima di iniziare](#)
- [Determinare se sono disponibili campioni di dati sensibili ai fini di una ricerca](#)
- [Recupero di campioni di dati sensibili per una ricerca](#)

Prima di iniziare

Prima di poter recuperare e rivelare campioni di dati sensibili per i risultati, devi [configurare e abilitare le impostazioni per il tuo account Amazon Macie](#). Inoltre, devi collaborare con il tuo AWS amministratore per verificare di disporre delle autorizzazioni e delle risorse necessarie.

Quando recuperi e riveli campioni di dati sensibili per una ricerca, Macie esegue una serie di attività per localizzare, recuperare, crittografare e rivelare i campioni. Macie non utilizza il [ruolo collegato al servizio Macie per il tuo account per eseguire](#) queste attività. Invece, usi la tua identità AWS Identity and Access Management (IAM) o consenti a Macie di assumere un ruolo IAM nel tuo account.

Per recuperare e rivelare campioni di dati sensibili per un risultato, devi avere accesso al risultato della scoperta, al corrispondente risultato della scoperta dei dati sensibili e a AWS KMS key quello che hai configurato Macie per utilizzare per crittografare i campioni di dati sensibili. Inoltre, a te o al ruolo IAM deve essere consentito di accedere al bucket S3 e all'oggetto S3 interessato. A te o al ruolo deve inoltre essere consentito di utilizzare AWS KMS key ciò che è stato utilizzato per crittografare l'oggetto interessato, se applicabile. Se alcune politiche IAM, politiche delle risorse o altre impostazioni di autorizzazione negano l'accesso richiesto, si verifica un errore e Macie non restituisce alcun esempio del risultato.

Devi inoltre avere il permesso di eseguire le seguenti azioni di Macie:

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

Le prime tre azioni ti consentono di accedere al tuo account Macie e recuperare i dettagli dei risultati. L'ultima azione consente di recuperare e rivelare campioni di dati sensibili per i risultati.

Per utilizzare la console Amazon Macie per recuperare e rivelare campioni di dati sensibili, devi inoltre essere autorizzato a eseguire la seguente azione:

`macie2:GetSensitiveDataOccurrencesAvailability` Questa azione consente di determinare se i campioni sono disponibili per i singoli risultati. Non è necessaria l'autorizzazione per eseguire questa azione per recuperare e rivelare campioni a livello di codice. Tuttavia, disporre di questa autorizzazione può semplificare il recupero dei campioni.

Se sei l'amministratore Macie delegato di un'organizzazione e hai configurato Macie per assumere un ruolo IAM per recuperare campioni di dati sensibili, devi anche essere autorizzato a eseguire

la seguente azione: `macie2:GetMember`. Questa azione ti consente di recuperare informazioni sull'associazione tra il tuo account e un account interessato. Consente a Macie di verificare che tu sia attualmente l'amministratore Macie dell'account interessato.

Se non sei autorizzato a eseguire le azioni richieste o ad accedere ai dati e alle risorse necessari, chiedi assistenza all'amministratore AWS .

Determinare se sono disponibili campioni di dati sensibili ai fini di una ricerca

Per recuperare e rivelare campioni di dati sensibili per un risultato, il risultato deve soddisfare determinati criteri. Deve includere dati sulla posizione per occorrenze specifiche di dati sensibili. Inoltre, deve specificare la posizione di un risultato valido e corrispondente alla scoperta di dati sensibili. Il risultato della scoperta di dati sensibili deve essere archiviato nello Regione AWS stesso del risultato. Se hai configurato Amazon Macie per accedere agli oggetti S3 interessati assumendo un ruolo AWS Identity and Access Management (IAM), anche il risultato del rilevamento dei dati sensibili deve essere archiviato in un oggetto S3 firmato da Macie con un codice di autenticazione dei messaggi basato su Hash (HMAC). AWS KMS key

L'oggetto S3 interessato deve inoltre soddisfare determinati criteri. Il tipo MIME dell'oggetto deve essere uno dei seguenti:

- `application/avro`, per un file contenitore di oggetti Apache Avro (.avro)
- `application/gzip`, per un file di archivio compresso GNU Zip (.gz o .gzip)
- `application/json`, per un file JSON o JSON Lines (.json o .jsonl)
- `application/parquet`, per un file Apache Parquet (.parquet)
- `application/vnd.openxmlformats-officedocument.spreadsheetml.sheet`, per un file di cartella di lavoro di Microsoft Excel (.xlsx)
- `application/zip`, per un file di archivio compresso ZIP (.zip)
- `text/csv`, per un file CSV (.csv)
- `text/plain`, per un file di testo non binario diverso da un file CSV, JSON, JSON Lines o TSV
- `text/tab-separated-values`, per un file TSV (.tsv)

Inoltre, il contenuto dell'oggetto S3 deve essere lo stesso di quando è stato creato il risultato. Macie controlla il tag di entità (ETag) dell'oggetto per determinare se corrisponde a quello ETag specificato dal risultato. Inoltre, la dimensione di archiviazione dell'oggetto non può superare la quota di dimensioni applicabile per il recupero e la rivelazione di campioni di dati sensibili. Per un elenco delle quote applicabili, vedere. [Quote per Macie](#)

Se un risultato e l'oggetto S3 interessato soddisfano i criteri precedenti, sono disponibili esempi di dati sensibili per il risultato. Facoltativamente, è possibile determinare se questo è il caso di un particolare risultato prima di provare a recuperarlo e rivelarne degli esempi.

Per determinare se sono disponibili campioni di dati sensibili per un risultato

Puoi utilizzare la console Amazon Macie o l'API Amazon Macie per determinare se sono disponibili campioni di dati sensibili per una ricerca.

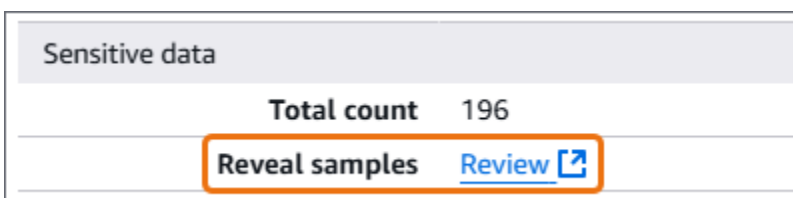
Console

Segui questi passaggi sulla console Amazon Macie per determinare se sono disponibili campioni di dati sensibili per una ricerca.

Per determinare se i campioni sono disponibili per un risultato

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Nella pagina Risultati, scegli il risultato. Il pannello dei dettagli mostra le informazioni relative al risultato.
4. Nel pannello dei dettagli, scorri fino alla sezione Dati sensibili. Quindi fai riferimento al campo Reveal samples.

Se sono disponibili campioni di dati sensibili per la ricerca, nel campo viene visualizzato un link Revisione, come mostrato nell'immagine seguente.



Se per la ricerca non sono disponibili campioni di dati sensibili, nel campo Rivela esempi viene visualizzato un testo che indica il motivo:

- Account non appartenente all'organizzazione: non ti è consentito accedere all'oggetto S3 interessato utilizzando Macie. L'account interessato non fa attualmente parte della tua organizzazione. Oppure l'account fa parte della tua organizzazione ma Macie non è attualmente abilitato per l'account nella versione corrente Regione AWS.

- Risultato di classificazione non valido: non esiste un risultato corrispondente all'individuazione di dati sensibili per il risultato. Oppure il risultato dell'individuazione dei dati sensibili corrispondente non è disponibile nella versione corrente Regione AWS, è difettoso o danneggiato o utilizza un formato di archiviazione non supportato. Macie non può verificare la posizione dei dati sensibili da recuperare.
- Firma del risultato non valida: il risultato corrispondente del rilevamento dei dati sensibili è archiviato in un oggetto S3 che non è stato firmato da Macie. Macie non può verificare l'integrità e l'autenticità del risultato del rilevamento dei dati sensibili. Pertanto, Macie non può verificare la posizione dei dati sensibili da recuperare.
- Ruolo del membro troppo permissivo: la politica di fiducia o di autorizzazione per il ruolo IAM nell'account membro interessato non soddisfa i requisiti di Macie per la limitazione dell'accesso al ruolo. Oppure la policy di fiducia del ruolo non specifica l'ID esterno corretto per la tua organizzazione. Macie non può assumersi il ruolo di recuperare i dati sensibili.
- GetMember Autorizzazione mancante: non ti è consentito recuperare informazioni sull'associazione tra il tuo account e l'account interessato. Macie non è in grado di determinare se sei autorizzato ad accedere all'oggetto S3 interessato come amministratore Macie delegato per l'account interessato.
- L'oggetto supera la quota di dimensione: la dimensione di archiviazione dell'oggetto S3 interessato supera la quota di dimensioni per il recupero e la visualizzazione di campioni di dati sensibili da quel tipo di file.
- Oggetto non disponibile: l'oggetto S3 interessato non è disponibile. L'oggetto è stato rinominato, spostato o eliminato o il suo contenuto è stato modificato dopo che Macie ha creato il risultato. Oppure l'oggetto è crittografato con un file AWS KMS key che non è disponibile. Ad esempio, la chiave è disabilitata, è pianificata per l'eliminazione o è stata eliminata.
- Risultato non firmato: il risultato corrispondente del rilevamento dei dati sensibili viene archiviato in un oggetto S3 che non è stato firmato. Macie non può verificare l'integrità e l'autenticità del risultato della scoperta dei dati sensibili. Pertanto, Macie non può verificare la posizione dei dati sensibili da recuperare.
- Ruolo troppo permissivo: il tuo account è configurato per recuperare le occorrenze di dati sensibili utilizzando un ruolo IAM la cui politica di fiducia o di autorizzazione non soddisfa i requisiti di Macie per la limitazione dell'accesso al ruolo. Macie non può assumersi il ruolo di recuperare i dati sensibili.
- Tipo di oggetto non supportato: l'oggetto S3 interessato utilizza un formato di file o di archiviazione che Macie non supporta per il recupero e la rivelazione di campioni di

dati sensibili. [Il tipo MIME dell'oggetto S3 interessato non è uno dei valori nell'elenco precedente.](#)

Se c'è un problema con il risultato dell'individuazione di dati sensibili relativi al risultato, le informazioni nel campo Posizione dettagliata dei risultati del risultato possono aiutarvi a risolvere il problema. Questo campo specifica il percorso originale del risultato in Amazon S3. Per esaminare un problema relativo a un ruolo IAM, assicurati che le politiche del ruolo soddisfino tutti i requisiti necessari per l'assunzione del ruolo da parte di Macie. Per questi dettagli, vedi [Configurazione di un ruolo IAM per accedere agli oggetti S3 interessati](#).

API

Per determinare in modo programmatico se sono disponibili campioni di dati sensibili per una ricerca, utilizza il [GetSensitiveDataOccurrencesAvailability](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza il `findingId` parametro per specificare l'identificatore univoco per il risultato. Per ottenere questo identificatore, è possibile utilizzare l'[ListFindings](#) operazione.

Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando [get-sensitive-data-occurrences-availability](#) e usa il `finding-id` parametro per specificare l'identificatore univoco per il risultato. [Per ottenere questo identificatore, puoi eseguire il comando list-finding.](#)

Se la richiesta ha esito positivo e sono disponibili campioni per la ricerca, si ottiene un risultato simile al seguente:

```
{
  "code": "AVAILABLE",
  "reasons": []
}
```

Se la richiesta ha esito positivo e i campioni non sono disponibili per la ricerca, il valore del `code` campo è `UNAVAILABLE` e l'`reasons` array specifica il motivo. Per esempio:

```
{
  "code": "UNAVAILABLE",
  "reasons": [
    "UNSUPPORTED_OBJECT_TYPE"
  ]
}
```

Se c'è un problema con il risultato dell'individuazione di dati sensibili relativi al risultato, le informazioni contenute nel `classificationDetails.detailedResultsLocation` campo del risultato possono aiutarti a risolvere il problema. Questo campo specifica il percorso originale del risultato in Amazon S3. Per esaminare un problema relativo a un ruolo IAM, assicurati che le politiche del ruolo soddisfino tutti i requisiti necessari per l'assunzione del ruolo da parte di Macie. Per questi dettagli, vedi [Configurazione di un ruolo IAM per accedere agli oggetti S3 interessati](#).

Recupero di campioni di dati sensibili per una ricerca

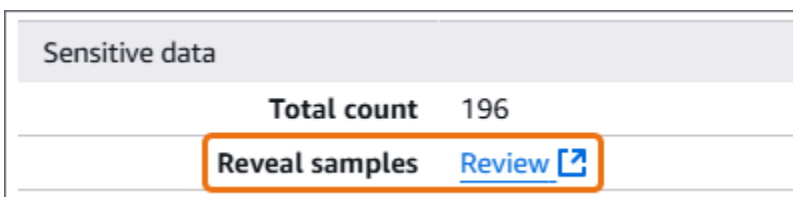
Per recuperare e rivelare campioni di dati sensibili per una ricerca, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per recuperare e rivelare campioni di dati sensibili per una ricerca utilizzando la console Amazon Macie.

Per recuperare e rivelare campioni di dati sensibili ai fini di una scoperta

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Nella pagina Risultati, scegli il risultato. Il pannello dei dettagli mostra le informazioni relative al risultato.
4. Nel pannello dei dettagli, scorri fino alla sezione Dati sensibili. Quindi, nel campo Reveal samples, scegli Revisione:



Note

Se il link Review non viene visualizzato nel campo Reveal samples, non sono disponibili esempi di dati sensibili per il risultato. Per determinare il motivo di questa situazione, consultate l'[argomento precedente](#).

Dopo aver scelto **Revisione**, Macie visualizza una pagina che riassume i dettagli chiave del risultato. I dettagli includono le categorie, i tipi e il numero di occorrenze di dati sensibili che Macie ha trovato nell'oggetto S3 interessato.

5. Nella sezione **Dati sensibili** della pagina, scegli **Reveal samples**. Macie recupera quindi e rivela i campioni delle prime 1-10 occorrenze di dati sensibili riportate dalla scoperta. Ogni campione contiene i primi 1—128 caratteri di una occorrenza di dati sensibili. Il recupero e la visualizzazione dei campioni possono richiedere diversi minuti.

Se il risultato riporta diversi tipi di dati sensibili, Macie recupera e rivela campioni per un massimo di 100 tipi. Ad esempio, l'immagine seguente mostra esempi che comprendono più categorie e tipi di dati sensibili: AWS credenziali, numeri di telefono statunitensi e nomi di persone.

Sensitive data

Reveal samples

Macie found the following types of sensitive data in the S3 object. You can retrieve and reveal samples of the sensitive data that Macie found.

Category	Type	Sample
Credentials	Aws credentials	je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
Credentials	Aws credentials	wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Credentials	Aws credentials	je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
Personal information	Phone number	425-555-0100
Personal information	Phone number	425-555-0101
Personal information	Phone number	425-555-0102
Personal information	Name	John Doe
Personal information	Name	Martha Rivera
Personal information	Name	Wang Xiulan

I campioni sono organizzati prima per categoria di dati sensibili e poi per tipo di dati sensibili.

API

Per recuperare e rivelare campioni di dati sensibili per una ricerca a livello di codice, utilizza il [GetSensitiveDataOccurrences](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza il `findingId` parametro per specificare l'identificatore univoco per il risultato. Per ottenere questo identificatore, è possibile utilizzare l'[ListFindings](#) operazione.

Per recuperare e rivelare campioni di dati sensibili utilizzando AWS Command Line Interface (AWS CLI), esegui il [get-sensitive-data-occurrences](#) comando e utilizza il `finding-id` parametro per specificare l'identificatore univoco per il risultato. Per esempio:

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
"1f1c2d74db5d8caa76859ec52example"
```

1f1c2d74db5d8caa76859ec52example Dov'è l'identificatore univoco del risultato. Per ottenere questo identificatore utilizzando AWS CLI, è possibile eseguire il comando [list-finding](#).

Se la tua richiesta ha esito positivo, Macie inizia a elaborarla e ricevi un output simile al seguente:

```
{
  "status": "PROCESSING"
}
```

L'elaborazione della richiesta può richiedere diversi minuti. Entro pochi minuti, invia nuovamente la richiesta.

Se Macie è in grado di localizzare, recuperare e crittografare i campioni di dati sensibili, Macie restituisce gli esempi in una mappa. `sensitiveDataOccurrences` La mappa specifica da 1 a 100 tipi di dati sensibili riportati dalla scoperta e da 1 a 10 campioni per ogni tipo. Ogni campione contiene i primi 1-128 caratteri di un'occorrenza di dati sensibili segnalati dal risultato.

Nella mappa, ogni chiave è l'ID dell'identificatore di dati gestito che ha rilevato i dati sensibili oppure il nome e l'identificatore univoco dell'identificatore di dati personalizzato che ha rilevato i dati sensibili. I valori sono esempi per l'identificatore di dati gestito o l'identificatore di dati personalizzato specificato. Ad esempio, la risposta seguente fornisce tre esempi di nomi di persone e due esempi di chiavi di accesso AWS segrete rilevate dagli identificatori di dati gestiti (`NAME` e `AWS_CREDENTIALS`, rispettivamente).

```
{
  "sensitiveDataOccurrences": {
    "NAME": [
      {
        "value": "Akua Mansa"
      },
      {
        "value": "John Doe"
      },
      {
        "value": "Martha Rivera"
      }
    ],

```

```
    "AWS_CREDENTIALS": [
      {
        "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
      },
      {
        "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
      }
    ]
  },
  "status": "SUCCESS"
}
```

Se la richiesta ha esito positivo ma non sono disponibili campioni di dati sensibili per la ricerca, riceverai un `UnprocessableEntityException` messaggio che indica il motivo per cui i campioni non sono disponibili. Per esempio:

```
{
  "message": "An error occurred (UnprocessableEntityException) when calling the
  GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

Nell'esempio precedente, Macie ha tentato di recuperare campioni dall'oggetto S3 interessato, ma l'oggetto non è più disponibile. Il contenuto dell'oggetto è cambiato dopo che Macie ha creato il risultato.

Se la richiesta ha esito positivo ma un altro tipo di errore ha impedito a Macie di recuperare e rivelare campioni di dati sensibili necessari alla ricerca, riceverai un output simile al seguente:

```
{
  "error": "Macie can't retrieve the samples. You're not allowed to access the
  affected S3 object or the object is encrypted with a key that you're not allowed to
  use.",
  "status": "ERROR"
}
```

Il valore del `status` campo è `ERROR` e il campo descrive l'errore che si è verificato `error`. Le informazioni contenute nell'[argomento precedente](#) possono aiutarti a esaminare l'errore.

Schema per la segnalazione della posizione dei dati sensibili

Amazon Macie utilizza strutture JSON standardizzate per archiviare informazioni su dove trova dati sensibili negli oggetti Amazon Simple Storage Service (Amazon S3). Le strutture vengono utilizzate per la rilevazione di dati sensibili e per i risultati della scoperta di dati sensibili. Per i risultati di dati sensibili, le strutture fanno parte dello schema JSON per i risultati. Per esaminare lo schema JSON completo per i risultati, consulta [Findings](#) in Amazon Macie API Reference. Per ulteriori informazioni sui risultati della scoperta di dati sensibili, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

Argomenti

- [Panoramica dello schema](#)
- [Dettagli ed esempi dello schema](#)

Panoramica dello schema

Per segnalare la posizione dei dati sensibili che Amazon Macie ha trovato in un oggetto S3 interessato, lo schema JSON per il rilevamento di dati sensibili e i risultati del rilevamento di dati sensibili include un `customDataIdentifiers` oggetto e un oggetto `sensitiveData`. [L'oggetto `customDataIdentifiers` fornisce dettagli sui dati rilevati da Macie utilizzando identificatori di dati personalizzati.](#) L'oggetto `sensitiveData` fornisce dettagli sui dati rilevati da Macie utilizzando identificatori di dati [gestiti](#).

Ogni `customDataIdentifiers` `sensitiveData` oggetto contiene uno o più `detections` array:

- In un `customDataIdentifiers` oggetto, l'`detections` array indica quali identificatori di dati personalizzati hanno rilevato i dati e prodotto il risultato. Per ogni identificatore di dati personalizzato, l'array indica anche il numero di occorrenze dei dati rilevati dall'identificatore. Può anche indicare la posizione dei dati rilevati dall'identificatore.
- In un `sensitiveData` oggetto, un `detections` array indica i tipi di dati sensibili rilevati da Macie utilizzando identificatori di dati gestiti. Per ogni tipo di dati sensibili, l'array indica anche il numero di occorrenze dei dati e può indicare la posizione dei dati.

Per la ricerca di dati sensibili, un `detections` array può includere da 1 `occurrences` a 15 oggetti. Ogni `occurrences` oggetto specifica dove Macie ha rilevato le singole occorrenze di un tipo specifico di dati sensibili.

Ad esempio, l'`detectionsarray` seguente indica la posizione di tre occorrenze di dati sensibili (numeri di previdenza sociale degli Stati Uniti) che Macie ha trovato in un file CSV.

```
"sensitiveData": [
  {
    "category": "PERSONAL_INFORMATION",
    "detections": [
      {
        "count": 30,
        "occurrences": {
          "cells": [
            {
              "cellReference": null,
              "column": 1,
              "columnName": "SSN",
              "row": 2
            },
            {
              "cellReference": null,
              "column": 1,
              "columnName": "SSN",
              "row": 3
            },
            {
              "cellReference": null,
              "column": 1,
              "columnName": "SSN",
              "row": 4
            }
          ]
        }
      },
      {
        "type": "USA_SOCIAL_SECURITY_NUMBER"
      }
    ]
  }
]
```

La posizione e il numero di occurrences oggetti in un detections array variano in base alle categorie, ai tipi e al numero di occorrenze di dati sensibili rilevati da Macie durante un ciclo di analisi automatizzato di rilevamento di dati sensibili o l'esecuzione di un processo di rilevamento di dati sensibili. Per ogni ciclo di analisi o processo eseguito, Macie utilizza un algoritmo di ricerca basato sulla profondità per compilare i risultati risultanti con i dati sulla posizione per 1-15 occorrenze di dati sensibili che Macie rileva negli oggetti S3. Queste occorrenze sono indicative delle categorie e dei tipi di dati sensibili che un bucket e un oggetto S3 interessati potrebbero contenere.

Un `occurrences` oggetto può contenere una delle seguenti strutture, a seconda del tipo di file o del formato di archiviazione dell'oggetto S3 interessato:

- `cellarray`: questo array si applica alle cartelle di lavoro di Microsoft Excel, ai file CSV e ai file TSV. Un oggetto in questo array specifica una cella o un campo in cui Macie ha rilevato una presenza di dati sensibili.
- `lineRangesarray`: questo array si applica ai file di messaggi di posta elettronica (EML) e ai file di testo non binari diversi dai file CSV, JSON, JSON Lines e TSV, ad esempio file HTML, TXT e XML. Un oggetto in questo array specifica una riga o un intervallo di righe inclusivo in cui Macie ha rilevato la presenza di dati sensibili e la posizione dei dati sulla riga o sulle righe specificate.

In alcuni casi, un oggetto in un `lineRanges` array specifica la posizione del rilevamento di dati sensibili in un tipo di file o formato di archiviazione supportato da un altro tipo di array. Questi casi sono: un rilevamento in una sezione non strutturata di un file altrimenti strutturato, ad esempio un commento in un file; un rilevamento in un file non valido che Macie analizza come testo normale; e un file CSV o TSV con uno o più nomi di colonna in cui Macie ha rilevato dati sensibili.

- `offsetRangesarray` — Questo array è riservato per utilizzi futuri. Se questo array è presente, il suo valore è nullo.
- `pagesarray`: questo array si applica ai file Adobe Portable Document Format (PDF). Un oggetto in questo array specifica una pagina in cui Macie ha rilevato una presenza di dati sensibili.
- `recordsarray`: questo array si applica ai contenitori di oggetti Apache Avro, ai file Apache Parquet, ai file JSON e ai file JSON Lines. Per i contenitori di oggetti Avro e i file Parquet, un oggetto in questo array specifica un indice di record e il percorso di un campo in un record in cui Macie ha rilevato una presenza di dati sensibili. Per i file JSON e JSON Lines, un oggetto in questo array specifica il percorso di un campo o di un array in cui Macie ha rilevato una presenza di dati sensibili. Per i file JSON Lines, specifica anche l'indice della riga che contiene i dati.

Il contenuto di questi array varia in base al tipo di file o al formato di archiviazione dell'oggetto S3 interessato e al relativo contenuto.

Dettagli ed esempi dello schema

Amazon Macie personalizza i contenuti delle strutture JSON utilizzate per indicare dove ha rilevato dati sensibili in tipi specifici di file e contenuti. I seguenti argomenti spiegano e forniscono esempi di queste strutture.

Argomenti

- [Matrice di celle](#)
- [LineRangesmatrice](#)
- [Matrice di pagine](#)
- [Matrice di record](#)

Per un elenco completo delle strutture JSON che possono essere incluse in una ricerca di dati sensibili, consulta [Findings](#) in the Amazon Macie API Reference.

Matrice di celle

Si applica a: cartelle di lavoro Microsoft Excel, file CSV e file TSV

In un `cells` array, un `Cell` oggetto specifica una cella o un campo in cui Macie ha rilevato una presenza di dati sensibili. La tabella seguente descrive lo scopo di ogni campo in un `Cell` oggetto.

Campo	Tipo	Descrizione
<code>cellReference</code>	Stringa	La posizione della cella, come riferimento assoluto, che contiene l'occorrenza. Questo campo si applica solo alle cartelle di lavoro di Excel. Questo valore è nullo per i file CSV e TSV.
<code>column</code>	Numero intero	Il numero di colonna della colonna che contiene l'occorrenza. Per una cartella di lavoro di Excel, questo valore è correlato ai caratteri alfabetici di un identificatore di colonna, ad esempio per la colonna A, 1 per la colonna B e così 2 via.

Campo	Tipo	Descrizione
columnName	Stringa	Il nome della colonna che contiene l'occorrenza, se disponibile.
row	Numero intero	Il numero di riga della riga che contiene l'occorrenza.

L'esempio seguente mostra la struttura di un `Cell` oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie in un file CSV.

```
"cells": [  
  {  
    "cellReference": null,  
    "column": 3,  
    "columnName": "SSN",  
    "row": 5  
  }  
]
```

Nell'esempio precedente, la scoperta indica che Macie ha rilevato dati sensibili nel campo nella quinta riga della terza colonna (denominata SSN) del file.

L'esempio seguente mostra la struttura di un `Cell` oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie in una cartella di lavoro di Excel.

```
"cells": [  
  {  
    "cellReference": "Sheet2!C5",  
    "column": 3,  
    "columnName": "SSN",  
    "row": 5  
  }  
]
```

Nell'esempio precedente, la scoperta indica che Macie ha rilevato dati sensibili nel foglio di lavoro denominato Sheet2 della cartella di lavoro. In quel foglio di lavoro, Macie ha rilevato dati sensibili nella cella nella quinta riga della terza colonna (colonna C, denominata SSN).

LineRangesmatrice

Si applica a: file di messaggi di posta elettronica (EML) e file di testo non binari diversi dai file CSV, JSON, JSON Lines e TSV, ad esempio file HTML, TXT e XML.

In un `lineRanges` array, un `Range` oggetto specifica una riga o un intervallo di righe inclusivo in cui Macie ha rilevato la presenza di dati sensibili e la posizione dei dati sulla riga o sulle righe specificate.

Questo oggetto è spesso vuoto per i tipi di file supportati da altri tipi di matrici negli oggetti.

`occurrences` Le eccezioni sono:

- Dati in sezioni non strutturate di un file altrimenti strutturato, ad esempio un commento in un file.
- Dati in un file in formato errato che Macie analizza come testo non crittografato.
- Un file CSV o TSV con uno o più nomi di colonne in cui Macie ha rilevato dati sensibili.

La tabella seguente descrive lo scopo di ogni campo in un `Range` oggetto di un array. `lineRanges`

Campo	Tipo	Descrizione
<code>end</code>	Numero intero	Il numero di righe dall'inizio del file alla fine dell'occorrenza.
<code>start</code>	Numero intero	Il numero di righe dall'inizio del file all'inizio dell'occorrenza.
<code>startColumn</code>	Numero intero	Il numero di caratteri, con spazi e a partire da 1, dall'inizio della prima riga che contiene l'occorrenza (<code>start</code>) all'inizio dell'occorrenza.

L'esempio seguente mostra la struttura di un `Range` oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie su una singola riga di un file TXT.

```
"lineRanges": [  
  {  
    "end": 1,  
    "start": 1,
```

```
    "startColumn": 119
  }
]
```

Nell'esempio precedente, la scoperta indica che Macie ha rilevato un'occorrenza completa di dati sensibili (un indirizzo postale) nella prima riga del file. Il primo carattere dell'occorrenza corrisponde a 119 caratteri (con spazi) dall'inizio di quella riga.

L'esempio seguente mostra la struttura di un Range oggetto che specifica la posizione di un'occorrenza di dati sensibili che si estende su più righe in un file TXT.

```
"lineRanges": [
  {
    "end": 54,
    "start": 51,
    "startColumn": 1
  }
]
```

Nell'esempio precedente, la scoperta indica che Macie ha rilevato una presenza di dati sensibili (un indirizzo postale) tra le righe da 51 a 54 del file. Il primo carattere dell'occorrenza è il primo carattere sulla riga 51 del file.

Matrice di pagine

Si applica a: file Adobe Portable Document Format (PDF)

In un pages array, un Page oggetto specifica una pagina in cui Macie ha rilevato una presenza di dati sensibili. L'oggetto contiene un pageNumber campo. Il pageNumber campo memorizza un numero intero che specifica il numero di pagina della pagina che contiene l'occorrenza.

L'esempio seguente mostra la struttura di un Page oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie in un file PDF.

```
"pages": [
  {
    "pageNumber": 10
  }
]
```

Nell'esempio precedente, il risultato indica che la pagina 10 del file contiene l'occorrenza.

Matrice di record

Si applica a: contenitori di oggetti Apache Avro, file Apache Parquet, file JSON e file JSON Lines

Per un contenitore di oggetti Avro o un file Parquet, un `Record` oggetto in un `records` array specifica un indice di record e il percorso di un campo in un record in cui Macie ha rilevato una presenza di dati sensibili. Per i file JSON e JSON Lines, un `Record` oggetto specifica il percorso di un campo o di un array in cui Macie ha rilevato una presenza di dati sensibili. Per i file JSON Lines, specifica anche l'indice della riga che contiene l'occorrenza.

La tabella seguente descrive lo scopo di ogni campo in un `Record` oggetto.

Campo	Tipo	Descrizione
<code>jsonPath</code>	Stringa	Il percorso, come <code>JSONPath</code> espressione, dell'occorrenza. Per un contenitore di oggetti Avro o un file Parquet, questo è il percorso del campo nel record (<code>recordIndex</code>) che contiene l'occorrenza. Per un file JSON o JSON Lines, questo è il percorso del campo o dell'array che contiene l'occorrenza. Se i dati sono un valore in una matrice, il percorso indica anche quale valore contiene l'occorrenza. Se Macie rileva dati sensibili nel nome di qualsiasi elemento del percorso, Macie omette il <code>jsonPath</code> campo da un oggetto. <code>Record</code> Se il nome di un elemento del percorso supera i 240 caratteri, Macie tronca il nome

Campo	Tipo	Descrizione
		rimuovendo i caratteri dall'inizio del nome. Se il percorso completo risultante supera i 250 caratteri, Macie tronca anche il percorso, a partire dal primo elemento del percorso, finché il percorso non contiene 250 caratteri o meno.
recordIndex	Numero intero	Per un contenitore di oggetti Avro o un file Parquet, l'indice dei record, a partire da 0, per il record che contiene l'occorrenza. Per un file JSON Lines, l'indice di riga, a partire da 0, per la riga che contiene l'occorrenza. Questo valore è sempre valido 0 per i file JSON.

L'esempio seguente mostra la struttura di un Record oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie in un file Parquet.

```
"records": [  
  {  
    "jsonPath": "$['abcdefghijklmnopqrstuvwxy']",  
    "recordIndex": 7663  
  }  
]
```

Nell'esempio precedente, la scoperta indica che Macie ha rilevato dati sensibili nel record dell'indice 7663 (numero di record 7664). In quel record, Macie ha rilevato dati sensibili nel campo denominato. `abcdefghijklmnopqrstuvwxy` Il percorso JSON completo del campo nel record è. `$.abcdefghijklmnopqrstuvwxy` Il campo è un discendente diretto dell'oggetto radice (di livello esterno).

L'esempio seguente mostra anche la struttura di un Record oggetto per un'occorrenza di dati sensibili rilevati da Macie in un file Parquet. Tuttavia, in questo esempio, Macie ha troncato il nome del campo che contiene l'occorrenza perché il nome supera il limite di caratteri.

```
"records": [
  {
    "jsonPath":
"$['...uvwxyzabcdefghijklmnopqrstuvwxyabcdefghijklmnopqrstuvwxyabc
    "recordIndex": 7663
  }
]
```

Nell'esempio precedente, il campo è un discendente diretto dell'oggetto radice (di livello esterno).

Nell'esempio seguente, sempre per un'occorrenza di dati sensibili rilevata da Macie in un file Parquet, Macie ha troncato il percorso completo del campo che contiene l'occorrenza. Il percorso completo supera il limite di caratteri.

```
"records": [
  {
    "jsonPath":
"$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
    "recordIndex": 2335
  }
]
```

Nell'esempio precedente, il risultato indica che Macie ha rilevato dati sensibili nel record dell'indice 2335 (numero di record 2336). In quel record, Macie ha rilevato dati sensibili nel campo denominato. abcdefghijklmnopqrstuvwxyz Il percorso JSON completo del campo nel record è:

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

L'esempio seguente mostra la struttura di un Record oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie in un file JSON. In questo esempio, l'occorrenza è un valore specifico in una matrice.

```
"records": [
  {
    "jsonPath": "$.access.key[2]",
    "recordIndex": 0
  }
]
```

```
}  
]
```

Nell'esempio precedente, il risultato indica che Macie ha rilevato dati sensibili nel secondo valore di un array denominato `key`. L'array è un elemento secondario di un oggetto denominato `access`.

L'esempio seguente mostra la struttura di un Record oggetto che specifica la posizione di un'occorrenza di dati sensibili rilevati da Macie in un file JSON Lines.

```
"records": [  
  {  
    "jsonPath": "$.access.key",  
    "recordIndex": 3  
  }  
]
```

Nell'esempio precedente, la scoperta indica che Macie ha rilevato dati sensibili nel terzo valore (riga) del file. In quella riga, l'occorrenza si trova in un campo denominato `key`, che è un elemento secondario di un oggetto denominato `access`.

Sopprimere le scoperte di Macie

Per semplificare l'analisi dei risultati, è possibile creare e utilizzare regole di soppressione. Una regola di soppressione è un insieme di criteri di filtro basati sugli attributi che definisce i casi in cui si desidera che Amazon Macie archivi automaticamente i risultati. Le regole di soppressione sono utili in situazioni in cui hai esaminato una classe di risultati e non desideri riceverne nuovamente una notifica.

Ad esempio, potresti decidere di consentire ai bucket S3 di contenere indirizzi postali, se i bucket non consentono l'accesso pubblico e crittografano automaticamente i nuovi oggetti con un particolare AWS KMS key. In questo caso, puoi creare una regola di soppressione che specifichi i criteri di filtro per i seguenti campi: tipo di rilevamento dei dati sensibili, autorizzazione di accesso pubblico al bucket S3 e id della chiave KMS di crittografia del bucket S3. La regola elimina i risultati futuri che corrispondono ai criteri di filtro.

Se sopprimi i risultati con una regola di soppressione, Macie continua a generare i risultati relativi alle successive occorrenze di dati sensibili e alle potenziali violazioni delle politiche che soddisfano i criteri della regola. Tuttavia, Macie modifica automaticamente lo stato dei risultati in Archiviato. Ciò significa

che i risultati non vengono visualizzati per impostazione predefinita sulla console Amazon Macie, ma persistono in Macie fino alla scadenza. Macie archivia i risultati per 90 giorni.

Inoltre, Macie non pubblica i risultati soppressi su Amazon EventBridge come eventi o come tali. AWS Security Hub Macie, tuttavia, continua a creare e archiviare i [risultati della scoperta di dati sensibili](#) correlati ai dati sensibili che tu sopprimi. Questo aiuta a garantire una cronologia immutabile delle rilevazioni di dati sensibili per i controlli o le indagini sulla privacy e sulla protezione dei dati da te eseguite.

Note

Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, le regole di soppressione potrebbero funzionare in modo diverso per il tuo account. Dipende dalla categoria di risultati che vuoi eliminare e dal fatto che tu abbia un account amministratore o membro di Macie:

- **Risultati delle policy:** solo un amministratore Macie può sopprimere i risultati delle policy per gli account dell'organizzazione.

Se disponi di un account amministratore Macie e crei una regola di soppressione, Macie applica la regola ai risultati delle politiche per tutti gli account dell'organizzazione, a meno che non configuri la regola per escludere account specifici. Se disponi di un account membro e desideri eliminare i risultati delle policy relativi al tuo account, contatta l'amministratore di Macie.

- **Rilevamenti su dati sensibili:** un amministratore di Macie e i singoli membri possono sopprimere i risultati di dati sensibili prodotti dai loro lavori di rilevamento di dati sensibili. Un amministratore Macie può anche eliminare i risultati generati da Macie durante l'individuazione automatica di dati sensibili per l'organizzazione.

Solo l'account che crea un processo di rilevamento di dati sensibili può sopprimere o accedere in altro modo ai risultati di dati sensibili prodotti dal lavoro. Solo l'account amministratore Macie di un'organizzazione può sopprimere o accedere in altro modo ai risultati prodotti dall'individuazione automatica di dati sensibili per gli account dell'organizzazione.

Per ulteriori informazioni sulle attività che gli amministratori e i membri possono eseguire, consulta [Relazioni tra amministratore e account membro di Macie](#)

Argomenti

- [Creazione di una regola di soppressione per i risultati di Macie](#)
- [Analisi dei risultati soppressi in Macie](#)
- [Modifica di una regola di soppressione per i risultati di Macie](#)
- [Eliminazione di una regola di soppressione per i risultati di Macie](#)

Creazione di una regola di soppressione per i risultati di Macie

Una regola di soppressione è un insieme di criteri di filtro basati sugli attributi che definisce i casi in cui si desidera che Amazon Macie archivi automaticamente i risultati. Le regole di soppressione sono utili in situazioni in cui hai esaminato una classe di risultati e non desideri riceverne nuovamente una notifica. Quando create una regola di soppressione, specificate i criteri di filtro, un nome e, facoltativamente, una descrizione della regola. Macie utilizza quindi i criteri della regola per determinare quali risultati archiviare automaticamente. Utilizzando le regole di soppressione, è possibile semplificare l'analisi dei risultati.

Se sopprimi i risultati con una regola di soppressione, Macie continua a generare risultati per le successive occorrenze di dati sensibili e per le potenziali violazioni delle politiche che soddisfano i criteri della regola. Tuttavia, Macie modifica automaticamente lo stato dei risultati in Archiviato. Ciò significa che i risultati non vengono visualizzati per impostazione predefinita sulla console Amazon Macie, ma persistono in Macie fino alla scadenza. (Macie archivia i risultati per 90 giorni.) Ciò significa anche che Macie non pubblica i risultati su Amazon EventBridge come eventi o come tali.

AWS Security Hub

Tieni presente che le regole di soppressione potrebbero funzionare in modo diverso per il tuo account, se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie. Dipende dalla categoria di risultati che vuoi eliminare e dal fatto che tu abbia un account amministratore o membro di Macie:

- **Risultati delle policy:** solo un amministratore Macie può sopprimere i risultati delle policy per gli account dell'organizzazione.

Se disponi di un account amministratore Macie e crei una regola di soppressione, Macie applica la regola ai risultati delle politiche per tutti gli account dell'organizzazione, a meno che non configuri la regola per escludere account specifici. Se disponi di un account membro e desideri eliminare i risultati delle policy relativi al tuo account, collabora con l'amministratore di Macie per eliminarli.

- Rilevamenti relativi a dati sensibili: un amministratore di Macie e i singoli membri possono eliminare i risultati di dati sensibili prodotti dai loro lavori di rilevamento di dati sensibili. Un amministratore Macie può anche eliminare i risultati generati da Macie durante l'individuazione automatica di dati sensibili per l'organizzazione.

Solo l'account che crea un processo di rilevamento di dati sensibili può sopprimere o accedere in altro modo ai risultati di dati sensibili prodotti dal lavoro. Solo l'account amministratore Macie di un'organizzazione può sopprimere o accedere in altro modo ai risultati prodotti dall'individuazione automatica di dati sensibili per gli account dell'organizzazione.

Per ulteriori informazioni sulle attività che gli amministratori e i membri possono eseguire, consulta.

[Relazioni tra amministratore e account membro di Macie](#)

Si noti inoltre che le regole di soppressione sono diverse dalle regole di filtro. Una regola di filtro è un insieme di criteri di filtro che crei e salvi per riutilizzarli quando esamini i risultati sulla console Amazon Macie. Sebbene entrambi i tipi di regole memorizzino e applichino criteri di filtro, una regola di filtro non esegue alcuna azione sui risultati che corrispondono ai criteri della regola. Invece, una regola di filtro determina solo quali risultati vengono visualizzati sulla console dopo l'applicazione della regola. Per ulteriori informazioni, consulta [Definizione delle regole di filtro](#). A seconda degli obiettivi di analisi, potresti decidere che sia meglio creare una regola di filtro anziché una regola di soppressione.

Per creare una regola di soppressione per i risultati

Puoi creare una regola di soppressione utilizzando la console Amazon Macie o l'API Amazon Macie. Prima di creare una regola di soppressione, è importante notare che non è possibile ripristinare (annullare l'archiviazione) i risultati soppressi utilizzando una regola di soppressione. Tuttavia, puoi [esaminare i risultati soppressi](#) utilizzando Macie.

Console

Segui questi passaggi per creare una regola di soppressione utilizzando la console Amazon Macie.

Come creare una regola di eliminazione

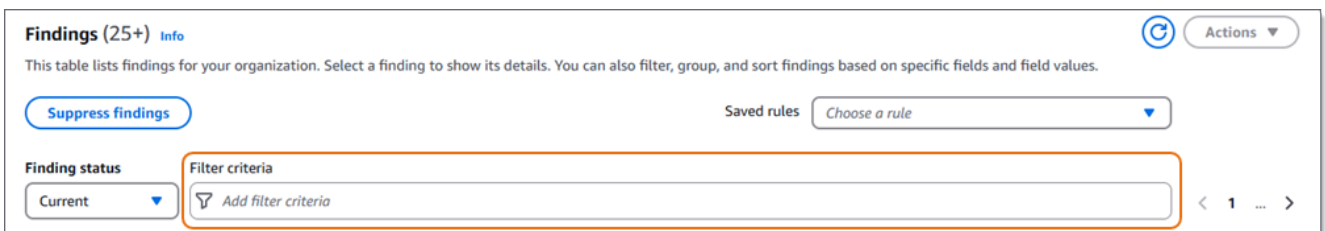
1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.

Tip

Per utilizzare una regola di soppressione o filtro esistente come punto di partenza, scegli la regola dall'elenco Regole salvate.

È inoltre possibile semplificare la creazione di una regola eseguendo innanzitutto il pivot e analizzando i risultati in base a un gruppo logico predefinito. In questo caso, Macie crea e applica automaticamente le condizioni di filtro appropriate, che possono essere un utile punto di partenza per creare una regola. Per fare ciò, scegli Per bucket, Per tipo o Per lavoro nel riquadro di navigazione (sotto Risultati). Quindi scegli un elemento nella tabella. Nel pannello dei dettagli, scegli il link relativo al campo su cui eseguire il pivot.

3. Nella casella Criteri di filtro, aggiungi le condizioni di filtro che specificano gli attributi dei risultati che desideri eliminare dalla regola.



The screenshot shows the 'Findings (25+)' section of the Amazon Macie console. It includes a 'Suppress findings' button, a 'Saved rules' dropdown menu, and a 'Filter criteria' section. The 'Filter criteria' section is highlighted with an orange box and contains a text input field with a filter icon and the placeholder text 'Add filter criteria'. Below the input field is a 'Finding status' dropdown menu set to 'Current'. The interface also features a 'Refresh' button and an 'Actions' dropdown menu.

Per informazioni su come aggiungere condizioni di filtro, consulta [Creazione e applicazione di filtri ai risultati di Macie](#).

4. Quando hai finito di aggiungere le condizioni di filtro per la regola, scegli Sopprimi risultati.
5. In Regola di soppressione, inserisci un nome e, facoltativamente, una descrizione della regola.
6. Seleziona Salva.

API

Per creare una regola di soppressione a livello di codice, utilizza il [CreateFindingsFilter](#) funzionamento dell'API Amazon Macie e specifica i valori appropriati per i parametri richiesti:

- Per il `action` parametro, specifica `ARCHIVE` per assicurarti che Macie sopprima i risultati che corrispondono ai criteri della regola.

- Per il `criterion` parametro, specifica una mappa di condizioni che definiscono i criteri di filtro per la regola.

Nella mappa, ogni condizione deve specificare un campo, un operatore e uno o più valori per il campo. Il tipo e il numero di valori dipendono dal campo e dall'operatore scelti. Per informazioni sui campi, gli operatori e i tipi di valori che è possibile utilizzare in una condizione, vedere:

[Campi per filtrare i risultati di Macie](#), [Utilizzo degli operatori in condizioni](#), e [Specificare i valori per i campi](#).

Per creare una regola di soppressione utilizzando il comando AWS Command Line Interface (AWS CLI), esegui il [create-findings-filter](#) comando e specifica i valori appropriati per i parametri richiesti. Gli esempi seguenti creano una regola di soppressione che restituisce tutti i dati sensibili rilevati negli attuali dati Regione AWS e riporta le occorrenze degli indirizzi postali (e nessun altro tipo di dati sensibili) negli oggetti S3.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (`^`) per migliorare la leggibilità.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={"criterion\":
{"classificationDetails.result.sensitiveData.detections.type\":{"eqExactMatch\":
["ADDRESS"]}}}
```

Dove:

- *my_suppression_rule* è il nome personalizzato per la regola.
- *criterion* è una mappa delle condizioni di filtro per la regola:

- `classificationDetails.result.sensitiveData.detections.type` è il nome JSON del campo Tipo di rilevamento dei dati sensibili.
- `eqExactMatch` specifica l'operatore equals exact match.
- `ADDRESS` è un valore enumerato per il campo Tipo di rilevamento dei dati sensibili.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-aa2f-4940-b347-d1451example",
  "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

`arn` è l'Amazon Resource Name (ARN) della regola di soppressione che è stata creata e `id` l'identificatore univoco della regola.

Per ulteriori esempi di criteri di filtro, consulta [Filtraggio dei risultati in modo programmatico con l'API Amazon Macie](#)

Analisi dei risultati soppressi in Macie

Se sopprimi i risultati con una regola di soppressione, Amazon Macie continua a generare risultati per successive occorrenze di dati sensibili e potenziali violazioni delle politiche che soddisfano i criteri della regola. Tuttavia, Macie modifica automaticamente lo stato dei risultati in archiviati. Ciò significa che i risultati non vengono visualizzati per impostazione predefinita sulla console Amazon Macie, ma persistono in Macie fino alla scadenza. (Macie archivia i risultati per 90 giorni.) Ciò significa anche che Macie non pubblica i risultati su Amazon EventBridge come eventi o come tali. AWS Security Hub

Poiché i risultati soppressi persistono in Macie per un massimo di 90 giorni, puoi accedervi e rivederli prima che scadano. Oltre ad ampliare l'analisi dei risultati, questo può aiutarvi a determinare se modificare i criteri di soppressione. Per modificare i criteri, [modifica le regole di soppressione per il tuo account](#).

Puoi esaminare i risultati soppressi sulla console Amazon Macie modificando le impostazioni del filtro.

Per esaminare i risultati soppressi sulla console

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti. La pagina Risultati mostra i risultati che Macie ha creato o aggiornato per il tuo account Regione AWS negli ultimi 90 giorni. Per impostazione predefinita, questo non include i risultati che sono stati soppressi da una regola di soppressione.
3. Per analizzare e analizzare i risultati in base a un gruppo logico predefinito, scegli Per bucket, Per tipo o Per processo nel riquadro di navigazione (sotto Risultati).
4. Per lo stato di ricerca, effettuate una delle seguenti operazioni:
 - Per visualizzare solo i risultati soppressi, scegliete Archiviato.
 - Per visualizzare sia i risultati soppressi che quelli non soppressi, scegliete Tutti.
 - Per nascondere nuovamente i risultati soppressi, scegliete Corrente.

Puoi anche accedere ai risultati soppressi utilizzando l'API Amazon Macie. Per recuperare un elenco di risultati soppressi, usa l'operazione. [ListFindings](#) Nella richiesta, includi una condizione di filtro che specifichi `true` il campo. `archived` Per un esempio di come eseguire questa operazione utilizzando AWS Command Line Interface (AWS CLI), vedi [Filtraggio dei risultati a livello di codice](#). Per recuperare quindi i dettagli di uno o più risultati soppressi, utilizzate l'[GetFindings](#) operazione. Nella richiesta, specificate l'identificatore univoco per ogni risultato da recuperare.

Note

Mentre esaminate i risultati, tenete presente che le regole di soppressione possono funzionare in modo diverso per gli account che fanno parte di un'organizzazione. Dipende dalla categoria dei risultati e dal fatto che tu abbia un account amministratore o membro di Macie:

- Risultati delle policy: solo un amministratore Macie può sopprimere i risultati delle policy per gli account dell'organizzazione.

Se disponi di un account amministratore Macie e hai creato una regola di soppressione, Macie applica la regola ai risultati delle politiche per tutti gli account dell'organizzazione, a meno che tu non abbia configurato la regola per escludere account specifici. Se disponi di un account membro e desideri eliminare i risultati delle policy relativi al tuo account, collabora con l'amministratore di Macie per eliminarli.

- Rilevamenti relativi a dati sensibili: un amministratore di Macie e i singoli membri possono eliminare i risultati di dati sensibili prodotti dai loro lavori di rilevamento di dati sensibili. Un amministratore Macie può anche eliminare i risultati generati da Macie durante l'individuazione automatica di dati sensibili per l'organizzazione.

Solo l'account che crea un processo di rilevamento di dati sensibili può sopprimere o accedere in altro modo ai risultati di dati sensibili prodotti dal lavoro. Solo l'account amministratore Macie di un'organizzazione può sopprimere o accedere in altro modo ai risultati prodotti dall'individuazione automatica di dati sensibili per gli account dell'organizzazione.

Per ulteriori informazioni sulle attività che gli amministratori e i membri possono eseguire, consulta [Relazioni tra amministratore e account membro di Macie](#)

Modifica di una regola di soppressione per i risultati di Macie

Dopo aver creato una regola di soppressione, è possibile modificare le impostazioni della regola. Una regola di soppressione è un insieme di criteri di filtro basati sugli attributi che definisce i casi in cui si desidera che Amazon Macie archivi automaticamente i risultati. Le regole di soppressione sono utili in situazioni in cui hai esaminato una classe di risultati e non desideri riceverne nuovamente una notifica. Ogni regola è composta da un insieme di criteri di filtro, un nome e, facoltativamente, una descrizione.

Se si modificano i criteri di una regola di soppressione, i risultati precedentemente soppressi dalla regola continuano a essere soppressi. I risultati continuano ad avere lo stato di archiviato e Macie non li pubblica su Amazon EventBridge o AWS Security Hub Macie applica i nuovi criteri solo ai nuovi risultati relativi ai dati sensibili, alle nuove conclusioni relative alle politiche e alle successive occorrenze di scoperte relative alle politiche esistenti.

Oltre a modificare i criteri o altre impostazioni di una regola, puoi assegnare tag a una regola. Un tag è un'etichetta che definisci e assegni a determinati tipi di AWS risorse. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Per ulteriori informazioni, consulta [Etichettare le risorse di Macie](#).

Per modificare una regola di soppressione dei risultati

Per assegnare tag o modificare le impostazioni per una regola di soppressione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per assegnare tag o modificare le impostazioni per una regola di soppressione utilizzando la console Amazon Macie.

Per modificare una regola di soppressione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Nell'elenco delle regole salvate, scegli l'icona di modifica ) accanto alla regola di soppressione a cui desideri modificare o assegnare i tag.
4. Effettua una delle seguenti operazioni:
 - Per modificare i criteri della regola, utilizza la casella Criteri di filtro. Nella casella, inserite le condizioni che specificano gli attributi dei risultati che desiderate che la regola sopprima. Per scoprire come, consulta [Creazione e applicazione di filtri ai risultati di Macie](#).
 - Per modificare il nome della regola, inserite un nuovo nome nella casella Nome sotto Regola di soppressione.
 - Per modificare la descrizione della regola, inserite una nuova descrizione nella casella Descrizione sotto Regola di soppressione.
 - Per assegnare tag alla regola, scegli Gestisci tag in Regola di soppressione. Quindi aggiungi, rivedi e modifica i tag secondo necessità. Una regola può avere fino a 50 tag.
5. Una volta completate le modifiche, scegliere Save (Salva).

API

Per modificare una regola di soppressione a livello di codice, utilizza il [UpdateFindingsFilter](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza i parametri supportati per specificare un nuovo valore per ogni impostazione che desideri modificare.

Per il `id` parametro, specifica l'identificatore univoco della regola da modificare. Puoi ottenere questo identificatore utilizzando l'[ListFindingsFilter](#) operazione per recuperare un elenco di regole

di soppressione e filtro per il tuo account. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il [list-findings-filters](#) comando per recuperare questo elenco.

Per modificare una regola di soppressione utilizzando il AWS CLI, esegui il [update-findings-filter](#) comando e utilizza i parametri supportati per specificare un nuovo valore per ogni impostazione che desideri modificare. Ad esempio, il comando seguente modifica il nome di una regola di soppressione esistente.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --  
name mailing_addresses_only
```

Dove:

- **8a3c5608-aa2f-4940-b347-d1451example** è l'identificatore univoco della regola.
- **mailing_addresses_only** è il nuovo nome della regola.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{  
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-  
aa2f-4940-b347-d1451example",  
  "id": "8a3c5608-aa2f-4940-b347-d1451example"  
}
```

arnDov'è l'Amazon Resource Name (ARN) della regola che è stata modificata ed id è l'identificatore univoco della regola.

Analogamente, l'esempio seguente converte una [regola di filtro](#) in una regola di soppressione modificando il valore del parametro da `action NOOP ARCHIVE`

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --  
action ARCHIVE
```

Dove:

- **8a1c3508-aa2f-4940-b347-d1451example** è l'identificatore univoco della regola.
- **ARCHIVE** è la nuova azione che Macie deve eseguire sui risultati che corrispondono ai criteri della regola: sopprime i risultati.

Se il comando viene eseguito correttamente, si ottiene un output simile al seguente:

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-aa2f-4940-b347-d1451example",
  "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

`arn` è l'Amazon Resource Name (ARN) della regola che è stata modificata ed `id` è l'identificatore univoco della regola.

Eliminazione di una regola di soppressione per i risultati di Macie

È possibile eliminare una regola di soppressione in qualsiasi momento. Se elimini una regola di soppressione, Amazon Macie interrompe la soppressione di nuove e successive occorrenze di risultati che soddisfano i criteri della regola e non sono soppressi da altre regole. Tieni presente, tuttavia, che Macie potrebbe continuare a sopprimere i risultati che è attualmente in fase di elaborazione e che corrispondono ai criteri della regola.

Dopo aver eliminato una regola di soppressione, le nuove e successive occorrenze dei risultati che corrispondono ai criteri della regola hanno lo stato corrente (non archiviato). Ciò significa che vengono visualizzati per impostazione predefinita sulla console Amazon Macie. Inoltre, Macie li pubblica su Amazon EventBridge come eventi. A seconda delle [impostazioni di pubblicazione del](#) tuo account, Macie pubblica i risultati anche su AWS Security Hub.

Per eliminare una regola di soppressione per i risultati

Puoi eliminare una regola di soppressione utilizzando la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per eliminare una regola di soppressione utilizzando la console Amazon Macie.

Per eliminare una regola di soppressione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel riquadro di navigazione, seleziona Esiti.

3. Nell'elenco delle regole salvate, scegli l'icona di modifica
() accanto alla regola di soppressione che desideri eliminare.
4. In Regola di soppressione, scegliete Elimina.

API

Per eliminare una regola di soppressione a livello di codice, utilizza il [DeleteFindingsFilter](#) funzionamento dell'API Amazon Macie. Per il `id` parametro, specifica l'identificatore univoco per la regola di soppressione da eliminare. Puoi ottenere questo identificatore utilizzando l'[ListFindingsFilter](#) operazione per recuperare un elenco di regole di soppressione e filtro per il tuo account. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il [list-findings-filters](#) comando per recuperare questo elenco.

Per eliminare una regola di soppressione utilizzando il AWS CLI, esegui il comando. [delete-findings-filter](#) Per esempio:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

8a3c5608-aa2f-4940-b347-d1451example Dov'è l'identificatore univoco per la regola di soppressione da eliminare.

Se il comando viene eseguito correttamente, Macie restituisce una risposta HTTP 200 vuota. Altrimenti, Macie restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Monitoraggio ed elaborazione dei risultati di Macie

Per supportare l'integrazione con altre applicazioni, servizi e sistemi, come i sistemi di monitoraggio o di gestione degli eventi, Amazon Macie pubblica automaticamente i risultati delle policy e dei dati sensibili su Amazon EventBridge come eventi. Per ulteriore assistenza e un'analisi più ampia del livello di sicurezza della tua organizzazione, puoi configurare Macie in modo che pubblichi anche i risultati relativi a policy e dati sensibili. AWS Security Hub

Amazon EventBridge

Amazon EventBridge, precedentemente Amazon CloudWatch Events, è un servizio di bus eventi senza server che fornisce un flusso di dati in tempo reale da applicazioni e servizi e indirizza tali dati verso destinazioni come funzioni AWS Lambda, argomenti di Amazon Simple Notification Service e flussi Amazon Kinesis. Con EventBridge, puoi automatizzare il monitoraggio e l'elaborazione di determinati tipi di eventi, inclusi gli eventi pubblicati da Macie a scopo di rilevazione. Per ulteriori informazioni, consulta [Elaborazione dei risultati con Amazon EventBridge](#).

Se ti integri Notifiche all'utente AWS con Macie, puoi anche utilizzare EventBridge gli eventi per generare automaticamente notifiche sugli eventi che Macie pubblica per i risultati. Con Notifiche all'utente, puoi creare regole personalizzate e configurare i canali di consegna per ricevere notifiche sugli EventBridge eventi di interesse. I canali di distribuzione includono e-mail, Amazon Q Developer nelle applicazioni di chat e notifiche push in AWS Console Mobile Application. Puoi anche esaminare le notifiche in una posizione centrale su AWS Management Console. Per ulteriori informazioni, consulta [Monitoraggio dei risultati con Notifiche all'utente AWS](#).

AWS Security Hub

AWS Security Hub è un servizio di sicurezza che fornisce una visione completa dello stato di sicurezza in tutto l'AWS ambiente. Raccoglie dati di sicurezza dalle soluzioni di AWS Partner Network sicurezza supportate Servizi AWS e consente di verificare la conformità dell'ambiente agli standard e alle best practice del settore della sicurezza. Inoltre, consente di analizzare le tendenze in materia di sicurezza e identificare problemi ad alta priorità.

Con Security Hub, puoi esaminare e valutare i risultati di Macie come parte di un'analisi più ampia del livello di sicurezza della tua organizzazione. Puoi anche aggregare i risultati di più risultati e monitorare ed elaborare Regioni AWS i dati aggregati dei risultati provenienti da una singola regione. Per ulteriori informazioni, consulta [Valutazione dei risultati con AWS Security Hub](#).

Quando Macie crea un risultato, lo pubblica automaticamente EventBridge come nuovo evento. A seconda delle impostazioni di pubblicazione scelte per il tuo account, Macie può anche pubblicare i risultati su Security Hub. Macie pubblica ogni nuovo risultato immediatamente dopo aver terminato l'elaborazione del risultato. Se Macie rileva una successiva ricorrenza di una decisione politica esistente, pubblica un aggiornamento dell'evento esistente EventBridge relativo alla scoperta. A seconda delle impostazioni di pubblicazione, Macie può anche pubblicare l'aggiornamento su Security Hub. Macie pubblica questi aggiornamenti su base ricorrente, utilizzando una frequenza di pubblicazione specificata nelle impostazioni di pubblicazione del tuo account.

Oltre alle opzioni precedenti, puoi interrogare e recuperare i dati dei risultati direttamente utilizzando l'API Amazon Macie. L'API Amazon Macie offre un accesso completo e programmatico ai dati. Per interrogare i dati, puoi inviare richieste HTTPS direttamente a Macie o utilizzare una versione corrente di un AWS SDK o uno strumento da riga di comando. AWS Se esegui una query sui dati, Macie restituisce i risultati in una risposta JSON. È quindi possibile passare i risultati a un altro servizio o applicazione per ulteriori elaborazioni, monitoraggio o report. Per ulteriori informazioni, consulta [Amazon Macie API Reference](#).

Argomenti

- [Configurazione delle impostazioni di pubblicazione per i risultati di Macie](#)
- [Elaborazione dei risultati di Macie con Amazon EventBridge](#)
- [Monitoraggio dei risultati di Macie con Notifiche all'utente AWS](#)
- [Valutazione dei risultati di Macie con AWS Security Hub](#)
- [Schema di EventBridge eventi Amazon per i risultati di Macie](#)

Configurazione delle impostazioni di pubblicazione per i risultati di Macie

Per supportare l'integrazione con altre applicazioni, servizi e sistemi, Amazon Macie pubblica automaticamente su Amazon EventBridge sia i risultati delle policy che i dati sensibili sotto forma di eventi. Per informazioni su come monitorare ed elaborare EventBridge i risultati, consulta.

[Elaborazione dei risultati con Amazon EventBridge](#)

Puoi configurare Macie in modo che pubblichi automaticamente i risultati AWS Security Hub anche su, utilizzando le opzioni di destinazione che specifichi nelle impostazioni di pubblicazione del tuo account. Con queste opzioni, puoi configurare Macie in modo che pubblichi solo i risultati delle

policy, solo i risultati dei dati sensibili o entrambi i risultati delle policy e dei dati sensibili su Security Hub. Puoi anche configurare Macie per interrompere la pubblicazione di qualsiasi risultato su Security Hub. Per informazioni su come utilizzare Security Hub per valutare ed elaborare i risultati, vedere [Valutazione dei risultati con AWS Security Hub](#).

Per quanto riguarda i risultati delle politiche, la tempistica con cui Macie pubblica una scoperta per un altro utente Servizio AWS dipende dal fatto che la scoperta sia nuova e dalla frequenza di pubblicazione specificata per il proprio account. Per le rilevazioni di dati sensibili, la tempistica è sempre immediata: Macie pubblica un risultato relativo a dati sensibili subito dopo aver terminato l'elaborazione del risultato. A differenza dei risultati delle politiche, Macie considera tutti i risultati relativi ai dati sensibili come nuovi (unici).

[Tieni presente che Macie non pubblica i risultati delle policy o dei dati sensibili che vengono archiviati automaticamente in base a una regola di soppressione.](#) In altre parole, Macie non pubblica i risultati soppressi ad altri. Servizi AWS

Argomenti

- [Scelta delle destinazioni di pubblicazione dei risultati](#)
- [Modifica della frequenza di pubblicazione dei risultati](#)

Scelta delle destinazioni di pubblicazione dei risultati

Puoi configurare Amazon Macie per pubblicare automaticamente i risultati delle policy e dei dati sensibili oltre che AWS Security Hub su Amazon. EventBridge Per impostazione predefinita, Macie pubblica solo i risultati delle policy nuovi e aggiornati su Security Hub. Per modificare o estendere la configurazione predefinita, modifica le impostazioni della destinazione di pubblicazione per il tuo account.

Quando modifichi le impostazioni di destinazione, scegli le categorie di risultati che desideri che Macie pubblichi su Security Hub: solo i risultati delle politiche, solo i risultati dei dati sensibili o i risultati sia delle policy che dei dati sensibili. Puoi anche scegliere di interrompere la pubblicazione di qualsiasi categoria di risultati su Security Hub.

Se modifichi le impostazioni di destinazione, la modifica si applica solo a quella attuale Regione AWS. Se sei l'amministratore Macie di un'organizzazione, la modifica si applica solo al tuo account. Non si applica agli account dei membri della tua organizzazione. Per ulteriori informazioni, consulta [Gestione di più account](#).

Per scegliere le destinazioni di pubblicazione dei risultati

Segui questi passaggi per modificare le impostazioni di destinazione utilizzando la console Amazon Macie. Per eseguire questa operazione a livello di codice, utilizza il [PutFindingsPublicationConfiguration](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella sezione Pubblicazione dei risultati, in Destinazioni, scegli tra le seguenti opzioni:
 - **Pubblica i risultati delle policy su Security Hub:** seleziona questa casella di controllo per iniziare a pubblicare automaticamente i risultati delle policy nuovi e aggiornati su Security Hub. Per interrompere la pubblicazione dei risultati delle policy nuovi e aggiornati su Security Hub, deseleziona questa casella di controllo.

Se selezioni questa casella di controllo e disponi di risultati delle politiche esistenti, Macie non li pubblica su Security Hub. Macie pubblica invece solo i risultati delle policy che crea o aggiorna dopo aver salvato la modifica.

- **Pubblica i risultati dei dati sensibili su Security Hub:** seleziona questa casella di controllo per iniziare a pubblicare automaticamente i nuovi risultati relativi ai dati sensibili su Security Hub. Per interrompere la pubblicazione di nuovi risultati relativi ai dati sensibili su Security Hub, deseleziona questa casella di controllo.

Se selezioni questa casella di controllo e disponi di dati sensibili esistenti, Macie non li pubblica su Security Hub. Macie pubblica invece solo i risultati relativi ai dati sensibili che crea dopo il salvataggio delle modifiche.

4. Seleziona Salva.

Se hai scelto di pubblicare qualsiasi categoria di risultati su Security Hub, assicurati di abilitare anche Security Hub nella regione corrente e di configurarlo per accettare i risultati di Macie. Altrimenti, non potrai accedere ai risultati in Security Hub. Per informazioni su come accettare i risultati in Security Hub, consulta [Abilitazione e gestione delle integrazioni](#) nella Guida per l'AWS Security Hub utente.

Modifica della frequenza di pubblicazione dei risultati

In Amazon Macie, ogni risultato ha un identificatore univoco. Macie utilizza questo identificatore per determinare quando pubblicare un risultato su un altro: Servizio AWS

- **Nuove scoperte:** quando Macie crea una nuova policy o una scoperta di dati sensibili, assegna un identificatore univoco alla scoperta come parte dell'elaborazione della scoperta. Immediatamente dopo che Macie ha terminato l'elaborazione del risultato, lo pubblica su Amazon EventBridge come nuovo evento. A seconda delle impostazioni di pubblicazione del tuo account, Macie pubblica la scoperta anche come nuova scoperta in AWS Security Hub.
- **Risultati aggiornati:** quando Macie rileva una ricorrenza successiva di una decisione politica esistente, aggiorna la scoperta esistente aggiungendo dettagli sull'occorrenza successiva e incrementando il numero di ricorrenze. Macie pubblica anche questi aggiornamenti all'EventBridge evento esistente e, a seconda delle impostazioni di pubblicazione per l'account, ai risultati esistenti del Security Hub. Per impostazione predefinita, Macie pubblica gli aggiornamenti ogni 15 minuti come parte di un ciclo di pubblicazione ricorrente. Ciò significa che tutti i risultati delle politiche aggiornati dopo il ciclo di pubblicazione più recente verranno conservati, aggiornati nuovamente se necessario e inclusi nel ciclo di pubblicazione successivo (circa 15 minuti dopo).

È possibile modificare la frequenza con cui Macie pubblica gli aggiornamenti ai risultati delle politiche esistenti in altri Servizi AWS. Ad esempio, potresti configurare Macie per pubblicare gli aggiornamenti ogni ora. Se esegui questa operazione e una pubblicazione viene pubblicata alle 12:00, tutti gli aggiornamenti che si verificano dopo le 12:00 vengono pubblicati alle 13:00.

Se si modifica la frequenza, la modifica si applica solo alla frequenza corrente. Regione AWS Se sei l'amministratore Macie di un'organizzazione, la modifica si applica anche a tutti gli account dei membri dell'organizzazione. Per ulteriori informazioni, consulta [Gestione di più account](#).

Per modificare la frequenza di pubblicazione dei risultati aggiornati

Segui questi passaggi per modificare la frequenza di pubblicazione utilizzando la console Amazon Macie. Per eseguire questa operazione a livello di codice, utilizza il [UpdateMacieSession](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella sezione Pubblicazione dei risultati, in Frequenza di aggiornamento dei risultati delle politiche, scegli la frequenza con cui desideri che Macie pubblichi gli aggiornamenti ai risultati delle politiche in altri siti. Servizi AWS
4. Seleziona Salva.

Elaborazione dei risultati di Macie con Amazon EventBridge

Amazon EventBridge, precedentemente Amazon CloudWatch Events, è un servizio di bus eventi senza server. EventBridge fornisce un flusso di dati in tempo reale da applicazioni e servizi e indirizza tali dati verso destinazioni quali AWS Lambda funzioni, argomenti di Amazon Simple Notification Service (Amazon SNS) e flussi Amazon Kinesis. Per ulteriori informazioni su EventBridge, consulta la [Amazon EventBridge User Guide](#).

Con EventBridge, puoi automatizzare il monitoraggio e l'elaborazione di determinati tipi di eventi. Ciò include gli eventi che Amazon Macie pubblica automaticamente in base a nuove policy e rilevazioni di dati sensibili. Sono inclusi anche gli eventi che Macie pubblica automaticamente in caso di successive rilevazioni di policy esistenti. Per dettagli su come e quando Macie pubblica questi eventi, vedi. [Configurazione delle impostazioni di pubblicazione per i risultati](#)

Utilizzando EventBridge gli eventi pubblicati da Macie per i risultati, puoi monitorare ed elaborare i risultati quasi in tempo reale. È quindi possibile agire in base ai risultati utilizzando altre applicazioni e servizi. Ad esempio, è possibile utilizzare EventBridge per inviare tipi specifici di nuovi risultati a una AWS Lambda funzione. La funzione Lambda potrebbe quindi elaborare e inviare i dati al sistema di gestione degli incidenti e degli eventi di sicurezza (SIEM). Se esegui l'[integrazione Notifiche all'utente AWS con Macie](#), puoi anche utilizzare gli eventi per ricevere automaticamente notifiche dei risultati tramite i canali di distribuzione da te specificati.

Oltre al monitoraggio e all'elaborazione automatizzati, l'uso di EventBridge consente la conservazione a lungo termine dei dati dei risultati. Macie archivia i risultati per 90 giorni. Con EventBridge, puoi inviare i dati dei risultati alla tua piattaforma di archiviazione preferita e archivarli per tutto il tempo che desideri.

Note

Per una conservazione a lungo termine, configura anche Macie per archiviare i risultati della scoperta dei dati sensibili in un bucket S3. Un risultato di scoperta di dati sensibili è un record che registra i dettagli dell'analisi eseguita da Macie su un oggetto S3 per determinare se l'oggetto contiene dati sensibili. Per ulteriori informazioni, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

Argomenti

- [Lavorare con Amazon EventBridge](#)

- [Creazione di EventBridge regole Amazon per i risultati di Macie](#)

Lavorare con Amazon EventBridge

Con Amazon EventBridge, crei regole per specificare quali eventi vuoi monitorare e quali obiettivi desideri eseguire azioni automatizzate per tali eventi. Un target è una destinazione a cui EventBridge invia eventi.

Per automatizzare le attività di monitoraggio ed elaborazione dei risultati, puoi creare una EventBridge regola che rileva automaticamente gli eventi di ricerca di Amazon Macie e li invia a un'altra applicazione o servizio per l'elaborazione o altre azioni. Puoi personalizzare la regola per inviare solo gli eventi che soddisfano determinati criteri. A tale scopo, specificate i criteri che derivano da. [Schema di EventBridge eventi Amazon per i risultati di Macie](#)

Ad esempio, è possibile creare una regola che invia tipi specifici di nuovi risultati a una AWS Lambda funzione. La funzione Lambda può quindi eseguire attività come: elaborare e inviare i dati al sistema SIEM; applicare automaticamente un certo tipo di crittografia lato server a un oggetto S3; oppure limitare l'accesso a un oggetto S3 modificando l'elenco di controllo degli accessi (ACL) dell'oggetto. Oppure puoi creare una regola che invii automaticamente nuovi risultati ad alta gravità a un argomento di Amazon SNS, che a sua volta notifica la scoperta al team di risposta agli incidenti.

Oltre a richiamare le funzioni Lambda e notificare EventBridge gli argomenti di Amazon SNS, supporta altri tipi di obiettivi e azioni, come l'inoltro di eventi ai AWS Step Functions flussi di Amazon Kinesis, l'attivazione di macchine a stati e la chiamata del comando run. AWS Systems Manager Per informazioni sulle destinazioni supportate, consulta [Event bus targets](#) nella Amazon EventBridge User Guide.

Creazione di EventBridge regole Amazon per i risultati di Macie

Le seguenti procedure spiegano come utilizzare la EventBridge console Amazon e [AWS Command Line Interface \(AWS CLI\)](#) per creare una EventBridge regola per i risultati di Amazon Macie. La regola rileva EventBridge gli eventi che utilizzano lo schema e il pattern degli eventi per i risultati di Macie e invia tali eventi a una AWS Lambda funzione per l'elaborazione.

AWS Lambda è un servizio di elaborazione che è possibile utilizzare per eseguire codice senza fornire o gestire server. Impacchettate il codice e lo caricate AWS Lambda come funzione Lambda. AWS Lambda quindi esegue la funzione quando la funzione viene richiamata. Puoi richiamare una funzione manualmente, come risposta automatica agli eventi o in risposta a richieste provenienti

da applicazioni o servizi. Per ulteriori informazioni su come creare e richiamare le funzioni Lambda, consulta [Guida per gli sviluppatori di AWS Lambda](#).

Console

Segui questi passaggi per utilizzare la EventBridge console Amazon per creare una regola che invii automaticamente tutti gli eventi di ricerca di Macie a una funzione Lambda per l'elaborazione. La regola utilizza le impostazioni predefinite per le regole che vengono eseguite quando vengono ricevuti eventi specifici. Per dettagli sulle impostazioni delle regole o per scoprire come creare una regola che utilizza impostazioni personalizzate, consulta [Creazione di regole che reagiscono agli eventi](#) nella Amazon EventBridge User Guide.

Tip

Puoi anche creare una regola che utilizzi uno schema personalizzato per rilevare e agire solo su un sottoinsieme di eventi di ricerca di Macie. Questo sottoinsieme può essere basato su campi specifici che Macie include in un evento di ricerca. Per maggiori informazioni sui campi disponibili, consulta [Schema di EventBridge eventi Amazon per i risultati di Macie](#). Per ulteriori informazioni sull'utilizzo di modelli personalizzati nelle regole, consulta la sezione [Creazione di modelli di eventi](#) nella Amazon EventBridge User Guide.

Prima di creare questa regola, create la funzione Lambda che desiderate che la regola utilizzi come destinazione. Quando crei la regola, dovrai specificare questa funzione come sua destinazione.

Per creare una regola di evento utilizzando la console

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, in Autobus, scegli Regole.
3. Nella sezione Rules (Regole), scegli Create rule (Crea regola).
4. Nella pagina di dettaglio Definisci regola, procedi come segue:
 - In Name (Nome), inserisci un nome per la regola.
 - (Facoltativo) In Descrizione, inserisci una breve descrizione della regola.
 - Per Event bus, assicuratevi che sia selezionato il valore predefinito e che l'opzione Abilita la regola sul bus eventi selezionato sia attivata.

- Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
5. Al termine, selezionare Next (Avanti).
 6. Nella pagina Crea modello di eventi, procedi come segue:
 - Per Origine evento, scegli AWS eventi o eventi EventBridge partner.
 - (Facoltativo) Per un evento di esempio, esamina un esempio di evento di ricerca per Macie per scoprire cosa potrebbe contenere un evento. Per fare ciò, scegli AWS gli eventi. Quindi, per gli eventi di esempio, scegli Macie Finding.
 - In Metodo di creazione scegli Utilizza modulo del modello.
 - Per Event pattern, inserisci le seguenti impostazioni:
 - In Event source (Origine eventi), selezionare Servizi AWS.
 - Per Servizio AWS, scegli Macie.
 - Per Tipo di evento, scegli Macie Finding.
 7. Al termine, selezionare Next (Avanti).
 8. Nella pagina Seleziona destinazioni, procedi come segue:
 - Per Target types (Tipi di target), scegli Servizio AWS.
 - Per Select a target (Seleziona destinazione), scegli Lambda function (Funzione Lambda). Quindi, per Funzione, scegliete la funzione Lambda a cui inviare gli eventi di ricerca.
 - Per Configura versione/alias, inserisci le impostazioni della versione e dell'alias per la funzione Lambda di destinazione.
 - (Facoltativo) Per Impostazioni aggiuntive, immettete impostazioni personalizzate per specificare quali dati degli eventi desiderate inviare alla funzione Lambda. Puoi anche specificare come gestire gli eventi che non vengono consegnati correttamente alla funzione.
 9. Al termine, selezionare Next (Avanti).
 10. Nella pagina Configura tag, inserisci facoltativamente uno o più tag da assegnare alla regola. Quindi scegli Successivo.
 11. Nella pagina Rivedi e crea, rivedi le impostazioni della regola e verifica che siano corrette.

Per modificare un'impostazione, scegli Modifica nella sezione che contiene l'impostazione, quindi inserisci l'impostazione corretta. Puoi anche utilizzare le schede di navigazione per andare alla pagina che contiene un'impostazione.

12. Al termine della verifica delle impostazioni, scegli Crea regola.

AWS CLI

Segui questi passaggi per AWS CLI creare una EventBridge regola che invii tutti gli eventi di ricerca di Macie a una funzione Lambda per l'elaborazione. La regola utilizza le impostazioni predefinite per le regole che vengono eseguite quando vengono ricevuti eventi specifici. In questa procedura, i comandi sono formattati per Microsoft Windows. Per Linux, macOS o Unix, sostituisci il carattere di continuazione di riga del cursore (^) con una barra rovesciata (\).

Prima di creare questa regola, create la funzione Lambda che desiderate che la regola utilizzi come destinazione. Quando crei la funzione, annota l'Amazon Resource Name (ARN) della funzione. Dovrai inserire questo ARN quando specificherai la destinazione della regola.

Per creare una regola di evento utilizzando AWS CLI

1. Crea una regola che rilevi gli eventi per tutti i risultati pubblicati da Macie. EventBridge [Per fare ciò, esegui il comando put-rule. EventBridge](#) Per esempio:

```
C:\> aws events put-rule ^  
--name MacieFindings ^  
--event-pattern "{\"source\":\"[\"aws.macie\"]}\"
```

MacieFindings Dov'è il nome che desideri per la regola.

Tip

Puoi anche creare una regola che utilizzi un pattern personalizzato (event-pattern) per rilevare e agire solo su un sottoinsieme di eventi di ricerca di Macie. Questo sottoinsieme può essere basato su campi specifici che Macie include in un evento di ricerca. Per maggiori informazioni sui campi disponibili, consulta. [Schema di EventBridge eventi Amazon per i risultati di Macie](#) Per ulteriori informazioni sull'utilizzo di modelli personalizzati nelle regole, consulta la sezione [Creazione di modelli di eventi](#) nella Amazon EventBridge User Guide.

Se il comando viene eseguito correttamente, EventBridge risponde con l'ARN della regola. Prendi nota di questo ARN. Dovrai inserirlo una volta arrivato alla fase 3.

2. Specificate la funzione Lambda da utilizzare come destinazione per la regola. Per fare ciò, esegui il comando EventBridge [put-targets](#). Per esempio:

```
C:\> aws events put-targets ^  
--rule MacieFindings ^  
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-  
findings-function
```

Dove *MacieFindings* è il nome specificato per la regola nel passaggio 1 e il valore del Arn parametro è l'ARN della funzione che si desidera che la regola utilizzi come destinazione.

3. Aggiungi le autorizzazioni che consentono alla regola di richiamare la funzione Lambda di destinazione. A tale scopo, esegui il comando Lambda [add-permission](#). Per esempio:

```
C:\> aws lambda add-permission ^  
--function-name my-findings-function ^  
--statement-id Sid ^  
--action lambda:InvokeFunction ^  
--principal events.amazonaws.com ^  
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

Dove:

- *my-findings-function* è il nome della funzione Lambda che si desidera che la regola utilizzi come destinazione.
- *Sid* è un identificatore di istruzione che definisci per descrivere l'istruzione nella policy della funzione Lambda.
- *source-arn* è l'ARN della EventBridge regola.

Se il comando viene eseguito correttamente, si ottiene un output simile al seguente:

```
{  
  "Statement": "{\"Sid\":\"sid\",  
    \"Effect\":\"Allow\",  
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},  
    \"Action\":\"lambda:InvokeFunction\",  
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-  
function\",  
    \"Condition\":  
      {\"ArnLike\":
```

```
{\ "AWS:SourceArn\":  
  \ "arn:aws:events:us-east-1:111122223333:rule/MacieFindings\ "}}}  
}
```

Il valore di `Statement` è una versione in formato stringa JSON dell'istruzione aggiunta alla policy della funzione Lambda.

Monitoraggio dei risultati di Macie con Notifiche all'utente AWS

Notifiche all'utente AWS è un servizio che funge da posizione centrale per le AWS notifiche su. AWS Management Console Ciò include notifiche come CloudWatch allarmi Amazon, Supporto AWS casi e comunicazioni da altri Servizi AWS. Con Notifiche all'utente, puoi configurare regole e canali di consegna personalizzati per ricevere notifiche su determinati tipi di EventBridge eventi Amazon. I canali di distribuzione includono e-mail, Amazon Q Developer nelle applicazioni di chat e notifiche push in AWS Console Mobile Application. Puoi anche controllare le notifiche sulla Notifiche all'utente AWS console. Per ulteriori informazioni Notifiche all'utente, consulta la [Guida Notifiche all'utente AWS per l'utente](#).

Amazon Macie si integra con Notifiche all'utente AWS, il che significa che puoi configurarlo Notifiche all'utente per notificarti gli eventi su cui Macie pubblica informazioni EventBridge relative a policy e dati sensibili. Se un evento di ricerca soddisfa i criteri specificati, Notifiche all'utente genera una notifica. La notifica include i dettagli chiave del risultato associato, come il tipo e la gravità del risultato e il nome della risorsa interessata. Notifiche all'utente può anche inviare la notifica a uno o più canali di distribuzione specificati dall'utente. Puoi personalizzare la tua scelta di canali di distribuzione per allinearla ai tuoi flussi di lavoro di sicurezza e conformità.

Ad esempio, potresti configurare la generazione Notifiche all'utente di notifiche per tipi specifici di nuovi risultati ad alta gravità. Puoi anche specificare Amazon Q Developer nelle applicazioni di chat come canale di distribuzione per tali notifiche. Notifiche all'utente rileva quindi EventBridge gli eventi relativi ai risultati, genera notifiche che includono i dati dei risultati e invia le notifiche ad Amazon Q Developer nelle applicazioni di chat. Amazon Q Developer nelle applicazioni di chat potrebbe quindi indirizzare le notifiche a un canale Slack o a una chat room di Amazon Chime per informare il tuo team di risposta agli incidenti.

Argomenti

- [Lavorare con Notifiche all'utente AWS](#)
- [Attivazione e configurazione dei risultati di Notifiche all'utente AWS Macie](#)

- [Mappatura dei Notifiche all'utente AWS campi ai campi di ricerca di Macie](#)
- [Modifica delle Notifiche all'utente AWS impostazioni per i risultati di Macie](#)
- [Disattivazione Notifiche all'utente AWS per i risultati di Macie](#)

Lavorare con Notifiche all'utente AWS

Con Notifiche all'utente AWS, crei regole per specificare i tipi di EventBridge eventi Amazon per i quali desideri monitorare e ricevere notifiche. Una regola definisce i criteri che un EventBridge evento deve soddisfare per generare una notifica. Puoi anche scegliere uno o più canali di distribuzione per una regola. I canali di distribuzione specificano dove desideri ricevere le notifiche per gli eventi che soddisfano i criteri di una regola.

Se Notifiche all'utente rileva un EventBridge evento che corrisponde ai criteri di una regola, esegue le seguenti attività generali:

1. Estrae un sottoinsieme di dati dall'evento.
2. Genera una notifica che contiene i dati estratti.
3. Invia la notifica ai canali di distribuzione specificati per quel tipo di evento.

Il design e la struttura della notifica sono ottimizzati per ogni canale di consegna a cui viene inviata.

Per controllare la frequenza o il numero di notifiche che ricevi, puoi configurare le impostazioni di aggregazione per una regola. Se abiliti queste impostazioni, Notifiche all'utente combina i dati di più eventi in un'unica notifica. Puoi scegliere di inviare notifiche aggregate di eventi in modo rapido e frequente, cosa che potresti voler fare per eventi di rilevamento con elevata gravità. Oppure inviale meno frequentemente per ricevere meno notifiche, cosa che potresti fare per gli eventi di rilevazione a bassa gravità. Se combini i dati degli eventi, puoi approfondire i dettagli di ogni evento aggregato utilizzando la console. Notifiche all'utente AWS Da lì, puoi anche accedere a ogni risultato associato sulla console Amazon Macie.

Attivazione e configurazione dei risultati di Notifiche all'utente AWS Macie

Notifiche all'utente AWS Per abilitare la generazione di notifiche per i risultati di Amazon Macie, crea una configurazione di notifica per Macie in. Notifiche all'utente Una configurazione di notifica specifica i criteri per una regola. Inoltre, specifica i canali di consegna e altre impostazioni per il monitoraggio e l'invio di notifiche sugli EventBridge eventi di Amazon che soddisfano i criteri della regola. Per

informazioni dettagliate sulla creazione di una configurazione di notifica, consulta la Guida [introduttiva Notifiche all'utente AWS](#) nella Guida per l'Notifiche all'utente AWS utente.

Per creare una configurazione di notifica per i risultati di Macie, scegli le seguenti opzioni per la regola dell'evento:

- Come Servizio AWS nome, scegli Macie.
- Per Tipo di evento, scegli Macie Finding.
- Per le regioni, seleziona ognuna Regione AWS in cui usi Macie e desideri ricevere notifiche sui risultati.

Con questa configurazione, Notifiche all'utente monitora EventBridge gli eventi per te Account AWS e genera notifiche per tutti gli eventi di ricerca di Macie nelle regioni che hai selezionato. Gli eventi soddisfano i seguenti criteri:

- `source` è uguale `aws.macie`
- `detail-type` è uguale `Macie Finding`

Il pattern JSON alla base della regola di evento è:

```
{
  "source": ["aws.macie"],
  "detail-type": ["Macie Finding"]
}
```

Per rifinire la regola e generare notifiche solo per un sottoinsieme di risultati, puoi personalizzare il pattern JSON per la regola. A tale scopo, specificate criteri aggiuntivi che derivano da [Schema di EventBridge eventi Amazon per i risultati di Macie](#)

Se crei una regola che utilizza un pattern JSON personalizzato, puoi creare più configurazioni di notifica per i risultati di Macie. Puoi quindi personalizzare i canali di distribuzione e altre impostazioni per ciascuna configurazione in modo da allinearli ai flussi di lavoro di sicurezza e conformità per tipi specifici di risultati.

Ad esempio, potresti creare una regola che ti avvisi se Macie genera o aggiorna un risultato. Policy: IAMUser/S3BucketPublic In questo caso, lo schema della regola potrebbe essere:

```
{
```

```

    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
      "type": ["Policy:IAMUser/S3BucketPublic"]
    }
  }
}

```

E potresti creare un'altra regola che ti avvisi se Macie genera una ricerca di dati sensibili per un bucket S3 accessibile pubblicamente. In questo caso, lo schema della regola potrebbe essere:

```

{
  "source": ["aws.macie"],
  "detail-type": ["Macie Finding"],
  "detail": {
    "type": [ { "prefix": "SensitiveData" } ],
    "resourcesAffected": {
      "effectivePermission": ["PUBLIC"]
    }
  }
}

```

Se crei più configurazioni di notifica per i risultati di Macie, è una buona idea assicurarsi che la regola per ogni configurazione sia unica. Altrimenti, potresti ricevere notifiche duplicate per singoli risultati.

Per ulteriori informazioni sulla personalizzazione dei modelli di eventi per le regole, consulta [Uso dei modelli di eventi JSON personalizzati](#) nella Guida per l'Notifiche all'utente AWS utente.

Mappatura dei Notifiche all'utente AWS campi ai campi di ricerca di Macie

Quando Notifiche all'utente AWS genera una notifica per un risultato di Amazon Macie, compila la notifica con i dati di un sottoinsieme di campi nell'evento Amazon corrispondente. EventBridge Questi campi forniscono i dettagli chiave del risultato associato, come il tipo e la gravità del risultato e il nome della risorsa interessata.

Se si esamina una notifica sulla Notifiche all'utente AWS console, la notifica include tutti i dati per questo sottoinsieme di campi. Fornisce inoltre un collegamento ai risultati associati sulla console Amazon Macie. Se esamini una notifica in altri canali di consegna, potrebbe contenere dati solo per alcuni campi. Questo perché Notifiche all'utente adatta il design e la struttura delle notifiche per adattarsi a ogni tipo di canale di consegna supportato.

La tabella seguente elenca i campi che possono essere inclusi in una notifica relativa a un risultato. Nella tabella, la colonna del campo Notifica descrive (in corsivo) o indica il nome di un campo in una notifica. La colonna del campo Finding event utilizza la notazione a punti per indicare il nome del campo JSON corrispondente in un EventBridge evento relativo a un risultato. La colonna Descrizione descrive i dati memorizzati nel campo.

Campo di notifica	Campo di ricerca dell'evento	Descrizione
Titolo del messaggio	<code>detail.type</code>	Il tipo di risultato. Ad esempio: <code>Policy:IAMUser/S3BucketPublic o Sensitive Data:S3object/Financial</code> .
Riepilogo	<code>detail.title</code>	Breve descrizione del ritrovamento. Ad esempio: <code>The S3 object contains financial information.</code>
Descrizione	<code>detail.description</code>	La descrizione completa del ritrovamento. Ad esempio: <code>The S3 object contains financial information such as bank account numbers or credit card numbers.</code>
Gravità	<code>detail.severity.description</code>	La rappresentazione qualitativa della gravità del riscontro: <code>LowMedium, oHigh</code> .

Campo di notifica	Campo di ricerca dell'evento	Descrizione
ID risultato	<code>detail.id</code>	L'identificatore univoco del risultato.
Creato	<code>detail.createdAt</code>	La data e l'ora in cui Macie ha creato il risultato.
Aggiornato	<code>detail.updatedAt</code>	La data e l'ora in cui Macie ha aggiornato il risultato per l'ultima volta. Per quanto riguarda i dati sensibili, questo valore è uguale al valore del campo <code>Created (detail.createdAt)</code>. Tutti i dati sensibili rilevati sono considerati nuovi (unici).
Bucket S3 interessato	<code>detail.resourcesAffected.s3Bucket.arn</code>	L'Amazon Resource Name (ARN) del bucket S3 interessato.
Oggetto S3 interessato	<code>detail.resourcesAffected.s3Object.path</code>	Il nome (chiave) dell'oggetto S3 interessato, incluso il nome del bucket che memorizza l'oggetto e, se applicabile, il prefisso dell'oggetto. Questo campo non è incluso nelle notifiche relative ai risultati delle politiche.

Campo di notifica	Campo di ricerca dell'evento	Descrizione
Rilevamenti di dati sensibili	<code>detail.classificationDetails.result.sensitiveData.detections...</code> e/o <code>detail.classificationDetails.result.customDataIdentifiers.detections...</code>	Si tratta di una concatenazione di più campi in un evento per la ricerca di dati sensibili. Questo campo non è incluso nelle notifiche relative ai risultati delle politiche. Se un identificatore di dati gestito ha rilevato i dati sensibili, questo campo specifica la categoria, il tipo e il numero (count) di occorrenze dei dati sensibili rilevati. Ad esempio: <code>PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences</code>. Se un identificatore di dati personalizzato ha rilevato dati sensibili, questo campo specifica il nome dell'identificatore di dati personalizzato e il numero (count) di occorrenze dei dati sensibili rilevati. Ad esempio: <code>Employee ID 20 occurrences</code>. Se un risultato riporta più tipi di dati sensibili, la notifica include dati per un massimo di quattro tipi. I dati vengono compilati prima con qualsiasi

Campo di notifica	Campo di ricerca dell'evento	Descrizione
		identificatore di dati personali zzato applicabile e poi con qualsiasi identificatore di dati gestito applicabile.

Modifica delle Notifiche all'utente AWS impostazioni per i risultati di Macie

Puoi modificare Notifiche all'utente AWS le impostazioni per i risultati di Amazon Macie in qualsiasi momento. A tale scopo, modifica la configurazione delle notifiche in Notifiche all'utente. Per sapere come, consulta [Gestione delle configurazioni di notifica](#) nella Guida per l'Notifiche all'utente AWS utente.

Se disponi di più configurazioni di notifica per i risultati di Macie, la modifica delle impostazioni per una configurazione non influisce sulle impostazioni delle altre configurazioni. Puoi modificare tutte o solo alcune delle tue configurazioni.

Disattivazione Notifiche all'utente AWS per i risultati di Macie

Per interrompere la generazione e la ricezione di notifiche Notifiche all'utente AWS per i risultati di Amazon Macie, elimina la configurazione delle notifiche in. Notifiche all'utente Per sapere come, consulta [Gestione delle configurazioni di notifica nella Guida](#) per l'Notifiche all'utente AWS utente.

Se disponi di più configurazioni di notifica per i risultati di Macie, l'eliminazione di una configurazione non influisce sulle altre configurazioni. Puoi eliminare tutte o solo alcune delle configurazioni.

Valutazione dei risultati di Macie con AWS Security Hub

AWS Security Hub è un servizio che offre una visione completa del livello di sicurezza in tutto AWS l'ambiente e consente di verificare la conformità dell'ambiente rispetto agli standard e alle best practice del settore della sicurezza. Lo fa in parte consumando, aggregando, organizzando e dando priorità ai risultati provenienti da più soluzioni di sicurezza Servizi AWS supportate. AWS Partner Network Security Hub ti aiuta ad analizzare le tendenze della sicurezza e a identificare i problemi di sicurezza con la massima priorità. Con Security Hub, puoi anche aggregare i risultati di più Regioni AWS risultati e quindi valutare ed elaborare tutti i dati aggregati dei risultati provenienti da una singola regione. Per ulteriori informazioni su Security Hub, consulta la [Guida AWS Security Hub per l'utente](#).

Amazon Macie si integra con Security Hub, il che significa che puoi pubblicare automaticamente i risultati di Macie su Security Hub. Security Hub può quindi includere tali risultati nella sua analisi della posizione di sicurezza. Inoltre, puoi utilizzare Security Hub per valutare ed elaborare i risultati delle policy e dei dati sensibili come parte di un set più ampio e aggregato di dati sui risultati per il tuo AWS ambiente. In altre parole, puoi valutare i risultati di Macie eseguendo analisi più ampie del livello di sicurezza della tua organizzazione e, se necessario, correggere i risultati. Security Hub riduce la complessità legata all'elaborazione di grandi volumi di risultati provenienti da più provider. Inoltre, utilizza un formato standard per tutti i risultati, compresi i risultati di Macie. L'uso di questo formato, il AWS Security Finding Format (ASFF), elimina la necessità di eseguire operazioni di conversione dei dati che richiedono molto tempo.

Argomenti

- [In che modo Macie pubblica i risultati su AWS Security Hub](#)
- [Esempi di scoperte di Macie in AWS Security Hub](#)
- [Integrazione di Macie con AWS Security Hub](#)
- [Interruzione della pubblicazione dei risultati di Macie su AWS Security Hub](#)

In che modo Macie pubblica i risultati su AWS Security Hub

Nel AWS Security Hub, i problemi di sicurezza vengono registrati come risultati. Alcuni risultati derivano da problemi rilevati da Servizi AWS, come Amazon Macie, o da soluzioni di AWS Partner Network sicurezza supportate. La Centrale di sicurezza dispone inoltre di una serie di regole che utilizza per rilevare problemi di sicurezza e generare esiti.

Security Hub fornisce strumenti per gestire i risultati provenienti da tutte queste fonti. È possibile esaminare e filtrare gli elenchi dei risultati e rivedere i dettagli dei singoli risultati. Per scoprire come, consulta la [cronologia dei risultati e la ricerca dei dettagli](#) nella Guida AWS Security Hub per l'utente. È inoltre possibile monitorare lo stato di un'indagine in un esito. Per sapere come, consulta [Impostazione dello stato dei risultati del flusso](#) di lavoro nella Guida AWS Security Hub per l'utente.

Tutti i risultati in Security Hub utilizzano un formato JSON standard denominato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine di un problema, sulle risorse interessate e sullo stato attuale di un risultato. Per ulteriori informazioni, consulta [AWS Security Finding Format \(ASFF\)](#) nella Guida per l'utente di AWS Security Hub .

Tipi di risultati che Macie pubblica su Security Hub

A seconda delle impostazioni di pubblicazione scelte per il tuo account Macie, Macie può pubblicare tutti i risultati che crea su Security Hub, sia i risultati relativi ai dati sensibili che i risultati delle politiche. Per informazioni su queste impostazioni e su come modificarle, consulta [Configurazione delle impostazioni di pubblicazione per i risultati](#). Per impostazione predefinita, Macie pubblica solo i risultati delle policy nuovi e aggiornati su Security Hub. Macie non pubblica dati sensibili su Security Hub.

Rilevamenti relativi a dati sensibili

Se configuri Macie per pubblicare [i risultati relativi ai dati sensibili](#) su Security Hub, Macie pubblica automaticamente ogni dato sensibile che crea per il tuo account e lo fa immediatamente dopo aver terminato l'elaborazione del risultato. [Macie esegue questa operazione per tutti i dati sensibili rilevati che non vengono archiviati automaticamente in base a una regola di soppressione.](#)

Se sei l'amministratore Macie di un'organizzazione, la pubblicazione è limitata ai risultati dei lavori di rilevamento di dati sensibili che hai eseguito e alle attività automatizzate di rilevamento di dati sensibili eseguite da Macie per la tua organizzazione. Solo l'account che crea un lavoro può pubblicare i risultati relativi ai dati sensibili prodotti dal lavoro. Solo l'account amministratore di Macie può pubblicare i risultati relativi ai dati sensibili che il rilevamento automatico di dati sensibili produce per la propria organizzazione.

Quando Macie pubblica i risultati dei dati sensibili su Security Hub, utilizza il [AWS Security Finding Format \(ASFF\)](#), che è il formato standard per tutti i risultati in Security Hub. Nell'ASFF, il Types campo indica il tipo di risultato. Questo campo utilizza una tassonomia leggermente diversa dalla tassonomia dei tipi di risultati di Macie.

La tabella seguente elenca il tipo di ricerca ASFF per ogni tipo di ricerca di dati sensibili che Macie può creare.

Tipo di ricerca Macie	Tipo di risultati ASFF
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/Sensitive Data:S3Object-CustomIdentifier

Tipo di ricerca Macie	Tipo di risultati ASFF
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

Risultati politici

Se configuri Macie per pubblicare [i risultati delle politiche](#) su Security Hub, Macie pubblica automaticamente ogni nuova ricerca di policy che crea e lo fa immediatamente dopo aver terminato l'elaborazione del risultato. Se Macie rileva una successiva occorrenza di un risultato di policy esistente, pubblica automaticamente un aggiornamento del risultato esistente in Security Hub, utilizzando una frequenza di pubblicazione specificata per il tuo account. [Macie esegue queste attività per tutti i risultati delle policy che non vengono archiviati automaticamente da una regola di soppressione.](#)

Se sei l'amministratore Macie di un'organizzazione, la pubblicazione è limitata ai risultati delle policy per i bucket S3 di proprietà diretta del tuo account. Macie non pubblica i risultati delle politiche che crea o aggiorna per gli account dei membri della tua organizzazione. Questo aiuta a garantire che non ci siano dati duplicati sui risultati in Security Hub.

Come nel caso delle rilevazioni di dati sensibili, Macie utilizza il AWS Security Finding Format (ASFF) quando pubblica i risultati delle politiche nuovi e aggiornati su Security Hub. Nell'ASFF, il Types campo utilizza una tassonomia leggermente diversa dalla tassonomia dei tipi di risultati di Macie.

La tabella seguente elenca il tipo di ricerca ASFF per ogni tipo di ricerca politica che Macie può creare. Se Macie ha creato o aggiornato un risultato di policy in Security Hub a partire dal 28 gennaio 2021, il risultato ha uno dei seguenti valori per il Types campo ASFF in Security Hub.

Tipo di ricerca di Macie	Tipo di risultati ASFF

Tipo di ricerca di Macie	Tipo di risultati ASFF
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Se Macie ha creato o aggiornato l'ultima volta un risultato di policy prima del 28 gennaio 2021, il risultato ha uno dei seguenti valori per il Types campo ASFF in Security Hub:

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

I valori dell'elenco precedente vengono mappati direttamente ai valori del campo Finding type (type) in Macie.

Note

Mentre esami e elabori i risultati delle policy in Security Hub, tieni presente le seguenti eccezioni:

- In alcuni casi Regioni AWS, Macie ha iniziato a utilizzare i tipi di ricerca ASFF per risultati nuovi e aggiornati già il 25 gennaio 2021.
- Se hai agito in base a una policy trovata in Security Hub prima che Macie iniziasse a utilizzare i tipi di ricerca ASFF nel tuo Regione AWS, il valore per il Types campo ASFF del risultato sarà uno dei tipi di ricerca Macie nell'elenco precedente. Non sarà uno dei tipi di risultati ASFF nella tabella precedente. Questo vale per i risultati delle politiche in base ai quali hai agito utilizzando la AWS Security Hub console o il BatchUpdateFindings funzionamento dell' AWS Security Hub API.

Latenza per la pubblicazione dei risultati su Security Hub

Quando Amazon Macie crea una nuova policy o una ricerca di dati sensibili, pubblica il risultato AWS Security Hub immediatamente dopo aver terminato l'elaborazione del risultato.

Se Macie rileva una successiva occorrenza di un risultato di policy esistente, pubblica un aggiornamento al risultato esistente del Security Hub. La tempistica dell'aggiornamento dipende dalla frequenza di pubblicazione scelta per il tuo account Macie. Per impostazione predefinita, Macie pubblica gli aggiornamenti ogni 15 minuti. Per ulteriori informazioni, incluso come modificare le impostazioni dell'account, consulta [Configurazione delle impostazioni di pubblicazione per i risultati](#)

Riprova a pubblicare quando Security Hub non è disponibile

Se non AWS Security Hub è disponibile, Amazon Macie crea una coda di risultati che non sono stati ricevuti da Security Hub. Quando il sistema viene ripristinato, Macie riprova a pubblicare finché i risultati non vengono ricevuti da Security Hub.

Aggiornamento degli esiti esistenti nella Centrale di sicurezza

Dopo che Amazon Macie ha pubblicato una decisione politica su AWS Security Hub, Macie aggiorna la scoperta per riflettere eventuali altre ricorrenze dell'attività di ricerca o di ricerca. Macie lo fa solo

per risultati politici. Le scoperte relative ai dati sensibili, a differenza delle risultanze relative alle politiche, vengono tutte trattate come nuove (uniche).

Quando Macie pubblica un aggiornamento di un risultato relativo a una policy, Macie aggiorna il valore del campo Updated At (UpdatedAt) del risultato. È possibile utilizzare questo valore per determinare quando Macie ha rilevato più di recente un successivo verificarsi della potenziale violazione delle politiche o del problema che ha prodotto la scoperta.

Macie potrebbe anche aggiornare il valore del campo Types (Types) di un risultato se il valore esistente per il campo non è un tipo di risultato [ASFF](#). Dipende dal fatto che tu abbia agito in base alla scoperta in Security Hub. Se non hai agito in base alla scoperta, Macie modifica il valore del campo impostando il tipo di risultato ASFF appropriato. Se hai agito in base alla scoperta, utilizzando la AWS Security Hub console o il BatchUpdateFindings funzionamento dell' AWS Security Hub API, Macie non modifica il valore del campo.

Esempi di scoperte di Macie in AWS Security Hub

Quando Amazon Macie pubblica i risultati su AWS Security Hub, utilizza il [AWS Security Finding Format](#) (ASFF). Questo è il formato standard per tutti i risultati in Security Hub. Gli esempi seguenti utilizzano dati di esempio per dimostrare la struttura e la natura dei dati dei risultati che Macie pubblica su Security Hub in questo formato:

- [Esempio di rilevamento di dati sensibili](#)
- [Esempio di scoperta politica](#)

Esempio di rilevamento di dati sensibili in Security Hub

Ecco un esempio di una scoperta di dati sensibili che Macie ha pubblicato su Security Hub utilizzando l'ASFF.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "5be50fce24526e670df77bc00example",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
  "ProductName": "Macie",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "aws/macie",
  "AwsAccountId": "111122223333",
  "Types": [
```



```

    "Sensitive Data Identifications/PII/SensitiveData:S3object-Personal"
  ],
  "CreatedAt": "2022-05-11T10:23:49.667Z",
  "UpdatedAt": "2022-05-11T10:23:49.667Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "The S3 object contains personal information.",
  "Description": "The object contains personal information such as first or last
names, addresses, or identification numbers.",
  "ProductFields": {
    "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
    "S3object.Path": "amzn-s3-demo-bucket/2022 Sourcing.tsv",
    "S3object.Extension": "tsv",
    "S3Bucket.effectivePermission": "NOT_PUBLIC",
    "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
    "S3object.PublicAccess": "false",
    "S3object.Size": "14",
    "S3object.StorageClass": "STANDARD",
    "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
    "JobId": "698e99c283a255bb2c992feceexample",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
    "aws/securityhub/ProductName": "Macie",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsS3Bucket",
      "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsS3Bucket": {
          "OwnerId":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
          "OwnerName": "johndoe",
          "OwnerAccountId": "444455556666",
          "CreatedAt": "2020-12-30T18:16:25.000Z",
          "ServerSideEncryptionConfiguration": {
            "Rules": [
              {

```

```

        "ApplyServerSideEncryptionByDefault": {
            "SSEAlgorithm": "aws:kms",
            "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true
    }
},
{
    "Type": "AwsS3Object",
    "Id": "arn:aws:s3:::amzn-s3-demo-bucket/2022 Sourcing.tsv",
    "Partition": "aws",
    "Region": "us-east-1",
    "DataClassification": {
        "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
        "Result": {
            "MimeType": "text/tsv",
            "SizeClassified": 14,
            "AdditionalOccurrences": false,
            "Status": {
                "Code": "COMPLETE"
            },
            "SensitiveData": [
                {
                    "Category": "PERSONAL_INFORMATION",
                    "Detections": [
                        {
                            "Count": 1,
                            "Type": "USA_SOCIAL_SECURITY_NUMBER",
                            "Occurrences": {
                                "Cells": [

```

```

        "Column": 10,
        "Row": 1,
        "ColumnName": "Other"
      }
    ]
  },
  "TotalCount": 1
},
],
"CustomDataIdentifiers": {
  "Detections": [
  ],
  "TotalCount": 0
}
},
],
"Details": {
  "AwsS3Object": {
    "LastModified": "2022-04-22T18:16:46.000Z",
    "ETag": "ebe1ca03ee8d006d457444445example",
    "VersionId": "S1BC72z5hArgex0Jifxw_IN57example",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
],
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "HIGH"
  },
  "Types": [
    "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
  ]
},
"Sample": false,

```

```
"ProcessedAt": "2022-05-11T10:23:49.667Z"
}
```

Esempio di una policy trovata in Security Hub

Ecco un esempio di una nuova scoperta politica che Macie ha pubblicato su Security Hub nell'ASFF.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "36ca8ba0-caf1-4fee-875c-37760example",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
  "ProductName": "Macie",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "aws/macie",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled"
  ],
  "CreatedAt": "2022-04-24T09:27:43.313Z",
  "UpdatedAt": "2022-04-24T09:27:43.313Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "Block Public Access settings are disabled for the S3 bucket",
  "Description": "All Amazon S3 block public access settings are disabled for the Amazon S3 bucket. Access to the bucket is controlled only by access control lists (ACLs) or bucket policies.",
  "ProductFields": {
    "S3Bucket.effectivePermission": "NOT_PUBLIC",
    "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/macie/36ca8ba0-caf1-4fee-875c-37760example",
    "aws/securityhub/ProductName": "Macie",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsS3Bucket",
      "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Partition": "aws",

```

```

    "Region": "us-east-1",
    "Tags": {
      "Team": "Recruiting",
      "Division": "HR"
    },
    "Details": {
      "AwsS3Bucket": {
        "OwnerId":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
        "OwnerName": "johndoe",
        "OwnerAccountId": "444455556666",
        "CreatedAt": "2020-11-25T18:24:38.000Z",
        "ServerSideEncryptionConfiguration": {
          "Rules": [
            {
              "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "aws:kms",
                "KMSEMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
              }
            }
          ]
        },
        "PublicAccessBlockConfiguration": {
          "BlockPublicAcls": false,
          "BlockPublicPolicy": false,
          "IgnorePublicAcls": false,
          "RestrictPublicBuckets": false
        }
      }
    }
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [

```

```
"Software and Configuration Checks/AWS Security Best Practices/  
Policy:IAMUser-S3BlockPublicAccessDisabled"  
]  
,  
"Sample": false  
}
```

Integrazione di Macie con AWS Security Hub

Per integrare Amazon Macie con AWS Security Hub, abilita Security Hub for your Account AWS. Per sapere come, consulta [Enabling Security Hub](#) nella Guida AWS Security Hub per l'utente.

Quando abiliti sia Macie che Security Hub, l'integrazione viene abilitata automaticamente. Per impostazione predefinita, Macie inizia a pubblicare automaticamente i risultati delle policy nuovi e aggiornati su Security Hub. Non è necessario eseguire ulteriori passaggi per configurare l'integrazione. Se disponi di risultati delle politiche esistenti quando l'integrazione è abilitata, Macie non li pubblica su Security Hub. Macie pubblica invece solo i risultati delle policy che crea o aggiorna dopo l'attivazione dell'integrazione.

Facoltativamente, puoi personalizzare la tua configurazione scegliendo la frequenza con cui Macie pubblica gli aggiornamenti ai risultati delle politiche in Security Hub. Puoi anche scegliere di pubblicare i risultati relativi ai dati sensibili su Security Hub. Per scoprire come, consulta [Configurazione delle impostazioni di pubblicazione per i risultati](#).

Interruzione della pubblicazione dei risultati di Macie su AWS Security Hub

Per interrompere la pubblicazione dei risultati di Amazon Macie su AWS Security Hub, puoi modificare le impostazioni di pubblicazione per il tuo account Macie. Per scoprire come, consulta [Scelta delle destinazioni di pubblicazione dei risultati](#). Puoi farlo anche usando Security Hub. Per sapere come, consulta [Disabilitazione del flusso di risultati da un'integrazione](#) nella Guida per l'AWS Security Hub utente.

Schema di EventBridge eventi Amazon per i risultati di Macie

Per supportare l'integrazione con altre applicazioni, servizi e sistemi, come i sistemi di monitoraggio o di gestione degli eventi, Amazon Macie pubblica automaticamente i risultati su Amazon EventBridge come eventi. EventBridge, precedentemente Amazon CloudWatch Events, è un servizio di bus eventi senza server che fornisce un flusso di dati in tempo reale da applicazioni e altro Servizi AWS verso

destinazioni quali funzioni AWS Lambda , argomenti di Amazon Simple Notification Service e flussi Amazon Kinesis. Per ulteriori informazioni EventBridge, consulta la [Amazon EventBridge User Guide](#).

Note

Se attualmente utilizzi CloudWatch Events, tieni presente che CloudWatch Events EventBridge e Events sono lo stesso servizio e API sottostanti. Tuttavia, EventBridge include funzionalità aggiuntive che consentono di ricevere eventi dalle applicazioni SaaS (Software as a Service) e dalle proprie applicazioni. Poiché il servizio e l'API sottostanti sono gli stessi, anche lo schema degli eventi per i risultati di Macie è lo stesso.

[Macie pubblica automaticamente gli eventi per tutte le nuove scoperte e le successive occorrenze dei risultati delle policy esistenti, ad eccezione dei risultati che vengono archiviati automaticamente in base a una regola di soppressione.](#) Gli eventi sono oggetti JSON conformi allo schema degli eventi. EventBridge AWS Ogni evento contiene una rappresentazione JSON di un particolare risultato. Poiché i dati sono strutturati come un EventBridge evento, è possibile monitorare, elaborare e agire più facilmente su un risultato utilizzando altre applicazioni, servizi e strumenti. Per dettagli su come e quando Macie pubblica gli eventi per i risultati, vedi. [Configurazione delle impostazioni di pubblicazione per i risultati](#)

Argomenti

- [Schema degli eventi per i risultati di Macie](#)
- [Esempio di evento relativo a una definizione di policy](#)
- [Esempio di evento per la ricerca di dati sensibili](#)

Schema degli eventi per i risultati di Macie

L'esempio seguente mostra lo schema di un [EventBridge evento Amazon](#) per un risultato di Amazon Macie. Per descrizioni dettagliate dei campi che possono essere inclusi in un evento di ricerca, consulta [Findings](#) in the Amazon Macie API Reference. La struttura e i campi di un evento di ricerca sono strettamente correlati all'Findingoggetto dell'API Amazon Macie.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "Macie Finding",
  "source": "aws.macie",
```

```

"account": "Account AWS ID (string)",
"time": "event timestamp (string)",
"region": "Regione AWS (string)",
"resources": [
    <-- ARNs of the resources involved in the event -->
],
"detail": {
    <-- Details of a policy or sensitive data finding -->
},
"policyDetails": null, <-- Additional details of a policy finding or null for a
sensitive data finding -->
"sample": Boolean,
"archived": Boolean
}

```

Esempio di evento relativo a una definizione di policy

L'esempio seguente utilizza dati di esempio per dimostrare la struttura e la natura di oggetti e campi in un EventBridge evento Amazon per la definizione di una [politica](#). In questo esempio, l'evento riporta una successiva rilevazione di una policy esistente: Amazon Macie ha rilevato che le impostazioni di accesso pubblico a blocchi erano disabilitate per un bucket S3. I seguenti campi e valori possono aiutarti a determinare che sia così:

- Il type campo è impostato su `Policy:IAMUser/S3BlockPublicAccessDisabled`.
- I `updatedAt` campi `createdAt` e hanno valori diversi. Si tratta di un indicatore del fatto che l'evento segnala un successivo verificarsi di un risultato politico esistente. I valori di questi campi sarebbero gli stessi se l'evento riportasse un nuovo risultato.
- Il `count` campo è impostato su `2`, il che indica che questa è la seconda occorrenza del risultato.
- Il `category` campo è impostato su `POLICY`.
- Il valore del `classificationDetails` campo è `null`, che aiuta a differenziare questo evento per una ricerca di policy da un evento per la ricerca di dati sensibili. Per un rilevamento di dati sensibili, questo valore sarebbe un insieme di oggetti e campi che forniscono informazioni su come e quali dati sensibili sono stati trovati.

Si noti inoltre che il valore del `sample` campo è `true`. Questo valore sottolinea che si tratta di un evento di esempio da utilizzare nella documentazione.

```

{
    "version": "0",

```



```

    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2024-04-30T23:12:15Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "schemaVersion": "1.0",
      "id": "64b917aa-3843-014c-91d8-937ffexample",
      "accountId": "123456789012",
      "partition": "aws",
      "region": "us-east-1",
      "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
      "title": "Block public access settings are disabled for the S3 bucket",
      "description": "All bucket-level block public access settings were disabled for
the S3 bucket. Access to the bucket is controlled by account-level block public access
settings, access control lists (ACLs), and the bucket's bucket policy.",
      "severity": {
        "score": 3,
        "description": "High"
      },
      "createdAt": "2024-04-29T15:46:02Z",
      "updatedAt": "2024-04-30T23:12:15Z",
      "count": 2,
      "resourcesAffected": {
        "s3Bucket": {
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket1",
          "name": "amzn-s3-demo-bucket1",
          "createdAt": "2020-04-03T20:46:56.000Z",
          "owner": {
            "displayName": "johndoe",
            "id":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
          },
          "tags": [
            {
              "key": "Division",
              "value": "HR"
            },
            {
              "key": "Team",
              "value": "Recruiting"
            }
          ]
        }
      }
    }
  }

```

```

    ],
    "defaultServerSideEncryption": {
      "encryptionType": "aws:kms",
      "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "publicAccess": {
      "permissionConfiguration": {
        "bucketLevelPermissions": {
          "accessControlList": {
            "allowsPublicReadAccess": false,
            "allowsPublicWriteAccess": false
          },
          "bucketPolicy": {
            "allowsPublicReadAccess": false,
            "allowsPublicWriteAccess": false
          },
          "blockPublicAccess": {
            "ignorePublicAcls": false,
            "restrictPublicBuckets": false,
            "blockPublicAcls": false,
            "blockPublicPolicy": false
          }
        },
        "accountLevelPermissions": {
          "blockPublicAccess": {
            "ignorePublicAcls": true,
            "restrictPublicBuckets": true,
            "blockPublicAcls": true,
            "blockPublicPolicy": true
          }
        }
      },
      "effectivePermission": "NOT_PUBLIC"
    },
    "allowsUnencryptedObjectUploads": "FALSE"
  },
  "s3Object": null
},
"category": "POLICY",
"classificationDetails": null,
"policyDetails": {
  "action": {
    "actionType": "AWS_API_CALL",

```

```

    "apiCallDetails": {
      "api": "PutBucketPublicAccessBlock",
      "apiServiceName": "s3.amazonaws.com",
      "firstSeen": "2024-04-29T15:46:02.401Z",
      "lastSeen": "2024-04-30T23:12:15.401Z"
    }
  },
  "actor": {
    "userIdentity": {
      "type": "AssumedRole",
      "assumedRole": {
        "principalId": "AR0A1234567890EXAMPLE:AssumedRoleSessionName",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",

        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": false,
            "creationDate": "2024-04-29T10:25:43.511Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A1234567890EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",

            "accountId": "123456789012",
            "userName": "RoleToBeAssumed"
          }
        }
      }
    },
    "root": null,
    "iamUser": null,
    "federatedUser": null,
    "awsAccount": null,
    "awsService": null
  },
  "ipAddressDetails": {
    "ipAddressV4": "192.0.2.0",
    "ipOwner": {
      "asn": "-1",
      "asnOrg": "ExampleFindingASN0rg",
      "isp": "ExampleFindingISP",
      "org": "ExampleFindingORG"
    }
  }
}

```

```
    },
    "ipCountry": {
      "code": "US",
      "name": "United States"
    },
    "ipCity": {
      "name": "Ashburn"
    },
    "ipGeoLocation": {
      "lat": 39.0481,
      "lon": -77.4728
    }
  },
  "domainDetails": null
}
},
"sample": true,
"archived": false
}
}
```

Esempio di evento per la ricerca di dati sensibili

L'esempio seguente utilizza dati di esempio per dimostrare la struttura e la natura di oggetti e campi in un EventBridge evento Amazon per la [ricerca di dati sensibili](#). In questo esempio, l'evento riporta una nuova scoperta di dati sensibili: Amazon Macie ha trovato più categorie e tipi di dati sensibili in un oggetto S3. I seguenti campi e valori possono aiutarti a determinare che sia così:

- Il `type` campo è impostato su `SensitiveData:S3Object/Multiple`.
- I `updatedAt` e `createdAt` campi hanno gli stessi valori. A differenza dei risultati politici, questo vale sempre per i risultati relativi ai dati sensibili. Tutti i risultati relativi ai dati sensibili sono considerati nuovi.
- Il `count` campo è impostato su `1`, il che indica che si tratta di una nuova scoperta. A differenza dei risultati politici, questo vale sempre per i risultati relativi ai dati sensibili. Tutti i risultati relativi ai dati sensibili sono considerati unici (nuovi).
- Il `category` campo è impostato su `CLASSIFICATION`.
- Il valore del `policyDetails` campo è `null`, che aiuta a differenziare questo evento per una ricerca di dati sensibili da un evento per una ricerca di policy. Per quanto riguarda una policy,

questo valore potrebbe essere un insieme di oggetti e campi che forniscono informazioni su una potenziale violazione delle policy o su un problema con la sicurezza o la privacy di un bucket S3.

Si noti inoltre che il valore del `sample` campo è `true`. Questo valore sottolinea che si tratta di un evento di esempio da utilizzare nella documentazione.

```
{
  "version": "0",
  "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
  "detail-type": "Macie Finding",
  "source": "aws.macie",
  "account": "123456789012",
  "time": "2024-04-20T08:19:10Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "schemaVersion": "1.0",
    "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
    "accountId": "123456789012",
    "partition": "aws",
    "region": "us-east-1",
    "type": "SensitiveData:S3Object/Multiple",
    "title": "The S3 object contains multiple categories of sensitive data",
    "description": "The S3 object contains more than one category of sensitive
data.",
    "severity": {
      "score": 3,
      "description": "High"
    },
    "createdAt": "2024-04-20T18:19:10Z",
    "updatedAt": "2024-04-20T18:19:10Z",
    "count": 1,
    "resourcesAffected": {
      "s3Bucket": {
        "arn": "arn:aws:s3:::amzn-s3-demo-bucket2",
        "name": "amzn-s3-demo-bucket2",
        "createdAt": "2020-05-15T20:46:56.000Z",
        "owner": {
          "displayName": "johndoe",
          "id":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
        }
      },
```

```

    "tags":[
      {
        "key":"Division",
        "value":"HR"
      },
      {
        "key":"Team",
        "value":"Recruiting"
      }
    ],
    "defaultServerSideEncryption": {
      "encryptionType": "aws:kms",
      "kmsMasterKeyId": "arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "publicAccess": {
      "permissionConfiguration": {
        "bucketLevelPermissions": {
          "accessControlList": {
            "allowsPublicReadAccess": false,
            "allowsPublicWriteAccess": false
          },
          "bucketPolicy":{
            "allowsPublicReadAccess": false,
            "allowsPublicWriteAccess": false
          },
          "blockPublicAccess": {
            "ignorePublicAcls": true,
            "restrictPublicBuckets": true,
            "blockPublicAcls": true,
            "blockPublicPolicy": true
          }
        },
        "accountLevelPermissions": {
          "blockPublicAccess": {
            "ignorePublicAcls": false,
            "restrictPublicBuckets": false,
            "blockPublicAcls": false,
            "blockPublicPolicy": false
          }
        }
      },
      "effectivePermission": "NOT_PUBLIC"
    },
  },

```

```

        "allowsUnencryptedObjectUploads": "TRUE"
    },
    "s3Object": {
        "bucketArn": "arn:aws:s3:::amzn-s3-demo-bucket2",
        "key": "2024 Sourcing.csv",
        "path": "amzn-s3-demo-bucket2/2024 Sourcing.csv",
        "extension": "csv",
        "lastModified": "2024-04-19T22:08:25.000Z",
        "versionId": "",
        "serverSideEncryption": {
            "encryptionType": "aws:kms",
            "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        "size": 4750,
        "storageClass": "STANDARD",
        "tags": [
            {
                "key": "Division",
                "value": "HR"
            },
            {
                "key": "Team",
                "value": "Recruiting"
            }
        ],
        "publicAccess": false,
        "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
    }
},
"category": "CLASSIFICATION",
"classificationDetails": {
    "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
    "jobId": "3ce05dbb7ec5505def334104bexample",
    "result": {
        "status": {
            "code": "COMPLETE",
            "reason": null
        },
        "sizeClassified": 4750,
        "mimeType": "text/csv",
        "additionalOccurrences": true,
        "sensitiveData": [

```

```

{
  "category": "PERSONAL_INFORMATION",
  "totalCount": 65,
  "detections": [
    {
      "type": "USA_SOCIAL_SECURITY_NUMBER",
      "count": 30,
      "occurrences": {
        "lineRanges": null,
        "offsetRanges": null,
        "pages": null,
        "records": null,
        "cells": [
          {
            "row": 2,
            "column": 1,
            "columnName": "SSN",
            "cellReference": null
          },
          {
            "row": 3,
            "column": 1,
            "columnName": "SSN",
            "cellReference": null
          },
          {
            "row": 4,
            "column": 1,
            "columnName": "SSN",
            "cellReference": null
          }
        ]
      }
    },
    {
      "type": "NAME",
      "count": 35,
      "occurrences": {
        "lineRanges": null,
        "offsetRanges": null,
        "pages": null,
        "records": null,
        "cells": [
          {

```



```

        "row": 2,
        "column": 3,
        "columnName": "Name",
        "cellReference": null
      },
      {
        "row": 3,
        "column": 3,
        "columnName": "Name",
        "cellReference": null
      }
    ]
  }
},
{
  "category": "FINANCIAL_INFORMATION",
  "totalCount": 30,
  "detections": [
    {
      "type": "CREDIT_CARD_NUMBER",
      "count": 30,
      "occurrences": {
        "lineRanges": null,
        "offsetRanges": null,
        "pages": null,
        "records": null,
        "cells": [
          {
            "row": 2,
            "column": 14,
            "columnName": "CCN",
            "cellReference": null
          },
          {
            "row": 3,
            "column": 14,
            "columnName": "CCN",
            "cellReference": null
          }
        ]
      }
    }
  ]
}

```

```
        ]
      }
    ],
    "customDataIdentifiers": {
      "totalCount": 0,
      "detections": []
    },
    "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
    "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
  },
  "policyDetails": null,
  "sample": true,
  "archived": false
}
}
```

Previsione e monitoraggio dei costi di Macie

Per aiutarti a prevedere e monitorare i costi di utilizzo di Amazon Macie, Macie calcola e fornisce una stima dei costi di utilizzo per il tuo account. Con questi dati, puoi determinare se modificare l'utilizzo del servizio o le quote del tuo account. Se attualmente stai partecipando a una prova gratuita di 30 giorni di Macie, puoi utilizzare questi dati per stimare i costi per l'utilizzo di Macie al termine della prova gratuita. Puoi anche controllare lo stato del periodo di prova.

Puoi rivedere i costi di utilizzo stimati sulla console Amazon Macie e accedervi a livello di codice con l'API Amazon Macie. Se sei l'amministratore Macie di un'organizzazione, puoi esaminare e accedere sia ai dati aggregati dell'organizzazione che alle suddivisioni dei dati per gli account dell'organizzazione.

Oltre ai costi di utilizzo stimati forniti da Macie, puoi rivedere e monitorare i costi effettivi utilizzando AWS Billing and Cost Management. AWS Billing and Cost Management offre funzionalità progettate per aiutarti a tenere traccia e analizzare i costi e gestire i budget per Servizi AWS il tuo account o la tua organizzazione. Fornisce inoltre funzionalità che possono aiutarti a prevedere i costi di utilizzo sulla base di dati storici. Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Billing](#).

Argomenti

- [Comprensione dei costi di utilizzo stimati per Macie](#)
- [Analisi dei costi di utilizzo stimati per Macie](#)
- [Partecipazione alla prova gratuita di Macie](#)

Comprensione dei costi di utilizzo stimati per Macie

I prezzi di Amazon Macie si basano sulle seguenti dimensioni.

Controllo preventivo e monitoraggio

Questi costi derivano dalla gestione di un inventario dei bucket generici Amazon Simple Storage Service (Amazon S3) per uso generico e dalla valutazione e dal monitoraggio dei bucket per la sicurezza e il controllo degli accessi. Per ulteriori informazioni, consulta [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#).

L'addebito viene effettuato in base al numero totale di bucket S3 per uso generico che Macie valuta e monitora per il tuo account, per un massimo di 10.000 bucket. Gli addebiti vengono ripartiti proporzionalmente al giorno.

Monitoraggio degli oggetti per il rilevamento automatico di dati sensibili

Questi costi derivano dal monitoraggio e dalla valutazione dell'inventario dei bucket S3 per identificare gli oggetti S3 idonei all'analisi mediante il rilevamento automatico di dati sensibili. Per ulteriori informazioni, consulta [Come funziona l'individuazione automatica dei dati sensibili](#).

L'addebito viene effettuato in base al numero totale di oggetti S3 archiviati in bucket generici per il tuo account. Gli addebiti vengono ripartiti proporzionalmente al giorno.

Analisi degli oggetti mediante processi di rilevamento di dati sensibili e rilevamento automatico di dati sensibili

Questi costi derivano dall'analisi degli oggetti S3 e dalla segnalazione dei dati sensibili che Macie trova negli oggetti. Ciò include analisi e report mediante processi di rilevamento di dati sensibili e rilevazione automatica di dati sensibili. Per ulteriori informazioni, consulta [Rilevamento dei dati sensibili](#).

I costi vengono addebitati in base alla quantità di dati non compressi che Macie analizza negli oggetti S3. Sono gratuiti gli oggetti che Macie non può analizzare per motivi come l'uso di una classe di storage Amazon S3 non supportata, l'uso di un file o di un formato di archiviazione non supportato o le impostazioni delle autorizzazioni. Inoltre, questi costi non variano in base al numero di dati sensibili rilevati dai lavori o dall'individuazione automatica di dati sensibili.

Per gestire i costi del rilevamento automatico di dati sensibili, puoi escludere singoli bucket S3 dalle analisi. Ad esempio, è possibile escludere i bucket noti per soddisfare i requisiti di sicurezza e conformità dell'organizzazione. Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, un'opzione aggiuntiva consiste nell'abilitare o disabilitare selettivamente l'individuazione automatica dei dati sensibili per i singoli account dell'organizzazione. Per ulteriori informazioni, consulta [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#).

I costi per i lavori di rilevamento di dati sensibili sono limitati dalla [quota mensile di scoperta di dati sensibili prevista](#) per il tuo account. (La quota predefinita è di 5 TB di dati). Se un lavoro è in esecuzione e l'analisi degli oggetti idonei raggiunge questa quota, Macie sospende automaticamente il lavoro fino all'inizio del mese solare successivo e la quota mensile viene reimpostata per il tuo account, oppure tu aumenti la quota per il tuo account.

Se sei l'amministratore Macie di un'organizzazione, i costi per i lavori di rilevamento di dati sensibili sono limitati dalla quota mensile di scoperta di dati sensibili per ogni account per cui analizzi i dati. La quota per un account membro definisce la quantità massima di dati che le tue offerte di lavoro e le offerte di lavoro dell'account membro possono analizzare per l'account durante un mese solare. Se un processo è in esecuzione e l'analisi degli oggetti idonei raggiunge questa quota per un account membro, Macie interrompe l'analisi degli oggetti nei bucket di proprietà dell'account. Quando Macie finisce di analizzare gli oggetti per tutti gli altri account che non hanno raggiunto la quota, Macie mette automaticamente in pausa il lavoro. Se si tratta di un lavoro una tantum, Macie lo riprende automaticamente all'inizio del mese di calendario successivo oppure la quota viene aumentata per tutti gli account interessati, a seconda dell'evento che si verifica per primo. Se si tratta di un processo periodico, Macie lo riprende automaticamente quando è programmato l'inizio dell'esecuzione successiva o inizia il mese di calendario successivo, a seconda di quale evento si verifica per primo. Se un'esecuzione pianificata inizia prima dell'inizio del mese di calendario successivo o la quota per un account interessato viene aumentata, Macie non analizza gli oggetti nei bucket di proprietà dell'account.

 Tip

Per suggerimenti utili sulla gestione o la riduzione dei costi di scoperta dei dati sensibili, consulta il seguente post sul blog sulla AWS sicurezza: [Come usare Amazon Macie per ridurre il costo della scoperta di dati sensibili](#).

Per informazioni dettagliate ed esempi di costi di utilizzo, consulta i prezzi di [Amazon Macie](#).

Quando usi Macie per esaminare i costi di utilizzo stimati, è importante capire come vengono calcolate le stime dei costi. Considera i seguenti aspetti:

- Le stime sono riportate in dollari USA (USD) e si riferiscono Regione AWS solo ai prezzi correnti. Se usi Macie in più regioni, i dati non vengono aggregati per tutte le regioni in cui usi Macie.
- Sulla console, le stime sono comprensive per il mese di calendario corrente fino alla data odierna. Se esegui una query sui dati a livello di codice con l'API Amazon Macie, puoi scegliere un intervallo di tempo inclusivo per le stime. Può trattarsi di un intervallo di tempo continuativo dei 30 giorni precedenti o del mese di calendario corrente fino alla data odierna.
- Le stime non riflettono tutti gli sconti che potrebbero essere applicati al tuo account. L'eccezione sono gli sconti che derivano dai livelli di prezzo regionali in base ai volumi, come descritto nei

prezzi di [Amazon Macie](#). Se il tuo account è idoneo per questo tipo di sconto, le stime riflettono tale sconto.

- Se sei l'amministratore Macie di un'organizzazione, le stime non riflettono gli sconti combinati sul volume di utilizzo per la tua organizzazione. Per informazioni su questi sconti, consulta [Sconti per grandi volumi](#) nella Guida per l'AWS Billing utente.
- Per il monitoraggio del controllo preventivo, la stima si basa sul costo medio giornaliero per l'intervallo di tempo applicabile. Il costo è ripartito proporzionalmente al giorno.
- Per quanto riguarda l'individuazione automatica dei dati sensibili, la stima complessiva si basa sul costo medio giornaliero per il monitoraggio degli oggetti (ripartito proporzionalmente al giorno) e sulla quantità di dati non compressi che Macie ha analizzato finora nell'intervallo di tempo applicabile. Se sei l'amministratore Macie di un'organizzazione e abiliti il rilevamento automatico dei dati sensibili per gli account dei membri, i costi stimati di tali attività sono inclusi nelle stime per ogni account membro applicabile.
- Per i lavori di rilevamento di dati sensibili, la stima si basa sulla quantità di dati non compressi che i job hanno analizzato finora durante l'intervallo di tempo applicabile. Se sei l'amministratore Macie di un'organizzazione e gestisci lavori che analizzano i dati per gli account dei membri, i costi stimati di tali lavori sono inclusi nella stima per ogni account membro applicabile.
- Se il tuo account è un account membro di un'organizzazione e il tuo amministratore Macie abilita il rilevamento automatico di dati sensibili o esegue processi di rilevamento di dati sensibili che analizzano i tuoi dati, i costi stimati di tali attività sono inclusi nelle stime relative al tuo account.
- Le stime non includono i costi sostenuti per l'utilizzo di altri dispositivi Servizi AWS con determinate funzionalità di Macie. Ad esempio, utilizzando Customer Managed per AWS KMS keys decrittografare gli oggetti S3 che desideri ispezionare per verificare la presenza di dati sensibili.

Tieni inoltre presente che Macie offre un piano mensile gratuito per l'analisi degli oggetti S3 mediante processi di rilevamento di dati sensibili e il rilevamento automatico di dati sensibili. Ogni mese, non è previsto alcun costo per analizzare fino a 1 GB di dati per scoprire e segnalare dati sensibili negli oggetti S3. Se in un determinato mese vengono analizzati più di 1 GB di dati, i costi di rilevamento dei dati sensibili iniziano a gravare sull'account dopo il primo GB di dati. Se in un determinato mese vengono analizzati meno di 1 GB di dati, l'allocazione residua non viene trasferita al mese successivo. Se il tuo account fa parte di un'organizzazione con fatturazione consolidata, il piano gratuito si applica alla quantità combinata di dati analizzati per la tua organizzazione. In altre parole, non è previsto alcun costo per analizzare fino a 1 GB di dati ogni mese per tutti gli account dell'organizzazione.

Analisi dei costi di utilizzo stimati per Macie

Per esaminare i costi di utilizzo stimati correnti per Amazon Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Sia la console che l'API forniscono costi stimati per le dimensioni dei prezzi di Macie. Se attualmente stai partecipando a una prova gratuita di 30 giorni, puoi utilizzare questi dati per stimare i costi per l'utilizzo di Macie al termine della prova gratuita. Per informazioni sulle dimensioni e le considerazioni relative ai prezzi di Macie, consulta [Comprendere i costi di utilizzo stimati](#). Per informazioni dettagliate ed esempi di costi di utilizzo, consulta i prezzi di [Amazon Macie](#).

In Macie, i costi di utilizzo stimati sono riportati in dollari USA (USD) e si applicano solo agli attuali. Regione AWS Se si utilizza la console per esaminare i dati, le stime dei costi si riferiscono al mese di calendario corrente fino alla data corrente (incluso). Se esegui una query sui dati a livello di codice con l'API Amazon Macie, puoi specificare un intervallo di tempo inclusivo per le stime, un intervallo continuativo dei 30 giorni precedenti o il mese di calendario corrente fino alla data corrente.

Argomenti

- [Analisi dei costi di utilizzo stimati sulla console Amazon Macie](#)
- [Interrogazione dei costi di utilizzo stimati con l'API Amazon Macie](#)

Analisi dei costi di utilizzo stimati sulla console Amazon Macie

Sulla console Amazon Macie, le stime dei costi sono organizzate come segue:

- Monitoraggio del controllo preventivo: si tratta del costo stimato per la manutenzione di un inventario dei bucket generici Amazon Simple Storage Service (Amazon S3) per uso generico e per la valutazione e il monitoraggio dei bucket per la sicurezza e il controllo degli accessi.
- Lavori di rilevamento di dati sensibili: si tratta del costo stimato dei processi di rilevamento di dati sensibili che hai eseguito.
- Rilevamento automatico di dati sensibili: questi sono i costi stimati dell'esecuzione del rilevamento automatico di dati sensibili. Ciò include il monitoraggio e la valutazione dell'inventario dei bucket S3 per identificare gli oggetti S3 idonei all'analisi. Include anche l'analisi degli oggetti idonei e la segnalazione di dati sensibili, statistiche, risultati e altri tipi di risultati.

Per esaminare le stime relative all'individuazione automatica di dati sensibili tramite la console, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo.

Per rivedere i costi di utilizzo stimati sulla console

Segui questi passaggi per rivedere i costi di utilizzo stimati utilizzando la console Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri rivedere i costi stimati.
3. Nel riquadro di navigazione, scegli Utilizzo.

Se disponi di un account Macie autonomo o di un account membro in un'organizzazione, la pagina Utilizzo mostra una ripartizione dei costi di utilizzo stimati per il tuo account.

Se sei l'amministratore Macie di un'organizzazione, la pagina Utilizzo elenca gli account della tua organizzazione. Nella tabella:

- Quota di servizio — Lavori: questa è la quota mensile attuale per l'esecuzione di processi di rilevamento di dati sensibili per analizzare gli oggetti S3 nei bucket di proprietà di un account.
- Prova gratuita: questi campi indicano se un account sta attualmente partecipando alla prova gratuita per il controllo preventivo, il monitoraggio o l'individuazione automatica di dati sensibili. Il campo Prova gratuita è vuoto se la prova gratuita applicabile per un account è terminata.
- Totale: si tratta del costo totale stimato per un account.

La sezione Costi stimati mostra il costo totale stimato per l'organizzazione e una suddivisione di tali costi. Per esaminare la ripartizione dei costi stimati per un account specifico dell'organizzazione, scegli il conto nella tabella. La sezione Costi stimati mostra quindi questa ripartizione. Per mostrare questi dati per un altro account, scegli l'account nella tabella. Per cancellare la selezione dell'account, scegli X accanto all'ID dell'account.

Interrogazione dei costi di utilizzo stimati con l'API Amazon Macie

Per interrogare i costi di utilizzo stimati a livello di codice, puoi utilizzare le seguenti operazioni dell'API Amazon Macie:

- **GetUsageTotals**— Questa operazione restituisce i costi di utilizzo totali stimati per il tuo account, raggruppati per metrica di utilizzo. Se sei l'amministratore Macie di un'organizzazione, questa operazione restituisce stime dei costi aggregate per tutti gli account dell'organizzazione. Per ulteriori informazioni su questa operazione, consulta [Usage Totals](#) nel Amazon Macie API Reference.

- **GetUsageStatistics**— Questa operazione restituisce le statistiche di utilizzo e i dati correlati per il tuo account, raggruppati per account e quindi per metrica di utilizzo. I dati includono i costi di utilizzo totali stimati e le quote delle partite correnti. Se applicabile, indica anche quando è iniziata la prova gratuita di 30 giorni per Macie e per il rilevamento automatico dei dati sensibili. Se sei l'amministratore Macie di un'organizzazione, questa operazione restituisce una suddivisione dei dati per tutti gli account dell'organizzazione. Puoi personalizzare la tua query ordinando e filtrando i risultati della query. Per ulteriori informazioni su questa operazione, consulta [Statistiche di utilizzo](#) nel riferimento alle API di Amazon Macie.

Quando utilizzi una delle due operazioni, puoi facoltativamente specificare un intervallo di tempo inclusivo per i dati. Questo intervallo di tempo può essere un intervallo temporale continuo dei 30 giorni precedenti (PAST_30_DAYS) o del mese di calendario corrente fino alla data (MONTH_TO_DATE). Se non specifichi un intervallo di tempo, Macie restituisce i dati per i 30 giorni precedenti.

Gli esempi seguenti mostrano come interrogare i costi di utilizzo e le statistiche stimati utilizzando [AWS Command Line Interface \(AWS CLI\)](#). Puoi anche interrogare i dati utilizzando una versione corrente di un altro strumento a riga di AWS comando o di un AWS SDK oppure inviando richieste HTTPS direttamente a Macie. Per informazioni sugli AWS strumenti e SDKs, consulta [Tools to Build on AWS](#).

Esempi

- [Esempio 1: Interrogazione dei costi di utilizzo totali stimati](#)
- [Esempio 2: interrogazione delle statistiche di utilizzo](#)

Esempio 1: Interrogazione dei costi di utilizzo totali stimati

Per interrogare i costi di utilizzo totali stimati utilizzando il AWS CLI, esegui il [get-usage-totals](#) comando e, facoltativamente, specifica un intervallo di tempo per i dati. Per esempio:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

Dove **MONTH_TO_DATE** specifica il mese corrente del calendario corrente come intervallo di tempo per i dati.

Se eseguirai il comando correttamente, riceverai un output simile al seguente.

```
{
  "timeRange": "MONTH_TO_DATE",
  "usageTotals": [
    {
      "currency": "USD",
      "estimatedCost": "153.45",
      "type": "SENSITIVE_DATA_DISCOVERY"
    },
    {
      "currency": "USD",
      "estimatedCost": "65.18",
      "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
    },
    {
      "currency": "USD",
      "estimatedCost": "1.51",
      "type": "DATA_INVENTORY_EVALUATION"
    },
    {
      "currency": "USD",
      "estimatedCost": "0.98",
      "type": "AUTOMATED_OBJECT_MONITORING"
    }
  ]
}
```

estimatedCostDov'è il costo di utilizzo totale stimato per la metrica di utilizzo associata ()type:

- SENSITIVE_DATA_DISCOVERY, per analizzare oggetti S3 con processi di rilevamento di dati sensibili.
- AUTOMATED_SENSITIVE_DATA_DISCOVERY, per analizzare oggetti S3 con rilevamento automatico di dati sensibili.
- DATA_INVENTORY_EVALUATION, per il monitoraggio e la valutazione dei bucket generici S3 per la sicurezza e il controllo degli accessi.
- AUTOMATED_OBJECT_MONITORING, per valutare e monitorare l'inventario dei bucket S3 per identificare gli oggetti S3 idonei all'analisi mediante il rilevamento automatico di dati sensibili.

Esempio 2: interrogazione delle statistiche di utilizzo

Per interrogare le statistiche di utilizzo utilizzando il AWS CLI, esegui il [get-usage-statistics](#) comando. Facoltativamente, è possibile ordinare, filtrare e specificare un intervallo di tempo per i risultati della query. L'esempio seguente recupera le statistiche di utilizzo per un account amministratore Macie per i 30 giorni precedenti. I risultati vengono ordinati in ordine crescente per ID. Account AWS

Per Linux, macOS o Unix, utilizzando il carattere di continuazione di riga con barra rovesciata (\) per migliorare la leggibilità:

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Per Microsoft Windows, utilizzando il carattere di continuazione di riga con cursore (^) per migliorare la leggibilità:

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={"key\":"accountId\","orderBy\":"ASC\"} ^
--time-range PAST_30_DAYS
```

Dove:

- **accountId** specifica il campo da utilizzare per ordinare i risultati.
- **ASC** è il tipo di ordinamento da applicare ai risultati, in base al valore del campo specificato (**accountId**).
- **PAST_30_DAYS** specifica i 30 giorni precedenti come intervallo di tempo per i dati.

Se il comando viene eseguito correttamente, Macie restituisce un array. records L'array contiene un oggetto per ogni account incluso nei risultati della query. Per esempio:

```
{
  "records": [
    {
      "accountId": "111122223333",
      "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
      "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
      "usage": [
        {
          "currency": "USD",
```

```

        "estimatedCost": "1.51",
        "type": "DATA_INVENTORY_EVALUATION"
    },
    {
        "currency": "USD",
        "estimatedCost": "65.18",
        "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
    },
    {
        "currency": "USD",
        "estimatedCost": "153.45",
        "serviceLimit": {
            "isServiceLimited": false,
            "unit": "TERABYTES",
            "value": 50
        },
        "type": "SENSITIVE_DATA_DISCOVERY"
    },
    {
        "currency": "USD",
        "estimatedCost": "0.98",
        "type": "AUTOMATED_OBJECT_MONITORING"
    }
]
},
{
    "accountId": "444455556666",
    "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
    "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
    "usage": [
        {
            "currency": "USD",
            "estimatedCost": "1.58",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "63.13",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "145.12",
            "serviceLimit": {

```

```

        "isServiceLimited": false,
        "unit": "TERABYTES",
        "value": 50
      },
      "type": "SENSITIVE_DATA_DISCOVERY"
    },
    {
      "currency": "USD",
      "estimatedCost": "1.02",
      "type": "AUTOMATED_OBJECT_MONITORING"
    }
  ]
},
"timeRange": "PAST_30_DAYS"
}

```

`estimatedCost` Dov'è il costo di utilizzo totale stimato per la metrica di utilizzo associata (`type`) per un account:

- `DATA_INVENTORY_EVALUATION`, per il monitoraggio e la valutazione dei bucket generici S3 per la sicurezza e il controllo degli accessi.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, per analizzare gli oggetti S3 con il rilevamento automatico di dati sensibili.
- `SENSITIVE_DATA_DISCOVERY`, per analizzare oggetti S3 con processi di rilevamento di dati sensibili.
- `AUTOMATED_OBJECT_MONITORING`, per valutare e monitorare l'inventario dei bucket S3 dell'account per identificare gli oggetti S3 idonei all'analisi mediante rilevamento automatico di dati sensibili.

Partecipazione alla prova gratuita di Macie

Quando abiliti Amazon Macie per la prima volta, vieni automaticamente registrato alla prova gratuita di 30 giorni di Macie. Account AWS Sono inclusi gli account dei singoli membri di un'organizzazione. AWS Organizations

Durante la prova gratuita, l'utilizzo di Macie è gratuito Regione AWS per:

- Esegui il monitoraggio del controllo preventivo: include la generazione e la manutenzione di un inventario dei bucket generici Amazon Simple Storage Service (Amazon S3) nella regione. Include anche la valutazione e il monitoraggio dei bucket per la sicurezza e il controllo degli accessi.

Per ulteriori informazioni, consulta [In che modo Macie monitora la sicurezza dei dati di Amazon S3](#).

- Esegui il rilevamento automatico dei dati sensibili: include il monitoraggio e la valutazione dell'inventario dei bucket S3 nella regione per identificare gli oggetti S3 idonei all'analisi. Include anche l'analisi degli oggetti idonei e la segnalazione di dati sensibili, statistiche, risultati e altri tipi di risultati. Per configurare e gestire questa funzionalità, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo. Se sei un amministratore Macie, puoi utilizzare questa funzione per analizzare gli oggetti nei bucket S3 di proprietà dei tuoi account membro.

Per ulteriori informazioni, consulta [Come funziona l'individuazione automatica dei dati sensibili](#).

Per un elenco delle regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

La prova gratuita è valida per 30 giorni consecutivi. Non puoi metterlo in pausa dopo l'avvio. Al termine della prova gratuita, iniziano a maturare i costi per l'esecuzione del monitoraggio del controllo preventivo. Cominciano a maturare anche i costi per l'individuazione automatica di dati sensibili. Se sei l'amministratore Macie di un'organizzazione, gli addebiti verranno addebitati a seconda dei casi per ogni account dell'organizzazione. Puoi utilizzare Macie per esaminare i dettagli dei costi di utilizzo stimati per i singoli account della tua organizzazione.

Note

Durante la prova gratuita, potresti incorrere in costi aggiuntivi per altre funzionalità utilizzate con determinate funzionalità di Macie, ad esempio l'utilizzo di Customer Managed per decrittografare gli oggetti S3 Servizi AWS che desideri ispezionare AWS KMS keys alla ricerca di dati sensibili.

La versione di prova gratuita non include l'analisi degli oggetti S3 mediante processi di rilevamento di dati sensibili. Ti verranno addebitati dei costi se crei ed esegui processi di rilevamento di dati sensibili che analizzano più di 1 GB di dati non compressi durante la prova gratuita. (Macie offre un piano gratuito mensile per l'individuazione di dati sensibili. Ogni mese, non è previsto alcun costo per analizzare fino a 1 GB di dati non compressi in oggetti S3. Dopo il primo GB di dati, i costi si accumulano.)

Durante la prova gratuita, puoi controllare lo stato della prova e rivedere i costi di utilizzo stimati per il tuo account. Le stime dei costi si basano sull'utilizzo di Macie finora utilizzato durante la prova gratuita. Possono aiutarti a capire quali potrebbero essere alcuni dei tuoi costi di utilizzo al termine del periodo di prova. Per informazioni dettagliate su come Macie calcola questi valori, consulta.

[Comprendere i costi di utilizzo stimati](#)

Per verificare lo stato e i costi stimati durante la prova gratuita

Segui questi passaggi per verificare lo stato della versione di prova e rivedere i costi di utilizzo stimati utilizzando la console Amazon Macie. Per accedere a questi dati a livello di codice, puoi utilizzare il [GetUsageStatistics](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri verificare lo stato della prova gratuita e i costi di utilizzo stimati.
3. Nel riquadro di navigazione, scegli Utilizzo.

La pagina di utilizzo indica il numero di giorni rimanenti della prova gratuita. Mostra anche una ripartizione dei costi di utilizzo stimati in dollari USA (USD):

- Monitoraggio del controllo preventivo: si tratta del costo totale previsto per la manutenzione di un inventario dei bucket generici S3 e per la valutazione e il monitoraggio dei bucket per motivi di sicurezza e controllo degli accessi al termine del periodo di prova gratuito.
- Lavori di rilevamento di dati sensibili: si tratta del costo totale stimato di tutti i job di rilevamento di dati sensibili che hai eseguito. I lavori di rilevamento di dati sensibili non sono inclusi nella versione di prova gratuita.
- Rilevamento automatico di dati sensibili: questi sono i costi totali previsti per l'esecuzione del rilevamento automatico di dati sensibili al termine del periodo di prova gratuito, suddivisi per dimensione del prezzo: monitoraggio degli oggetti e analisi degli oggetti. Per rivedere queste stime sulla console, devi essere l'amministratore Macie di un'organizzazione o disporre di un account Macie autonomo.

Se sei l'amministratore Macie di un'organizzazione, la pagina Utilizzo fornisce dettagli sugli account dell'organizzazione. Nella tabella:

- Quota di servizio — Lavori: questa è la quota mensile attuale per l'esecuzione di processi di rilevamento di dati sensibili per analizzare gli oggetti S3 nei bucket di proprietà di un account.

- **Prova gratuita:** questi campi indicano se un account sta attualmente partecipando alla prova gratuita per il controllo preventivo, il monitoraggio o l'individuazione automatica di dati sensibili. Il campo Prova gratuita è vuoto se la prova gratuita applicabile per un account è terminata.
- **Totale:** si tratta del costo totale stimato per un account.

La sezione Costi stimati mostra i costi stimati per l'intera organizzazione. Per esaminare la ripartizione dei costi stimati per un account specifico dell'organizzazione, scegli il conto nella tabella. La sezione Costi stimati mostra quindi questa ripartizione. Per mostrare questi dati per un altro account, scegli l'account nella tabella. Per cancellare la selezione dell'account, scegli X accanto all'ID dell'account.

Note

Se un account archivia più di 150 TB di dati in Amazon S3, i costi stimati ed effettivi dell'account per l'individuazione automatica di dati sensibili potrebbero essere superiori alle proiezioni dei costi fornite da Macie durante la prova gratuita di 30 giorni. Questo perché l'analisi degli oggetti mediante il rilevamento automatico dei dati sensibili viene sospesa quando vengono analizzati 150 GB di dati non compressi per un account registrato alla prova gratuita. L'analisi degli oggetti riprende per l'account al termine della prova gratuita. Per assistenza nella previsione dei costi per un account che archivia più di 150 TB di dati in Amazon S3, contatta [Supporto AWS](#).

Per gestire i costi per l'individuazione automatica dei dati sensibili al termine del periodo di prova gratuito, puoi escludere singoli bucket S3 dalle analisi successive. Se sei l'amministratore Macie di un'organizzazione, un'opzione aggiuntiva consiste nell'abilitare o disabilitare in modo selettivo il rilevamento automatico dei dati sensibili per i singoli account dell'organizzazione. Per informazioni su queste opzioni, consulta [Configurazione delle impostazioni per l'individuazione automatica dei dati sensibili](#).

Gestione di più account Macie come organizzazione

Se il tuo AWS ambiente ha più account, puoi associare gli account Amazon Macie nel tuo ambiente e gestirli centralmente come organizzazione in Macie. Con questa configurazione, un amministratore Macie designato può valutare e monitorare il livello di sicurezza generale dell'insieme di dati Amazon Simple Storage Service (Amazon S3) dell'organizzazione e scoprire i dati sensibili nei bucket S3 dell'organizzazione. L'amministratore può anche eseguire diverse attività di gestione e amministrazione degli account su larga scala, come il monitoraggio dei costi di utilizzo stimati e la valutazione delle quote degli account.

In Macie, un'organizzazione è composta da un account amministratore Macie designato e da uno o più account membro associati. È possibile associare gli account in due modi: integrando Macie con Macie AWS Organizations o inviando e accettando gli inviti di iscrizione in Macie. Ti consigliamo di integrare Macie con AWS Organizations.

AWS Organizations è un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire centralmente più account. Account AWS Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più piattaforme Servizi AWS, tra cui Macie e Amazon. AWS Security Hub GuardDuty Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Organizations](#).

Se preferisci gestire centralmente più account Macie senza utilizzarli AWS Organizations, puoi utilizzare invece gli inviti all'iscrizione. Se invii un invito e questo viene accettato da un altro account, quest'ultimo diventa l'account amministratore Macie dell'altro account. Se ricevi e accetti un invito, il tuo account diventa un account membro Macie e l'account amministratore Macie può accedere e gestire determinate impostazioni, dati e risorse per il tuo account Macie.

Argomenti

- [Relazioni tra amministratore e account membro di Macie](#)
- [Gestione di più account Macie con AWS Organizations](#)
- [Gestione di più account Macie su invito](#)

Relazioni tra amministratore e account membro di Macie

Se gestisci centralmente più account Amazon Macie come organizzazione, l'amministratore Macie ha accesso ai dati di inventario di Amazon Simple Storage Service (Amazon S3), ai risultati delle policy

e ad alcune impostazioni e risorse di Macie per gli account membro associati. L'amministratore può anche abilitare il rilevamento automatico dei dati sensibili ed eseguire processi di rilevamento di dati sensibili per rilevare i dati sensibili nei bucket S3 di proprietà degli account membri. Il supporto per attività specifiche varia a seconda che un account amministratore Macie sia associato a un account membro tramite AWS Organizations o su invito.

La tabella seguente fornisce dettagli sulla relazione tra l'amministratore di Macie e gli account dei membri. Indica le autorizzazioni predefinite per ogni tipo di account. Per limitare ulteriormente l'accesso alle funzionalità e alle operazioni di Macie, puoi utilizzare policy personalizzate [AWS Identity and Access Management \(IAM\)](#).

Nella tabella:

- Self indica che l'account non può eseguire l'operazione per nessun account associato.
- Qualsiasi indica che l'account può eseguire l'operazione per un singolo account associato.
- Tutto indica che l'account può eseguire l'operazione e l'attività si applica a tutti gli account associati.

Un trattino (—) indica che l'account non è in grado di eseguire l'operazione.

Attività	Tramite AWS Organizations		Su invito	
	Amministratore	Membro	Amministratore	Membro
Abilita Macie	Qualsiasi	—	Personale	Personale
Esamina l'inventario degli account dell'organizzazione 1	Tutti	—	Tutti	—
Aggiungi un account membro	Qualsiasi	—	Qualsiasi	—
Rivedi le statistiche e i metadati per i bucket S3	Tutti	Personale	Tutti	Personale

Esamina i risultati delle politiche	Tutti	Personale	Tutti	Personale
Sopprimere (archivia re) i risultati delle politiche 2	Tutti	–	Tutti	–
Pubblica i risultati delle politiche 3	Personale	Personale	Personale	Personale
Configurare un repository per i risultati del rilevamento di dati sensibili 4	Personale	Personale	Personale	Personale
Creare e utilizzare elenchi di autorizzazioni	Personale	Personale	Personale	Personale
Crea e utilizza identificatori di dati personalizzati	Personale	Personale	Personale	Personale
Configura le impostazioni di rilevamento automatico dei dati sensibili	Tutti	–	Tutti	–
Abilita o disabilita l'individuazione automatica dei dati sensibili	Qualsiasi	–	Qualsiasi	–

Rivedi le statistiche, i dati e i risultati automatizzati sull'individuazione dei dati sensibili 5	Tutti	Personale	Tutti	Personale
Crea ed esegui processi di rilevamento di dati sensibili 6	Qualsiasi	Personale	Qualsiasi	Personale
Esamina i dettagli dei processi di rilevamento di dati sensibili 7	Personale	Personale	Personale	Personale
Esamina i risultati relativi ai dati sensibili 8	Personale	Personale	Personale	Personale
Elimina (archivia) i risultati relativi ai dati sensibili 8	Personale	Personale	Personale	Personale
Pubblica i risultati relativi ai dati sensibili 8	Personale	Personale	Personale	Personale
Configura Macie per recuperare campioni di dati sensibili a fini di individuazione	Personale	Personale	Personale	Personale

Recupera campioni di dati sensibili per i risultati 9	Personale	Personale	Personale	Personale
Configura le destinazioni di pubblicazione per i risultati	Personale	Personale	Personale	Personale
Imposta la frequenza di pubblicazione dei risultati	Tutti	Personale	Tutti	Personale
Crea risultati di esempio	Personale	Personale	Personale	Personale
Rivedi le quote degli account e i costi di utilizzo stimati	Tutti	Personale	Tutti	Personale
Sospendere Macie 10	Qualsiasi	–	Qualsiasi	Personale
Disattiva Macie 11	Personale	Personale	Personale	Personale
Rimuovi (dissocia) un account membro	Qualsiasi	–	Qualsiasi	–
Dissociarsi da un account amministratore	–	–	–	Personale
Eliminare un'azione con un altro account 12	Qualsiasi	–	Qualsiasi	Personale

1.
L'amministratore di un'organizzazione AWS Organizations può esaminare tutti gli account dell'organizzazione, inclusi gli account che non hanno abilitato Macie. L'amministratore di un'organizzazione basata su invito può esaminare solo gli account che aggiunge al proprio inventario.
2.
Solo un amministratore può eliminare i risultati delle politiche. Se un amministratore crea una regola di soppressione, Macie la applica ai risultati delle politiche per tutti gli account dell'organizzazione, a meno che la regola non sia configurata per escludere account specifici. Se un membro crea una regola di soppressione, Macie non applica la regola ai risultati delle policy per l'account del membro.
3.
Solo l'account che possiede una risorsa interessata può pubblicare i risultati delle politiche relative alla risorsa. AWS Security Hub Sia gli account amministratore che quelli membri pubblicano automaticamente su Amazon i risultati delle politiche per una risorsa interessata EventBridge.
4.
Se un amministratore abilita il rilevamento automatico di dati sensibili o configura un processo per analizzare gli oggetti nei bucket S3 di proprietà di un account membro, Macie archivia i risultati del rilevamento dei dati sensibili nell'archivio dell'account amministratore.
5.
Solo un amministratore può accedere ai risultati di dati sensibili prodotti dal rilevamento automatico di dati sensibili. Sia un amministratore che un membro possono esaminare altri tipi di dati generati dall'individuazione automatica di dati sensibili per l'account del membro.
6.
Un membro può configurare un processo per analizzare gli oggetti solo nei bucket S3 di proprietà del proprio account. Un amministratore può configurare un processo per analizzare gli oggetti nei bucket di proprietà del proprio account o di un account membro. Per informazioni su come vengono applicate le quote e vengono calcolati i costi per i lavori con più account, vedere. [Comprendere i costi di utilizzo stimati](#)
7.
Solo l'account che crea un lavoro può accedere ai dettagli del lavoro. Ciò include i dettagli relativi al lavoro nell'inventario del bucket S3.
8.
Solo l'account che crea un lavoro può accedere, eliminare o pubblicare i risultati dei dati sensibili prodotti dal lavoro. Solo un amministratore può accedere, eliminare o pubblicare i risultati di dati sensibili prodotti dal rilevamento automatico di dati sensibili.
- 9.

Se un rilevamento di dati sensibili si applica a un oggetto S3 di proprietà di un account membro, l'amministratore potrebbe essere in grado di recuperare campioni di dati sensibili segnalati dal risultato. Ciò dipende dall'origine del risultato e dalle impostazioni e dalle risorse di configurazione nell'account amministratore e nell'account membro. Per ulteriori informazioni, consulta [Opzioni di configurazione per il recupero di campioni di dati sensibili](#).

10. Affinché un amministratore possa sospendere Macie per il proprio account, deve prima dissociare il proprio account da tutti gli account dei membri.
11. Affinché un amministratore possa disattivare Macie per il proprio account, deve prima dissociare il proprio account da tutti gli account membri ed eliminare le associazioni tra il proprio account e tutti gli account. L'amministratore di un'organizzazione AWS Organizations può farlo collaborando con l'account di gestione dell'organizzazione per designare un account diverso come account amministratore.

Affinché un membro di un' AWS Organizations organizzazione possa disattivare Macie, l'amministratore deve prima dissociare l'account del membro dal suo account amministratore. In un'organizzazione basata su inviti, il membro può dissociare il proprio account dall'account amministratore e quindi disattivare Macie.
12. L'amministratore di un'organizzazione AWS Organizations può eliminare un'associazione con un account membro dopo aver dissociato l'account dal proprio account amministratore. L'account continua a comparire nell'inventario degli account dell'amministratore, ma il suo stato indica che non è un account membro. In un'organizzazione basata su inviti, un amministratore e un membro possono eliminare un'associazione con un altro account dopo aver dissociato il proprio account dall'altro account. L'altro account smette quindi di apparire nell'inventario dell'account.

Gestione di più account Macie con AWS Organizations

Se utilizzi AWS Organizations la gestione centralizzata di più account Account AWS, puoi integrare Amazon Macie con AWS Organizations e quindi gestire centralmente Macie per gli account della tua organizzazione. Con questa configurazione, un amministratore Macie designato può abilitare e gestire Macie per un massimo di 10.000 account. L'amministratore può anche accedere ai dati di inventario di Amazon Simple Storage Service (Amazon S3) e scoprire i dati sensibili nei bucket S3 di proprietà degli account. Per informazioni dettagliate sulle attività che l'amministratore può eseguire, consulta [Relazioni tra amministratore e account membro di Macie](#)

AWS Organizations è un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire centralmente più account. Account AWS Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più piattaforme Servizi AWS, tra cui Macie e Amazon. AWS Security Hub GuardDuty Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Organizations](#).

Per integrare Macie con AWS Organizations, devi innanzitutto designare un account come account amministratore Macie delegato per l'organizzazione. L'amministratore Macie abilita quindi Macie per altri account dell'organizzazione, aggiunge tali account come account membro Macie e configura le impostazioni e le risorse di Macie per gli account.

Tip

Se hai già associato un account amministratore Macie agli account dei membri utilizzando gli inviti, puoi designare quell'account come account amministratore Macie delegato per la tua organizzazione in. AWS Organizations Se lo fai, tutti gli account membro attualmente associati rimangono membri e puoi sfruttare appieno i vantaggi della gestione degli account utilizzando. AWS Organizations Per ulteriori informazioni, consulta [Passaggio da un'organizzazione basata su inviti](#).

Gli argomenti di questa sezione spiegano come integrare Macie AWS Organizations e come amministrare e gestire Macie for account in un'organizzazione.

Argomenti

- [Considerazioni sull'utilizzo di Macie con AWS Organizations](#)
- [Integrazione e configurazione di un'organizzazione in Macie](#)
- [Revisione degli account Macie per un'organizzazione](#)
- [Gestione degli account dei membri Macie per un'organizzazione](#)
- [Modifica dell'account amministratore Macie per un'organizzazione](#)
- [Disattivazione dell'integrazione di Macie con AWS Organizations](#)

Considerazioni sull'utilizzo di Macie con AWS Organizations

Prima di integrare Amazon Macie AWS Organizations e configurare la tua organizzazione in Macie, considera i seguenti requisiti e consigli. Assicurati inoltre di comprendere la [relazione tra l'account amministratore di Macie e quello dei membri](#).

Argomenti

- [Designazione di un account amministratore Macie](#)
- [Modifica o rimozione della designazione di un account amministratore Macie](#)
- [Aggiungere e rimuovere gli account dei membri di Macie](#)
- [Passaggio da un'organizzazione basata su inviti](#)

Designazione di un account amministratore Macie

Mentre stabilisci quale account deve essere l'account amministratore Macie delegato per la tua organizzazione, tieni presente quanto segue:

- Un'organizzazione può avere un solo account amministratore Macie delegato.
- Un account non può essere un amministratore e un account membro di Macie allo stesso tempo.
- Solo l'account di AWS Organizations gestione di un'organizzazione può designare l'account amministratore Macie delegato per l'organizzazione. Solo l'account di gestione può successivamente modificare o rimuovere tale designazione.
- L'account di AWS Organizations gestione di un'organizzazione può anche essere l'account amministratore Macie delegato per l'organizzazione. Tuttavia, non consigliamo questa configurazione in base alle migliori pratiche AWS di sicurezza e al principio del privilegio minimo. È probabile che gli utenti che hanno accesso all'account di gestione per scopi di fatturazione siano diversi dagli utenti che devono accedere a Macie per motivi di sicurezza delle informazioni.

Se preferisci questa configurazione, devi abilitare Macie come account di gestione dell'organizzazione in almeno un account Regione AWS prima di designare l'account come account amministratore Macie delegato. Altrimenti, l'account non sarà in grado di accedere e gestire le impostazioni e le risorse di Macie per gli account dei membri.

- Al contrario AWS Organizations, Macie è un servizio regionale. Ciò significa che la designazione di un account amministratore Macie è una designazione regionale. Significa anche che le associazioni tra gli account amministratore e membro di Macie sono regionali. Ad esempio, se l'account di gestione indica un account amministratore Macie nella regione Stati Uniti orientali

(Virginia settentrionale), l'amministratore Macie può gestire gli account Macie for member solo in quella regione.

Per gestire centralmente più account Macie Regioni AWS, l'account di gestione deve accedere a ciascuna regione in cui l'organizzazione utilizza attualmente o utilizzerà Macie, e quindi designare l'account amministratore Macie in ciascuna di tali regioni. L'amministratore Macie può quindi configurare l'organizzazione in ciascuna di queste regioni. Per un elenco delle regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

- Un account può essere associato a un solo account amministratore Macie alla volta. Se l'organizzazione utilizza Macie in più regioni, l'account amministratore Macie designato deve essere lo stesso in tutte le regioni. Tuttavia, l'account di gestione dell'organizzazione deve designare l'account amministratore separatamente in ciascuna regione.
- Un account può essere l'account amministratore Macie delegato per una sola organizzazione alla volta. Se gestisci più organizzazioni in AWS Organizations, devi designare un account amministratore Macie diverso per ogni organizzazione. Ciò è dovuto a un AWS Organizations requisito: un account può essere membro di una sola organizzazione alla volta.

Se l'amministratore di Macie Account AWS viene sospeso, isolato o chiuso, tutti gli account dei membri Macie associati vengono rimossi automaticamente come account membro Macie, ma Macie continua a essere abilitato per gli account. Se il [rilevamento automatico dei dati sensibili](#) è stato abilitato per uno o più account membri, è disabilitato per gli account. Ciò disabilita anche l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni prodotte e fornite direttamente da Macie durante l'individuazione automatica degli account. Per ripristinare l'accesso a questi dati, deve avvenire quanto segue entro 30 giorni:

1. L'amministratore di Macie Account AWS viene ripristinato.
2. L'account AWS Organizations di gestione designa nuovamente l'account come account amministratore di Macie.
3. L'amministratore Macie configura l'organizzazione e abilita nuovamente l'individuazione automatica degli account appropriati.

Dopo 30 giorni, Macie elimina definitivamente i dati precedentemente prodotti e forniti direttamente durante l'individuazione automatica degli account applicabili.

Modifica o rimozione della designazione di un account amministratore Macie

Solo l'account di AWS Organizations gestione di un'organizzazione può modificare o rimuovere la designazione di un account amministratore Macie delegato per l'organizzazione.

Se l'account di gestione modifica o rimuove la designazione:

- Tutti gli account membro associati vengono rimossi come account membro Macie, ma Macie continua a essere abilitato per gli account. Gli account diventano account Macie indipendenti. Per mettere in pausa o smettere di usare Macie, un utente di un account membro deve sospendere (mettere in pausa) o disabilitare (interrompere) Macie per l'account.
- L'individuazione automatica dei dati sensibili è disattivata per ogni account per cui è stata abilitata. Ciò disabilita anche l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni prodotte e fornite direttamente da Macie durante l'esecuzione del rilevamento automatico per ciascun account. Per ripristinare l'accesso a questi dati, l'account di gestione deve designare nuovamente lo stesso account amministratore Macie entro 30 giorni. Inoltre, l'amministratore Macie deve configurare nuovamente l'organizzazione e riattivare il rilevamento automatico per ogni account entro 30 giorni. Dopo 30 giorni, i dati scadono e Macie li elimina definitivamente.

Aggiungere e rimuovere gli account dei membri di Macie

Quando aggiungi, rimuovi e gestisci in altro modo gli account dei membri della tua organizzazione, tieni presente quanto segue:

- Un account amministratore Macie può essere associato a non più di 10.000 account membri Macie ciascuno. Regione AWS Se l'organizzazione supera questa quota, l'amministratore Macie non potrà aggiungere account membro finché non rimuoverà il numero necessario di account membro esistenti nella regione. Quando un'organizzazione raggiunge questa quota, informiamo l'amministratore di Macie creando un AWS Health evento per il suo account. Inviamo anche e-mail all'indirizzo associato al loro account.

Se sei l'amministratore Macie di un'organizzazione, puoi determinare quanti account membro sono attualmente associati al tuo account utilizzando la pagina Account sulla console Amazon Macie o [ListMembers](#) il funzionamento dell'API Amazon Macie. Per ulteriori informazioni, consulta [Revisione degli account Macie per un'organizzazione](#).

- Un account può essere associato a un solo account amministratore Macie alla volta. Ciò significa che un account non può accettare un invito Macie da un altro account se è già associato all'account amministratore Macie di un'organizzazione in AWS Organizations

Allo stesso modo, se un account ha già accettato un invito, l'amministratore Macie di un'organizzazione non AWS Organizations può aggiungere l'account come account membro di Macie. L'account deve prima dissociarsi dal suo attuale account amministratore basato su invito.

- Per aggiungere l'account di AWS Organizations gestione come account membro Macie, un utente dell'account di gestione deve prima abilitare Macie per l'account. L'amministratore Macie non è autorizzato ad abilitare Macie per l'account di gestione.
- Se l'amministratore Macie rimuove un account membro Macie:
 - Macie continua a essere abilitato per l'account. L'account diventa un account Macie indipendente. Per mettere in pausa o smettere di usare Macie, un utente dell'account deve sospendere (mettere in pausa) o disabilitare (interrompere) Macie per l'account.
 - L'individuazione automatica dei dati sensibili è disabilitata per l'account, se è stata abilitata. Ciò disabilita anche l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni prodotte e fornite direttamente da Macie durante l'individuazione automatica dell'account.
- Un account membro non può dissociarsi dal proprio account amministratore Macie. Solo l'amministratore Macie può rimuovere un account come account membro Macie.

Passaggio da un'organizzazione basata su inviti

Se hai già associato un account amministratore Macie agli account dei membri utilizzando gli inviti all'iscrizione a Macie, ti consigliamo di designare quell'account come account amministratore Macie delegato per la tua organizzazione in AWS Organizations. Questo semplifica la transizione da un'organizzazione basata su inviti.

In tal caso, tutti gli account utente attualmente associati continueranno a essere membri. Se un account membro fa parte della tua organizzazione in AWS Organizations, l'associazione dell'account cambia automaticamente da Su invito a Via AWS Organizations in Macie. Se un account membro non fa parte della tua organizzazione in AWS Organizations, l'associazione dell'account continua a essere Su invito. In entrambi i casi, gli account continuano ad essere associati all'account amministratore delegato di Macie come account membro. Per quanto riguarda l'individuazione di dati sensibili, ciò significa anche che gli account possono continuare ad accedere a dati statistici e di altro tipo che Macie ha prodotto e fornito direttamente durante il rilevamento automatico dei dati sensibili per gli account. Inoltre, se l'amministratore di Macie ha configurato processi di rilevamento di dati sensibili per analizzare i dati relativi agli account, le esecuzioni successive continueranno a includere risorse di proprietà degli account.

Consigliamo questo approccio perché un account non può essere associato a più di un account amministratore Macie contemporaneamente. Se si designa un account diverso come account amministratore Macie per la propria organizzazione in AWS Organizations, l'amministratore designato non sarà in grado di gestire gli account che sono già associati a un altro account amministratore Macie tramite invito. Ogni account membro deve prima dissociarsi dal suo attuale account amministratore basato su invito. L'amministratore Macie dell'organizzazione AWS Organizations può quindi aggiungere l'account come account membro Macie e iniziare a gestire l'account.

Dopo aver integrato Macie AWS Organizations e aver configurato l'organizzazione in Macie, puoi facoltativamente designare un account amministratore Macie diverso per l'organizzazione. Puoi anche continuare a utilizzare gli inviti per associare e gestire gli account dei membri che non fanno parte della tua organizzazione. AWS Organizations

Integrazione e configurazione di un'organizzazione in Macie

Per iniziare a utilizzare Amazon Macie con AWS Organizations, l'account di AWS Organizations gestione dell'organizzazione designa un account come account amministratore Macie delegato per l'organizzazione. Ciò abilita Macie come servizio affidabile in AWS Organizations. Inoltre, abilita Macie nell'account Regione AWS amministratore designato e consente all'account amministratore designato di abilitare e gestire Macie per altri account dell'organizzazione in quella regione. Per informazioni su come vengono concesse queste autorizzazioni, consulta [Using AWS Organizations with other Servizi AWS](#) nella Guida per l'AWS Organizations utente.

L'amministratore delegato di Macie configura quindi l'organizzazione in Macie, principalmente aggiungendo gli account dell'organizzazione come account membri Macie nella regione.

L'amministratore può quindi accedere a determinate impostazioni, dati e risorse di Macie per quegli account in quella regione. Possono anche eseguire il rilevamento automatico di dati sensibili ed eseguire processi di rilevamento di dati sensibili per rilevare dati sensibili nei bucket Amazon Simple Storage Service (Amazon S3) di proprietà degli account.

Questo argomento spiega come designare un amministratore Macie delegato per un'organizzazione e come aggiungere gli account dell'organizzazione come account membri di Macie. Prima di eseguire queste attività, assicurati di comprendere la [relazione tra l'amministratore di Macie](#) e gli account dei membri. È anche una buona idea rivedere [le considerazioni e i consigli](#) sull'utilizzo di Macie con AWS Organizations

Attività

- [Passaggio 1: verifica le tue autorizzazioni](#)

- [Passaggio 2: designare l'account amministratore Macie delegato per l'organizzazione](#)
- [Passaggio 3: Abilita e aggiungi automaticamente nuovi account dell'organizzazione come account membri di Macie](#)
- [Passaggio 4: abilitare e aggiungere gli account aziendali esistenti come account membri di Macie](#)

Per integrare e configurare l'organizzazione in più regioni, l'account di AWS Organizations gestione e l'amministratore Macie delegato ripetono questi passaggi in ogni regione aggiuntiva.

Passaggio 1: verifica le tue autorizzazioni

Prima di designare l'account amministratore delegato Macie per la tua organizzazione, verifica che tu (come utente dell'account di AWS Organizations gestione) sia autorizzato a eseguire la seguente azione Macie: `macie2:EnableOrganizationAdminAccount`. Questa azione consente di designare l'account amministratore Macie delegato per l'organizzazione utilizzando Macie.

Verifica inoltre di avere il permesso di eseguire le seguenti azioni: AWS Organizations

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

Queste azioni ti consentono di: recuperare informazioni sulla tua organizzazione, integrare Macie con AWS Organizations, recuperare le informazioni con AWS Organizations cui Servizi AWS hai effettuato l'integrazione e designare un account amministratore Macie delegato per la tua organizzazione.

Per concedere queste autorizzazioni, includi la seguente dichiarazione in una policy AWS Identity and Access Management (IAM) per il tuo account:

```
{
  "Sid": "Grant permissions to designate a delegated Macie administrator",
  "Effect": "Allow",
  "Action": [
    "macie2:EnableOrganizationAdminAccount",
    "organizations:DescribeOrganization",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListAWSServiceAccessForOrganization",
```

```

    "organizations:RegisterDelegatedAdministrator"
  ],
  "Resource": "*"
}

```

Se desideri designare il tuo account di AWS Organizations gestione come account amministratore Macie delegato per l'organizzazione, il tuo account necessita anche dell'autorizzazione per eseguire la seguente azione IAM: `CreateServiceLinkedRole`. Questa azione ti consente di abilitare Macie per l'account di gestione. Tuttavia, in base alle migliori pratiche di AWS sicurezza e al principio del privilegio minimo, non è consigliabile eseguire questa operazione.

Se decidi di concedere questa autorizzazione, aggiungi la seguente dichiarazione alla politica IAM per il tuo account di AWS Organizations gestione:

```

{
  "Sid": "Grant permissions to enable Macie",
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/maciek.amazonaws.com/AWSServiceRoleForAmazonMacie",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "maciek.amazonaws.com"
    }
  }
}

```

Nell'estratto conto, sostituiscilo **111122223333** con l'ID dell'account di gestione.

Se desideri amministrare Macie in modalità opt-in Regione AWS (regione disabilitata per impostazione predefinita), aggiorna anche il valore per il principale del servizio Macie nell'Resource elemento e nella condizione. `iam:AWSServiceName` Il valore deve specificare il codice regionale per la regione. Ad esempio, per amministrare Macie nella regione del Medio Oriente (Bahrein), che ha il codice regionale `me-south-1`, procedi come segue:

- Nell'elemento, sostituisci Resource

```

arn:aws:iam::111122223333:role/aws-service-role/maciek.amazonaws.com/
AWSServiceRoleForAmazonMacie

```

con

```
arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie
```

Dove **111122223333** specifica l'ID dell'account di gestione e **me-south-1** specifica il codice regionale per la regione.

- Nella `iam:AWSServiceName` condizione, sostituisci `macie.amazonaws.com` con `macie.me-south-1.amazonaws.com`, dove **me-south-1** specifica il codice regionale per la regione.

Per un elenco delle regioni in cui Macie è attualmente disponibile e il codice regionale per ciascuna di esse, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS Per determinare se una regione è una regione a cui aderire, consulta [Attiva o disattiva Regioni AWS nel tuo account nella Guida](#) per l'utente. Gestione dell'account AWS

Passaggio 2: designare l'account amministratore Macie delegato per l'organizzazione

Dopo aver verificato le autorizzazioni, tu (come utente dell'account di AWS Organizations gestione) puoi designare l'account amministratore Macie delegato per la tua organizzazione.

Per designare l'account amministratore Macie delegato per un'organizzazione

Per designare l'account amministratore delegato Macie per la tua organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Solo un utente dell'account di AWS Organizations gestione può eseguire questa operazione.

Console

Segui questi passaggi per designare l'account amministratore delegato di Macie utilizzando la console Amazon Macie.

Per designare l'account amministratore delegato di Macie

1. Accedi all'account di gestione AWS Management Console utilizzando il tuo AWS Organizations account di gestione.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri designare l'account amministratore Macie delegato per la tua organizzazione.

3. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
4. Esegui una delle seguenti operazioni, a seconda che Macie sia abilitato per il tuo account di gestione nella regione corrente:
 - Se Macie non è abilitato, scegli Inizia nella pagina di benvenuto.
 - Se Macie è abilitato, scegli Impostazioni nel pannello di navigazione.
5. In Amministratore delegato, inserisci l'ID dell'account a 12 cifre per l'account Account AWS che desideri designare come account amministratore Macie.
6. Scegli Delega.

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui desideri integrare la tua organizzazione con Macie. È necessario designare lo stesso account amministratore Macie in ciascuna di queste regioni.

API

Per designare l'account amministratore Macie delegato a livello di codice, utilizza il funzionamento [EnableOrganizationAdminAccount](#) dell'API Amazon Macie. Per designare l'account in più regioni, invia la designazione per ogni regione in cui desideri integrare la tua organizzazione con Macie. È necessario designare lo stesso account amministratore Macie in ciascuna di queste regioni.

Quando invii la designazione, utilizza il `adminAccountId` parametro richiesto per specificare l'ID dell'account a 12 cifre da Account AWS designare come account amministratore Macie per l'organizzazione. Assicurati inoltre di specificare la regione a cui si riferisce la designazione.

Per designare l'account amministratore di Macie utilizzando [AWS Command Line Interface \(AWS CLI\)](#), esegui il comando. [enable-organization-admin-account](#) Per il `admin-account-id` parametro, specificate l'ID dell'account a 12 cifre da designare. Account AWS Utilizzate il `region` parametro per specificare la regione a cui si applica la designazione. Per esempio:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 111122223333
```

us-east-1 Dov'è la regione a cui si applica la designazione (la regione Stati Uniti orientali (Virginia settentrionale)) e **111122223333** l'ID dell'account da designare.

Dopo aver designato l'account amministratore Macie per l'organizzazione, l'amministratore Macie può iniziare a configurare l'organizzazione in Macie.

Passaggio 3: Abilita e aggiungi automaticamente nuovi account dell'organizzazione come account membri di Macie

Per impostazione predefinita, Macie non è abilitato automaticamente per i nuovi account quando gli account vengono aggiunti all'organizzazione in AWS Organizations. Inoltre, gli account non vengono aggiunti automaticamente come account membri di Macie. Gli account vengono visualizzati nell'inventario degli account dell'amministratore di Macie. Tuttavia, Macie non è necessariamente abilitato per gli account e l'amministratore Macie non può necessariamente accedere alle impostazioni, ai dati e alle risorse di Macie per gli account.

Se sei l'amministratore delegato di Macie dell'organizzazione, puoi modificare questa impostazione di configurazione. Puoi attivare l'abilitazione automatica per la tua organizzazione. Se lo fai, Macie viene abilitato automaticamente per i nuovi account quando gli account vengono aggiunti alla tua organizzazione in AWS Organizations. Inoltre, gli account vengono associati automaticamente all'account amministratore Macie come account membro. L'attivazione di questa impostazione non influisce sugli account esistenti nell'organizzazione. Per abilitare e gestire Macie per gli account esistenti, devi aggiungere manualmente gli account come account membro Macie. Il [passaggio successivo](#) spiega come eseguire questa operazione.

Note

Se attivi l'attivazione automatica, tieni presente la seguente eccezione. Se un nuovo account è già associato a un altro account amministratore Macie, Macie non aggiunge automaticamente l'account come account membro dell'organizzazione. L'account deve dissociarsi dall'account amministratore Macie corrente prima di poter far parte dell'organizzazione in Macie. È quindi possibile aggiungere manualmente l'account. Per identificare gli account in cui ciò si verifica, puoi [esaminare l'inventario degli account della](#) tua organizzazione.

Per abilitare e aggiungere automaticamente nuovi account dell'organizzazione come account membri di Macie

Per abilitare e aggiungere automaticamente nuovi account come account membro Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Solo l'amministratore Macie delegato dell'organizzazione può eseguire questa operazione.

Console

Per eseguire questa operazione utilizzando la console, è necessario disporre del permesso di eseguire la seguente AWS Organizations azione: `organizations:ListAccounts`. Questa azione consente di recuperare e visualizzare informazioni sugli account della propria organizzazione. Se disponi di queste autorizzazioni, segui questi passaggi per abilitare e aggiungere automaticamente nuovi account dell'organizzazione come account membro di Macie.

Per abilitare e aggiungere automaticamente nuovi account dell'organizzazione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri abilitare e aggiungere automaticamente nuovi account come account membro di Macie.
3. Dal riquadro di navigazione, selezionare Accounts (Account).
4. Nella pagina Account, nella sezione Nuovi account, scegli Modifica.
5. Nella finestra di dialogo Modifica le impostazioni per i nuovi account, seleziona Abilita Macie.

Per abilitare anche l'individuazione automatica dei dati sensibili per gli account dei nuovi membri, seleziona Abilita il rilevamento automatico dei dati sensibili. Se abiliti questa funzionalità per un account, Macie seleziona continuamente oggetti campione dai bucket S3 dell'account e li analizza per determinare se contengono dati sensibili. Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#).

6. Seleziona Save (Salva).

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui desideri configurare la tua organizzazione in Macie.

Per modificare successivamente queste impostazioni, ripeti i passaggi precedenti e deselecta la casella di controllo per ciascuna impostazione.

API

Per abilitare e aggiungere automaticamente nuovi account utente Macie a livello di codice, utilizza il [UpdateOrganizationConfiguration](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, imposta il valore del parametro su `autoEnable true` Il valore predefinito è `false`. Assicurati inoltre di specificare la regione a cui si riferisce la richiesta. Per abilitare e aggiungere automaticamente nuovi account in altre regioni, invia la richiesta per ogni regione aggiuntiva.

Se utilizzi il AWS CLI per inviare la richiesta, esegui il [update-organization-configuration](#) comando e specifica il `auto-enable` parametro per abilitare e aggiungere nuovi account automaticamente. Per esempio:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

us-east-1 Dov'è la regione in cui abilitare e aggiungere automaticamente nuovi account, la regione Stati Uniti orientali (Virginia settentrionale).

Per modificare successivamente questa impostazione e interrompere l'attivazione e l'aggiunta automatica di nuovi account, esegui nuovamente lo stesso comando e utilizza il `no-auto-enable` parametro, anziché il `auto-enable` parametro, in ciascuna regione applicabile.

È inoltre possibile abilitare automaticamente l'individuazione automatica dei dati sensibili per gli account dei nuovi membri. Se abiliti questa funzionalità per un account, Macie seleziona continuamente oggetti campione dai bucket S3 dell'account e li analizza per determinare se contengono dati sensibili. Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#). Per abilitare automaticamente questa funzionalità per gli account dei membri, utilizza l'[UpdateAutomatedDiscoveryConfiguration](#) operazione o, se utilizzi il, esegui il comando. AWS CLI [update-automated-discovery-configuration](#)

Passaggio 4: abilitare e aggiungere gli account aziendali esistenti come account membri di Macie

Quando integri Macie con AWS Organizations, Macie non viene abilitato automaticamente per tutti gli account esistenti nell'organizzazione. Inoltre, gli account non vengono associati automaticamente all'account amministratore delegato di Macie come account membri di Macie. Pertanto, il passaggio finale dell'integrazione e della configurazione dell'organizzazione in Macie consiste nell'aggiungere gli account dell'organizzazione esistenti come account membri di Macie. Quando aggiungi un account esistente come account membro Macie, Macie viene automaticamente abilitato per l'account e tu (in qualità di amministratore delegato di Macie) hai accesso a determinate impostazioni, dati e risorse di Macie per l'account.

Tieni presente che non puoi aggiungere un account attualmente associato a un altro account amministratore Macie. Per aggiungere l'account, contatta il proprietario dell'account per dissociare prima l'account dall'account amministratore corrente. Inoltre, non puoi aggiungere un account esistente se Macie è attualmente sospeso per l'account. Il proprietario dell'account deve prima

riattivare Macie per l'account. Infine, se desideri aggiungere l'account di AWS Organizations gestione come account membro, un utente di quell'account deve prima abilitare Macie per l'account.

Per abilitare e aggiungere account aziendali esistenti come account membri di Macie

Per abilitare e aggiungere account aziendali esistenti come account membri di Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Solo l'amministratore Macie delegato dell'organizzazione può eseguire questa operazione.

Console

Per eseguire questa operazione utilizzando la console, è necessario disporre del permesso di eseguire la seguente AWS Organizations azione: `organizations:ListAccounts`. Questa azione consente di recuperare e visualizzare informazioni sugli account della propria organizzazione. Se disponi di queste autorizzazioni, segui questi passaggi per abilitare e aggiungere account esistenti come account membri di Macie.

Per abilitare e aggiungere account aziendali esistenti

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri abilitare e aggiungi gli account esistenti come account membri di Macie.
3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account associati al tuo account Macie.

Se un account fa parte della tua organizzazione in AWS Organizations, il tipo è Via AWS Organizations. Se un account è già membro di Macie, il suo stato è Attivato o In pausa (sospeso).

4. Nella tabella Account esistenti, seleziona la casella di controllo per ogni account che desideri aggiungere come account membro Macie.
5. Nel menu Azioni, scegli Aggiungi membro.
6. Conferma di voler aggiungere gli account selezionati come account membro.

Dopo aver confermato l'aggiunta degli account selezionati, lo stato degli account cambia in Attivazione in corso e quindi Attivato. Dopo aver aggiunto un account membro, puoi anche abilitare l'individuazione automatica dei dati sensibili per l'account: nella tabella Account esistenti, seleziona la casella di controllo relativa a ciascun account per cui abilitarlo, quindi scegli Abilita

il rilevamento automatico dei dati sensibili nel menu Azioni. Se abiliti questa funzionalità per un account, Macie seleziona continuamente oggetti campione dai bucket S3 dell'account e li analizza per determinare se contengono dati sensibili. Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#).

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui desideri configurare la tua organizzazione in Macie.

API

Per abilitare e aggiungere a livello di codice uno o più account esistenti come account membri di Macie, utilizza il [CreateMember](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza i parametri supportati per specificare l'ID dell'account a 12 cifre e l'indirizzo e-mail di ciascuno da abilitare e aggiungere. Account AWS Specificate anche la regione a cui si riferisce la richiesta. Per abilitare e aggiungere account esistenti in altre regioni, invia la richiesta per ogni regione aggiuntiva.

Per recuperare l'ID account e l'indirizzo e-mail di un account Account AWS da abilitare e aggiungere, puoi opzionalmente utilizzare il [ListMembers](#) funzionamento dell'API Amazon Macie. Questa operazione fornisce dettagli sugli account associati al tuo account Macie, inclusi gli account che non sono account membri di Macie. Se il valore della `relationshipStatus` proprietà di un account non è `Enabled` o `Paused` l'account non è un account membro Macie.

Per abilitare e aggiungere uno o più account esistenti utilizzando AWS CLI, esegui il comando [create-member](#). Utilizzate il `region` parametro per specificare la regione in cui abilitare e aggiungere gli account. Utilizzate i `account` parametri per specificare l'ID dell'account e l'indirizzo e-mail per ciascuno Account AWS di essi da aggiungere. Per esempio:

```
C:\> aws macie2 create-member --region us-east-1 --account="{\"accountId\":  
\"123456789012\",\"email\": \"janedoe@example.com\"}"
```

us-east-1 Dov'è la regione in cui abilitare e aggiungere l'account come account membro Macie (regione Stati Uniti orientali (Virginia settentrionale)) e `account` i parametri specificano l'ID dell'account (**123456789012**) e l'indirizzo e-mail (**janedoe@example.com**) per l'account.

Se la richiesta ha esito positivo, lo stato (`relationshipStatus`) dell'account specificato diventa `Enabled` nell'inventario dell'account.

Per abilitare anche l'individuazione automatica dei dati sensibili per uno o più account, utilizza il [BatchUpdateAutomatedDiscoveryAccounts](#) operazione o, se utilizzi il AWS CLI, esegui il

comando [batch-update-automated-discovery-accounts](#). Se abiliti questa funzionalità per un account, Macie seleziona continuamente oggetti di esempio dai bucket S3 dell'account e analizza gli oggetti per determinare se contengono dati sensibili. Per ulteriori informazioni, consulta [Esecuzione del rilevamento automatico di dati sensibili](#).

Revisione degli account Macie per un'organizzazione

Dopo l'[integrazione e la configurazione](#) di un' AWS Organizations organizzazione in Amazon Macie, l'amministratore Macie delegato può accedere a un inventario degli account dell'organizzazione in Macie. In qualità di amministratore Macie di un'organizzazione, puoi utilizzare questo inventario per esaminare le statistiche e i dettagli degli account Macie della tua organizzazione in un. Regione AWS Puoi anche usarlo per [eseguire determinate attività di gestione degli](#) account.

Per esaminare gli account Macie di un'organizzazione

Per esaminare gli account della tua organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Se preferisci utilizzare la console, devi avere il permesso di eseguire la seguente AWS Organizations azione: `organizations:ListAccounts` Questa azione ti consente di recuperare e visualizzare informazioni sugli account che fanno parte della tua organizzazione. AWS Organizations

Console

Segui questi passaggi per esaminare gli account Macie della tua organizzazione utilizzando la console Amazon Macie.

Per esaminare gli account della tua organizzazione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri esaminare gli account della tua organizzazione.
3. Dal riquadro di navigazione, selezionare Accounts (Account).

La pagina Account si apre e mostra statistiche aggregate e una tabella degli account associati al tuo account Macie nell'attuale. Regione AWS

Nella parte superiore della pagina Account, troverai le seguenti statistiche aggregate.

Tramite AWS Organizations

Active riporta il numero totale di account associati all'account tramite gli account Macie dell'organizzazione AWS Organizations e che sono attualmente membri di Macie. Macie è abilitato per questi account e tu sei l'amministratore Macie degli account.

Tutto riporta il numero totale di account associati al tuo account tramite AWS Organizations. Ciò include gli account che attualmente non sono account membri di Macie. Include anche gli account dei membri per i quali Macie è attualmente sospeso.

Su invito

Active riporta il numero totale di account associati all'account su invito di Macie e che attualmente sono account membri Macie dell'organizzazione. Questi account non sono associati al tuo account tramite AWS Organizations. Macie è abilitato per gli account e tu sei l'amministratore degli account Macie perché hanno accettato un tuo invito a iscriversi a Macie.

Tutto riporta il numero totale di account associati al tuo account su invito di Macie, inclusi gli account che non hanno risposto a un tuo invito.

Attivi/Tutti

Active riporta il numero totale di account per i quali Macie è attualmente abilitato nell'organizzazione, incluso il proprio account. Sei l'amministratore Macie di questi account tramite AWS Organizations o su invito di Macie.

Tutto riporta il numero totale di account associati al tuo account, tramite AWS Organizations o tramite invito di Macie, più il tuo account. Ciò include gli account che fanno parte della tua organizzazione AWS Organizations e che attualmente non sono account membri di Macie. Sono inclusi anche tutti gli account che non hanno risposto a un tuo invito di iscrizione a Macie.

Nella tabella, troverai i dettagli su ciascun account nella regione corrente. La tabella include tutti gli account associati al tuo account Macie tramite AWS Organizations o tramite invito di Macie.

ID account

L'ID dell'account e l'indirizzo e-mail per Account AWS

Nome

Il nome dell'account per Account AWS. Questo valore è generalmente N/A per il tuo account e per tutti gli account associati al tuo account su invito di Macie.

Tipo

In che modo l'account è associato al tuo account, tramite AWS Organizations o tramite invito di Macie. Per il tuo account, questo valore è Conto corrente.

Stato

Lo stato della relazione tra il tuo account e l'account. Per un account in un' AWS Organizations organizzazione (Type is Via AWS Organizations), i valori possibili sono:

- Account sospeso: Account AWS è sospeso.
- Abilitato: l'account è un account membro di Macie. Macie è abilitato per l'account e tu sei l'amministratore Macie dell'account.
- Attivazione in corso: Macie sta elaborando una richiesta per abilitare e aggiungere l'account come account membro Macie.
- Non sei un membro: l'account fa parte della tua organizzazione AWS Organizations ma non è un account membro Macie.
- In pausa (sospeso): l'account è un account associato a Macie, ma Macie è attualmente sospeso per l'account.
- Regione disattivata: l'account fa parte della tua organizzazione, AWS Organizations ma la regione corrente è disabilitata per. Account AWS
- Rimosso (dissociato): l'account era precedentemente un account membro di Macie, ma è stato successivamente rimosso come account membro. Hai dissociato l'account dall'account amministratore di Macie. Macie continua a essere abilitato per l'account.

Ultimo aggiornamento dello stato

L'ultima volta che tu o l'account associato avete eseguito un'azione che ha influito sulla relazione tra i vostri account.

Rilevamento automatico di dati sensibili

Se il rilevamento automatico dei dati sensibili è attualmente abilitato o disabilitato per l'account.

Per ordinare la tabella in base a un campo specifico, scegli l'intestazione di colonna del campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna. Per filtrare la tabella, posiziona il cursore nella casella del filtro, quindi aggiungi una condizione di filtro per un campo. Per perfezionare ulteriormente i risultati, aggiungi condizioni di filtro per campi aggiuntivi.

API

Per esaminare gli account della tua organizzazione a livello di codice, utilizza il [ListMembers](#) funzionamento dell'API Amazon Macie e specifica la regione a cui si riferisce la richiesta. Per esaminare gli account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Quando invii la richiesta, utilizza il `onlyAssociated` parametro per specificare quali account includere nella risposta. Per impostazione predefinita, Macie restituisce i dettagli solo sugli account che sono account membri Macie nella regione specificata tramite AWS Organizations o su invito di Macie. Per recuperare questi dettagli per tutti gli account associati al tuo account Macie, inclusi gli account che non sono account membri, includi il `onlyAssociated` parametro nella richiesta e imposta il valore del parametro su `false`.

Per esaminare gli account della tua organizzazione utilizzando il comando [AWS Command Line Interface \(AWS CLI\)](#), esegui il comando [list-members](#). Per il `only-associated` parametro, specifica se includere tutti gli account associati o solo gli account dei membri di Macie. Per includere solo gli account dei membri, ometti questo parametro o imposta il valore del parametro su `true`. Per includere tutti gli account, imposta questo valore su `false`. Per esempio:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

us-east-1 Dov'è la regione a cui si riferisce la richiesta, la regione Stati Uniti orientali (Virginia settentrionale).

Se la richiesta ha esito positivo, Macie restituisce un array `members`. L'array contiene un `member` oggetto per ogni account che soddisfa i criteri specificati nella richiesta. In quell'oggetto, il `relationshipStatus` campo indica lo stato attuale della relazione tra il tuo account e l'altro account nella regione specificata. Per un account in un'AWS Organizations organizzazione, i valori possibili sono:

- **AccountSuspended**— Account AWS È sospeso.
- **Created**— Macie sta elaborando una richiesta per abilitare e aggiungere l'account come account membro Macie.
- **Enabled**— L'account è un account membro Macie. Macie è abilitato per l'account e tu sei l'amministratore Macie dell'account.
- **Paused**— L'account è un account associato a Macie, ma Macie è attualmente sospeso (in pausa) per l'account.

- **RegionDisabled**— L'account fa parte della tua organizzazione, AWS Organizations ma la regione corrente è disabilitata per. Account AWS
- **Removed**— L'account era precedentemente un account membro Macie, ma è stato successivamente rimosso come account membro. Hai dissociato l'account dall'account amministratore di Macie. Macie continua a essere abilitato per l'account.

Per informazioni sugli altri campi dell'oggetto, consulta [Members](#) in the Amazon Macie API Reference.

Gestione degli account dei membri Macie per un'organizzazione

Dopo l'[integrazione e la configurazione](#) di un' AWS Organizations organizzazione in Amazon Macie, l'amministratore Macie delegato dell'organizzazione può accedere a determinate impostazioni, dati e risorse di Macie per gli account dei membri. In qualità di amministratore Macie di un'organizzazione, puoi utilizzare Macie per eseguire centralmente determinate attività di gestione e amministrazione degli account. Ad esempio, puoi:

- Aggiungi e rimuovi account come account dei membri di Macie.
- Gestisci lo stato di Macie per i singoli account, ad esempio abilita o sospendi Macie per un account.
- Monitora le quote di Macie e i costi di utilizzo stimati per i singoli account e per l'intera organizzazione.

Puoi anche consultare i dati di inventario di Amazon Simple Storage Service (Amazon S3) e i risultati delle policy per gli account dei membri Macie. Inoltre, puoi scoprire dati sensibili nei bucket S3 di proprietà degli account. Per un elenco dettagliato delle attività che puoi eseguire, consulta [Relazioni tra amministratore e account membro di Macie](#)

Per impostazione predefinita, Macie ti offre la visibilità dei dati e delle risorse pertinenti per tutti gli account membri Macie della tua organizzazione. Puoi anche approfondire i dati e le risorse per i singoli account. Ad esempio, se [utilizzi la dashboard Summary](#) per valutare il livello di sicurezza di Amazon S3 della tua organizzazione, puoi filtrare i dati per account. Allo stesso modo, se [monitorate i costi di utilizzo stimati](#), potete accedere alle suddivisioni dei costi stimati per i singoli account membri.

Oltre alle attività comuni agli account amministratore e membro, è possibile eseguire diverse attività amministrative per l'organizzazione.

Attività

- [Aggiungere gli account dei membri di Macie a un'organizzazione](#)
- [Sospensione di Macie per gli account dei membri di un'organizzazione](#)
- [Rimuovere gli account dei membri di Macie da un'organizzazione](#)

In qualità di amministratore Macie di un'organizzazione, puoi eseguire queste attività utilizzando la console Amazon Macie o l'API Amazon Macie. Se preferisci utilizzare la console, devi avere il permesso di eseguire le seguenti AWS Organizations azioni: `organizations:ListAccounts`. Questa azione ti consente di recuperare e visualizzare informazioni sugli account che fanno parte della tua organizzazione. AWS Organizations

Aggiungere gli account dei membri di Macie a un'organizzazione

In alcuni casi, potrebbe essere necessario aggiungere manualmente un account come account membro di Amazon Macie. Questo è il caso degli account che in precedenza hai rimosso (dissociati) come account membri. Questo vale anche se non hai configurato Macie per [abilitare e aggiungere automaticamente nuovi account membro quando gli account](#) vengono aggiunti alla tua organizzazione in. AWS Organizations

Quando aggiungi un account come account membro Macie:

- Macie è abilitato per l'account corrente Regione AWS, se non è già abilitato nella regione.
- L'account è associato al tuo account amministratore Macie come account membro nella regione. L'account membro non riceve un invito o altra notifica che indica che hai stabilito questa relazione tra i tuoi account.
- Il rilevamento automatico dei dati sensibili potrebbe essere abilitato per l'account nella regione. Ciò dipende dalle impostazioni di configurazione specificate per l'organizzazione. Per ulteriori informazioni, consulta [Configurazione del rilevamento automatico dei dati sensibili](#).

Tieni presente che non puoi aggiungere un account già associato a un altro account amministratore di Macie. L'account deve prima dissociarsi dal suo account amministratore corrente. Inoltre, non puoi aggiungere l'account di AWS Organizations gestione come account membro a meno che Macie non sia già abilitato per l'account. Per ulteriori informazioni sui requisiti aggiuntivi, consulta [Considerazioni sull'utilizzo di Macie con AWS Organizations](#).

Per aggiungere un account membro Macie a un'organizzazione

Per aggiungere uno o più account membri Macie alla tua organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per aggiungere uno o più account membri Macie utilizzando la console Amazon Macie.

Per aggiungere un account membro Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri aggiungere un account membro.
3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account associati al tuo account.
4. (Facoltativo) Per identificare più facilmente gli account che fanno parte della tua organizzazione AWS Organizations e non sono account membri di Macie, usa la casella di filtro sopra la tabella Account esistenti per aggiungere le seguenti condizioni di filtro:
 - Tipo = Organizzazione
 - Status = Non sei un membro

Per visualizzare anche gli account che hai rimosso in precedenza e che potresti voler aggiungere come account membri, aggiungi anche la condizione di filtro Status = Removed.

5. Nella tabella Account esistenti, seleziona la casella di controllo per ogni account che desideri aggiungere come account membro.
6. Nel menu Azioni, scegli Aggiungi membro.
7. Conferma di voler aggiungere gli account selezionati come account membro.

Dopo aver confermato le selezioni, lo stato degli account selezionati cambia in Attivazione in corso e quindi Attivato nell'inventario degli account.

Per aggiungere un account membro in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Per aggiungere uno o più account membri Macie a livello di codice, utilizza il [CreateMember](#) funzionamento dell'API Amazon Macie.

Quando invii la richiesta, utilizza i parametri supportati per specificare l'ID dell'account a 12 cifre e l'indirizzo e-mail per ciascuno Account AWS di essi che desideri aggiungere. Specificate anche la regione a cui si riferisce la richiesta. Per aggiungere un account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per recuperare l'ID account e l'indirizzo e-mail di un account da aggiungere, puoi correlare l'output del [ListAccounts](#) funzionamento dell' AWS Organizations API e il [ListMembers](#) funzionamento dell'API Amazon Macie. Per il ListMembers funzionamento dell'API Macie, includi il `onlyAssociated` parametro nella richiesta e imposta il valore del parametro su `false`. Se l'operazione ha esito positivo, Macie restituisce un `members` array che fornisce dettagli su tutti gli account associati all'account amministratore Macie nella regione specificata, inclusi gli account che attualmente non sono account membri. Notate quanto segue nell'array:

- Se il valore della `relationshipStatus` proprietà di un account non è `Enabled` o `Paused`, l'account è associato al tuo account ma non è un account membro Macie.
- Se un account non è incluso nell'array ma è incluso nell'output del ListAccounts funzionamento dell' AWS Organizations API, l'account fa parte della tua organizzazione AWS Organizations ma non è associato al tuo account e, pertanto, non è un account membro di Macie.

Per aggiungere un account membro utilizzando AWS Command Line Interface (AWS CLI), esegui il comando [create-member](#). Utilizzate il `region` parametro per specificare la regione in cui aggiungere l'account. Utilizzate i `account` parametri per specificare l'ID e l'indirizzo e-mail dell'account per ogni account da aggiungere. Per esempio:

```
C:\> aws macie2 create-member --region us-east-1 --account="{\"accountId\":  
\"123456789012\",\"email\": \"janedoe@example.com\"}"
```

us-east-1 Dov'è la regione in cui aggiungere l'account come account membro (la regione Stati Uniti orientali (Virginia settentrionale)) e `account` i parametri specificano l'ID dell'account (**123456789012**) e l'indirizzo e-mail (**janedoe@example.com**) per l'account.

Se la richiesta ha esito positivo, lo stato (`relationshipStatus`) dell'account specificato diventa `Enabled` nell'inventario dell'account.

Sospensione di Macie per gli account dei membri di un'organizzazione

In qualità di amministratore di Amazon Macie per un'organizzazione in AWS Organizations, puoi sospendere Macie per un account membro della tua organizzazione. Se lo fai, puoi anche riattivare Macie per l'account in un secondo momento.

Quando sospendi Macie per un account utente:

- Attualmente Macie perde l'accesso e smette di fornire i metadati relativi ai dati Amazon S3 dell'account. Regione AWS
- Macie interrompe l'esecuzione di tutte le attività relative all'account nella regione. Ciò include il monitoraggio dei bucket S3 per la sicurezza e il controllo degli accessi, l'esecuzione del rilevamento automatico di dati sensibili e l'esecuzione di processi di rilevamento di dati sensibili attualmente in corso.
- Macie annulla tutti i processi di rilevamento di dati sensibili creati dall'account nella regione. Un lavoro non può essere ripreso o riavviato dopo essere stato annullato. Se hai creato offerte di lavoro per analizzare i dati di proprietà dell'account utente, Macie non annulla le tue offerte di lavoro. Invece, le offerte di lavoro ignorano le risorse di proprietà dell'account.

Mentre è sospeso, Macie conserva l'identificatore di sessione, le impostazioni e le risorse che archivia o gestisce per l'account nella regione applicabile. Macie conserva anche determinati dati dell'account nella Regione. Ad esempio, i risultati dell'account rimangono intatti e non vengono modificati per un massimo di 90 giorni. Se l'individuazione automatica dei dati sensibili è stata abilitata per l'account, anche i risultati esistenti rimangono intatti e non vengono modificati per un massimo di 30 giorni. La tua organizzazione non addebita addebiti Macie per l'account in quella regione mentre Macie è sospeso per l'account in quella regione.

Per sospendere Macie per un account membro di un'organizzazione

Per sospendere Macie per un account membro di un'organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per sospendere Macie per un account membro utilizzando la console Amazon Macie.

Per sospendere Macie per un account utente

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri sospendere Macie per un account membro.
3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account associati al tuo account.
4. Nella tabella Account esistenti, seleziona la casella di controllo relativa all'account per cui sospendere Macie.
5. Nel menu Azioni, scegli Sospendi Macie.
6. Conferma di voler sospendere Macie per l'account.

Dopo aver confermato la sospensione, lo stato dell'account cambia in Sospeso (sospeso) nell'inventario dell'account. Per sospendere Macie per l'account in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Per riattivare successivamente Macie per l'account, torna alla pagina Account sulla console. Seleziona la casella di controllo relativa all'account, quindi scegli Abilita Macie nel menu Azioni. Per riattivare Macie per l'account in altre regioni, ripeti questi passaggi in ogni regione aggiuntiva.

API

Per sospendere Macie for a member account a livello di codice, utilizza il [UpdateMemberSession](#) funzionamento dell'API Amazon Macie. Puoi utilizzare questa operazione anche per riattivare successivamente Macie per l'account.

Quando invii la richiesta, usa il `id` parametro per specificare l'ID dell'account a 12 cifre per Account AWS cui desideri sospendere Macie. Per il parametro `status`, specifica `PAUSED`. Specificate anche la regione a cui si riferisce la richiesta. Per sospendere Macie per l'account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per recuperare l'ID dell'account, puoi utilizzare il [ListMembers](#) funzionamento dell'API Amazon Macie. In tal caso, valuta la possibilità di filtrare i risultati includendo il `onlyAssociated` parametro nella richiesta. Se imposti il valore di questo parametro su `true`, Macie restituisce un `members` array che fornisce dettagli solo sugli account che sono attualmente account membri.

Per sospendere Macie per un account membro utilizzando il AWS CLI, esegui il comando. [update-member-session](#) Utilizzate il `region` parametro per specificare la regione in cui sospendere

Macie per l'account. Utilizzate il `id` parametro per specificare l'ID dell'account. Per il parametro `status`, specifica `PAUSED`. Per esempio:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status  
PAUSED
```

us-east-1 Dov'è la regione in cui sospendere Macie (regione Stati Uniti orientali (Virginia settentrionale)), **123456789012** è l'ID dell'account per cui sospendere Macie e `PAUSED` il nuovo stato di Macie per l'account.

Se la richiesta ha esito positivo, Macie restituisce una risposta vuota e lo stato dell'account specificato viene modificato nell'inventario dell'account. `Paused` Per riattivare successivamente Macie per l'account, esegui nuovamente il `update-member-session` comando e specifica `ENABLED` il parametro. `status`

Rimuovere gli account dei membri di Macie da un'organizzazione

Se desideri interrompere l'accesso alle impostazioni, ai dati e alle risorse di Amazon Macie per un account membro, puoi rimuovere l'account come account membro Macie. Puoi farlo dissociando l'account dal tuo account amministratore di Macie. Tieni presente che solo tu puoi farlo per un account membro. Un account AWS Organizations membro non può dissociarsi dal suo account amministratore Macie.

Quando rimuovi un account membro Macie, Macie rimane abilitato per l'account corrente. Regione AWS Tuttavia, l'account viene dissociato dall'account amministratore Macie e diventa un account Macie autonomo. Ciò significa che perderai l'accesso a tutte le impostazioni, i dati e le risorse di Macie per l'account, inclusi i metadati e i risultati delle policy per i dati Amazon S3 dell'account. Ciò significa anche che non puoi più usare Macie per scoprire dati sensibili nei bucket S3 di proprietà dell'account. Se hai già creato processi di rilevamento di dati sensibili a tale scopo, i lavori ignorano i bucket di proprietà dell'account. Se hai abilitato il rilevamento automatico dei dati sensibili per l'account, sia tu che l'account membro perderete l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni che Macie ha prodotto e fornito direttamente durante l'individuazione automatica dell'account.

Dopo aver rimosso un account membro Macie, l'account continua a comparire nell'inventario del tuo account. Macie non notifica al proprietario dell'account che hai rimosso l'account. Pertanto, valuta la possibilità di contattare il proprietario dell'account per assicurarti che inizi a gestire le impostazioni e le risorse del suo account.

Puoi aggiungere nuovamente l'account alla tua organizzazione in un secondo momento. Se esegui questa operazione e abiliti nuovamente l'individuazione automatica dei dati sensibili per l'account entro 30 giorni, potrai inoltre riaccedere ai dati e alle informazioni che Macie aveva precedentemente prodotto e fornito direttamente durante l'individuazione automatica dell'account. Inoltre, le esecuzioni successive dei job esistenti ricominciano a includere i bucket S3 dell'account.

Per rimuovere un account membro Macie da un'organizzazione

Per rimuovere un account membro Macie dalla tua organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per rimuovere un account membro Macie utilizzando la console Amazon Macie.

Per rimuovere un account membro Macie

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri rimuovere un account membro.
3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account associati al tuo account.
4. Nella tabella Account esistenti, seleziona la casella di controllo relativa all'account che desideri rimuovere come account membro.
5. Nel menu Azioni, scegli Dissocia account.
6. Conferma di voler rimuovere l'account selezionato come account membro.

Dopo aver confermato la selezione, lo stato dell'account cambia in Rimosso (dissociato) nell'inventario dell'account.

Per rimuovere l'account membro in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Per rimuovere un account membro Macie a livello di codice, utilizza il [DisassociateMember](#) funzionamento dell'API Amazon Macie.

Quando invii la richiesta, utilizza il `id` parametro per specificare l' Account AWS ID a 12 cifre dell'account membro da rimuovere. Specificate anche la regione a cui si riferisce la richiesta. Per rimuovere l'account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per recuperare l'ID dell'account membro da rimuovere, puoi utilizzare il [ListMembers](#) funzionamento dell'API Amazon Macie. In tal caso, valuta la possibilità di filtrare i risultati includendo il `onlyAssociated` parametro nella richiesta. Se imposti il valore di questo parametro su `true`, Macie restituisce un `members` array che fornisce dettagli solo sugli account che attualmente sono account membri di Macie.

[Per rimuovere un account membro Macie utilizzando AWS CLI, esegui il comando `disassociate-member`](#). Utilizzate il `region` parametro per specificare la regione in cui rimuovere l'account. Utilizza il `id` parametro per specificare l'ID dell'account membro da rimuovere. Per esempio:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

us-east-1 Dov'è la regione in cui rimuovere l'account (la regione Stati Uniti orientali (Virginia settentrionale)) e **123456789012** l'ID dell'account da rimuovere.

Se la richiesta ha esito positivo, Macie restituisce una risposta vuota e lo stato dell'account specificato viene modificato `Removed` nell'inventario dell'account.

Modifica dell'account amministratore Macie per un'organizzazione

Dopo l'[integrazione e la configurazione](#) di un' AWS Organizations organizzazione in Amazon Macie, l'account di AWS Organizations gestione può designare un account diverso come account amministratore Macie delegato per l'organizzazione. Il nuovo amministratore Macie può quindi configurare nuovamente l'organizzazione in Macie.

Come utente dell'account di AWS Organizations gestione di un'organizzazione, verifica di soddisfare i seguenti requisiti di autorizzazione prima di designare un account amministratore Macie diverso per la tua organizzazione:

- È necessario disporre delle [stesse autorizzazioni](#) necessarie per designare inizialmente un account amministratore Macie per l'organizzazione. È inoltre necessario essere autorizzati a eseguire la seguente azione: `AWS Organizations . organizations:DeregisterDelegatedAdministrator` Questa azione aggiuntiva consente di rimuovere la designazione corrente.

- Se il tuo account è attualmente un account membro Macie, l'attuale amministratore Macie deve rimuovere il tuo account come account membro Macie. Altrimenti, non ti sarà permesso di accedere alle operazioni di Macie per la designazione di un altro account amministratore. Dopo aver designato un nuovo account amministratore, il nuovo amministratore di Macie può aggiungere nuovamente il tuo account come account membro Macie.

Se la tua organizzazione utilizza Macie in più lingue Regioni AWS, assicurati inoltre di modificare la designazione in ogni regione in cui l'organizzazione utilizza Macie. L'account amministratore delegato di Macie deve essere lo stesso in tutte queste regioni. Se gestisci più organizzazioni in AWS Organizations, tieni inoltre presente che un account può essere l'account amministratore Macie delegato per una sola organizzazione alla volta. Per ulteriori informazioni sui requisiti aggiuntivi, consulta [Considerazioni sull'utilizzo di Macie con AWS Organizations](#)

Note

Quando si designa un account amministratore Macie diverso per l'organizzazione, si disabilita anche l'accesso ai dati statistici esistenti, ai dati di inventario e ad altre informazioni che Macie ha prodotto e fornito direttamente durante l'[individuazione automatica dei dati sensibili](#) per gli account dell'organizzazione. Il nuovo amministratore Macie non può accedere ai dati esistenti. Se si modifica la designazione e il nuovo amministratore Macie abilita l'individuazione automatica degli account, Macie genera e conserva nuovi dati quando esegue l'individuazione automatica degli account.

Per modificare la designazione di un account amministratore Macie

Per designare un account amministratore Macie diverso per la tua organizzazione, puoi utilizzare la console Amazon Macie o una combinazione di Amazon Macie e AWS Organizations APIs. Solo un utente dell'account di AWS Organizations gestione può modificare la designazione della propria organizzazione.

Console

Segui questi passaggi per modificare la designazione utilizzando la console Amazon Macie.

Per modificare la designazione

1. Accedi a AWS Management Console utilizzando il tuo account di AWS Organizations gestione.

2. Utilizzando il Regione AWS selettore nell'angolo in alto a destra della pagina, scegli la regione in cui desideri modificare la designazione.
3. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
4. Esegui una delle seguenti operazioni, a seconda che Macie sia abilitato per il tuo account di gestione nella regione corrente:
 - Se Macie non è abilitato, scegli Inizia nella pagina di benvenuto.
 - Se Macie è abilitato, scegli Impostazioni nel pannello di navigazione.
5. In Amministratore delegato, scegli Rimuovi. Per modificare la designazione, devi prima rimuovere la designazione corrente.
6. Confermate di voler rimuovere la designazione corrente.
7. In Amministratore delegato, inserisci l'ID dell'account a 12 cifre Account AWS da designare come nuovo account amministratore Macie per l'organizzazione.
8. Scegli Delega.

Ripeti i passaggi precedenti in ogni regione aggiuntiva in cui hai integrato Macie. AWS Organizations

API

Per modificare la designazione a livello di codice, utilizzi due operazioni dell'API Amazon Macie e un'operazione dell'API. AWS Organizations Questo perché devi rimuovere la designazione corrente sia in Macie che AWS Organizations prima di inviare la nuova designazione.

Per rimuovere la designazione attuale:

1. Usa il [DisableOrganizationAdminAccount](#) funzionamento dell'API Macie. Per il `adminAccountId` parametro richiesto, specifica l'ID account a 12 cifre dell' Account AWS account attualmente designato come account amministratore Macie per l'organizzazione.
2. Utilizza il [DeregisterDelegatedAdministrator](#) funzionamento dell'API. AWS Organizations Per il `AccountId` parametro, specifica l'ID account a 12 cifre per l'account attualmente designato come account amministratore Macie per l'organizzazione. Questo valore deve corrispondere all'ID dell'account specificato nella precedente richiesta Macie. Per il `ServicePrincipal` parametro, specifica il servizio Macie principal (`macie.amazonaws.com`)

Dopo aver rimosso la designazione corrente, invia la nuova designazione utilizzando il [EnableOrganizationAdminAccount](#) funzionamento dell'API Macie. Per il `adminAccountId`

parametro richiesto, specifica l'ID dell'account a 12 cifre da Account AWS designare come nuovo account amministratore Macie per l'organizzazione.

Per modificare la designazione utilizzando AWS Command Line Interface (AWS CLI), esegui il [disable-organization-admin-account](#) comando dell'API Macie e il comando dell'API. [deregister-delegated-administrator](#) AWS Organizations Questi comandi rimuovono la designazione corrente in Macie e, rispettivamente. AWS Organizations Per i account-id parametri admin-account-id and, specifica l'ID dell'account a 12 cifre Account AWS da rimuovere come account amministratore Macie corrente. Usa il region parametro per specificare la regione a cui si applica la rimozione. Per esempio:

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-account-id 111122223333 && aws organizations deregister-delegated-administrator --region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

Dove:

- **us-east-1** è la regione a cui si applica la rimozione, la regione Stati Uniti orientali (Virginia settentrionale).
- **111122223333** è l'ID dell'account da rimuovere come account amministratore di Macie.
- **macie.amazonaws.com** è il principale del servizio Macie.

Dopo aver rimosso la designazione corrente, invia la nuova designazione eseguendo il [enable-organization-admin-account](#) comando dell'API Macie. Per il admin-account-id parametro, specifica l'ID dell'account a 12 cifre da Account AWS designare come nuovo account amministratore Macie per l'organizzazione. Utilizzate il region parametro per specificare la regione a cui si applica la designazione. Per esempio:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 444455556666
```

us-east-1 Dov'è la regione a cui si applica la designazione (la regione Stati Uniti orientali (Virginia settentrionale)) ed **444455556666** è l'ID dell'account da designare come nuovo account amministratore di Macie.

Disattivazione dell'integrazione di Macie con AWS Organizations

Dopo l'integrazione di un' AWS Organizations organizzazione con Amazon Macie, l'account di AWS Organizations gestione può successivamente disabilitare l'integrazione. Come utente dell'account di AWS Organizations gestione, puoi farlo disabilitando l'accesso affidabile al servizio per Macie in AWS Organizations

Quando si disabilita l'accesso affidabile ai servizi per Macie, si verifica quanto segue:

- Macie perde lo status di servizio affidabile in AWS Organizations
- L'account amministratore Macie dell'organizzazione perde l'accesso a tutte le impostazioni, i dati e le risorse di Macie per tutti gli account membri Macie. Regioni AWS
- Tutti gli account dei membri Macie diventano account Macie indipendenti. Se Macie era abilitato per un account membro in una o più regioni, Macie continua ad essere abilitato per l'account in tali regioni. Tuttavia, l'account non è più associato a un account amministratore Macie in nessuna regione. Inoltre, l'account perde l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni prodotte e fornite direttamente da Macie durante l'individuazione automatica dei dati sensibili dell'account.

Per ulteriori informazioni sui risultati della disabilitazione dell'accesso affidabile ai servizi, consulta [Using AWS Organizations with other Servizi AWS nella Guida](#) per l'AWS Organizations utente.

Per disabilitare l'accesso affidabile ai servizi per Macie

Per disabilitare l'accesso affidabile ai servizi, puoi utilizzare la AWS Organizations console o l' AWS Organizations API. Solo un utente dell'account di AWS Organizations gestione può disabilitare l'accesso affidabile ai servizi per Macie. Per informazioni dettagliate sulle autorizzazioni necessarie, consulta [Autorizzazioni necessarie per disabilitare l'accesso affidabile](#) nella Guida per l'AWS Organizations utente.

Prima di disabilitare l'accesso affidabile ai servizi, opzionalmente collabora con l'amministratore Macie delegato della tua organizzazione per sospendere o disabilitare Macie for member account e per ripulire le risorse Macie relative agli account.

Console

Per disabilitare l'accesso affidabile ai servizi utilizzando la console, segui questi passaggi. AWS Organizations

Per disabilitare l'accesso al servizio attendibile

1. Accedi all'account di gestione AWS Management Console utilizzando il tuo account AWS Organizations di gestione.
2. Apri la AWS Organizations console all'indirizzo <https://console.aws.amazon.com/organizations/>.
3. Nel riquadro di navigazione, scegli Servizi.
4. In Servizi integrati, scegli Amazon Macie.
5. Scegli Disable trusted access (Disabilita accesso attendibile).
6. Conferma di voler disabilitare l'accesso affidabile.

API

Per disabilitare l'accesso affidabile ai servizi a livello di programmazione, utilizza l'operazione [Disable AWSService Access](#) dell' AWS Organizations API. Per il `ServicePrincipal` parametro, specificate il servizio Macie principal (`macie.amazonaws.com`).

Per disabilitare l'accesso affidabile ai servizi utilizzando [AWS Command Line Interface \(AWS CLI\)](#), esegui il [disable-aws-service-access](#) comando dell' AWS Organizations API. Per il `service-principal` parametro, specificate il servizio Macie principal (`macie.amazonaws.com`). Per esempio:

```
C:\> aws organizations disable-aws-service-access --service-principal
macie.amazonaws.com
```

Gestione di più account Macie su invito

Note

Ti consigliamo di utilizzare gli inviti AWS Organizations al posto di Macie per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione di più account Macie con AWS Organizations](#).

Puoi gestire centralmente più account Amazon Macie in due modi: integrando Macie AWS Organizations o utilizzando gli inviti all'iscrizione. Se utilizzi gli inviti all'iscrizione, un amministratore

Macie designato può gestire Macie per un massimo di 1.000 account. L'amministratore può anche accedere ai dati di inventario di Amazon Simple Storage Service (Amazon S3) e scoprire i dati sensibili nei bucket S3 di proprietà degli account. Per informazioni dettagliate sulle attività che l'amministratore può eseguire, consulta [Relazioni tra amministratore e account membro di Macie](#)

In un'organizzazione basata su inviti, si associano gli account Macie tra loro inviando e accettando inviti di iscrizione in Macie. Se invii un invito e questo viene accettato da un altro account, diventi l'amministratore Macie dell'altro account e l'altro account diventa un account membro della tua organizzazione. Se ricevi e accetti un invito, il tuo account diventa un account membro e l'amministratore Macie può accedere a determinate impostazioni, dati e risorse di Macie per il tuo account.

[Se crei un'organizzazione basata su inviti in Macie, puoi successivamente passare a utilizzare invece. AWS Organizations](#) Puoi anche usare entrambi i metodi contemporaneamente per gestire più account Macie. Ad esempio, se il tuo AWS ambiente include account di prova, puoi escludere gli account dalla tua organizzazione AWS Organizations e gestirli separatamente su invito.

Gli argomenti di questa sezione spiegano come creare e partecipare a un'organizzazione basata su inviti e come eseguire varie attività amministrative per l'organizzazione.

Argomenti

- [Considerazioni per le organizzazioni basate su inviti in Macie](#)
- [Creazione e gestione di un'organizzazione basata su inviti in Macie](#)
- [Revisione degli account Macie per un'organizzazione basata su inviti](#)
- [Modifica dell'account amministratore Macie per un'organizzazione basata su inviti](#)
- [Gestire l'appartenenza a un'organizzazione in Macie](#)

Considerazioni per le organizzazioni basate su inviti in Macie

Note

Ti consigliamo di utilizzare gli inviti AWS Organizations al posto di Macie per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione di più account Macie con AWS Organizations](#).

Prima di creare o iniziare a gestire un'organizzazione basata su inviti in Amazon Macie, considera i seguenti requisiti e consigli. Assicurati inoltre di comprendere la [relazione tra l'account amministratore di Macie](#) e quello dei membri.

Argomenti

- [Scelta di un account amministratore Macie](#)
- [Invio di inviti e gestione degli account dei membri di Macie](#)
- [Risposta e gestione degli inviti all'iscrizione](#)
- [Passaggio a AWS Organizations](#)

Scelta di un account amministratore Macie

Mentre stabilisci quale account deve essere l'account amministratore Macie per l'organizzazione, tieni presente quanto segue:

- Un'organizzazione può avere un solo account amministratore Macie.
- Un account non può essere un amministratore e un account membro di Macie allo stesso tempo.
- Macie è un servizio regionale. Ciò significa che l'associazione tra un account amministratore Macie e un account membro è regionale: l'associazione esiste solo se un invito viene inviato e accettato. Regione AWS Ad esempio, se l'amministratore Macie invia inviti nella regione Stati Uniti orientali (Virginia settentrionale) e tali inviti vengono accettati, l'amministratore Macie può gestire gli account dei membri solo in quella regione.
- Per gestire centralmente più account Macie Regioni AWS, l'amministratore Macie deve accedere a ciascuna regione in cui l'organizzazione utilizza attualmente o intende utilizzare Macie e inviare gli inviti agli account appropriati in ciascuna di tali regioni. Per un elenco delle regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS
- Un account membro può essere associato a un solo account amministratore Macie alla volta. Se l'organizzazione utilizza Macie in più regioni, significa che l'account amministratore Macie deve essere lo stesso in tutte le regioni. Tuttavia, gli account amministratore e membro devono inviare e accettare gli inviti separatamente in ciascuna regione.

Se l'account dell'amministratore di Macie Account AWS viene sospeso, isolato o chiuso, tutti gli account membro associati vengono automaticamente rimossi come account membro, ma Macie continua a essere abilitato per gli account. Gli account diventano account Macie indipendenti. Se il

[rilevamento automatico dei dati sensibili](#) è stato abilitato per un account membro, è disabilitato per l'account. Ciò disabilita anche l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni prodotte e fornite direttamente da Macie durante l'individuazione automatica dell'account. Dopo 30 giorni, questi dati scadono e Macie li elimina definitivamente. Per ripristinare l'accesso ai dati prima della scadenza, ripristina quello dell'amministratore di Macie Account AWS, quindi usa quell'account per creare e configurare nuovamente l'organizzazione.

Invio di inviti e gestione degli account dei membri di Macie

In qualità di amministratore di Macie di un'organizzazione basata sugli inviti, tieni presente quanto segue quando invii inviti e gestisci gli account dell'organizzazione:

- Se invii un invito, i dati correlati potrebbero essere trasferiti. Regioni AWS Questo accade perché Macie verifica l'indirizzo e-mail dell'account ricevente utilizzando un servizio di verifica e-mail che opera solo nella regione Stati Uniti orientali (Virginia settentrionale).
- Puoi inviare un invito a qualsiasi account attivo Account AWS, compresi gli account che non hanno abilitato Macie. Tuttavia, per accettare o rifiutare un invito, l'account ricevente deve abilitare Macie nella regione da cui è stato inviato l'invito.
- In ciascuno di essi Regione AWS, un account amministratore Macie può essere associato a non più di 1.000 account su invito. Ciò include gli account che non hanno ancora risposto agli inviti. Se il tuo account soddisfa questa quota, non puoi aggiungere o invitare altri account. Per determinare quanti account sono attualmente associati al tuo account, puoi utilizzare la pagina Account sulla console Amazon Macie o il [ListMembers](#) funzionamento dell'API Amazon Macie. Per ulteriori informazioni, consulta [Revisione degli account Macie per un'organizzazione basata su inviti](#).

Per ridurre il numero di account associati, puoi: eliminare le associazioni con account che attualmente non sono account membri, rimuovere il numero necessario di account membro o una combinazione dei due. Se un account si dimette dalla tua organizzazione o rifiuta un invito che hai inviato, riduce anche il numero di account associati al tuo account.

- Un account può essere associato a un solo account amministratore Macie alla volta. Ciò significa che un account non può accettare il tuo invito se è già associato a un altro account amministratore Macie. L'account deve prima dissociarsi dal suo attuale account amministratore Macie.
- In un'organizzazione basata su inviti, un account membro può dissociarsi dal proprio account amministratore Macie in qualsiasi momento. In tal caso, Macie continua a essere abilitato per l'account ma l'account diventa un account Macie autonomo. Macie non ti avvisa se un account membro si dissocia dal tuo account amministratore. Tuttavia, l'account continua a comparire nell'inventario del tuo account e ha lo stato di Membro dimesso.

- Se rimuovi un account membro dalla tua organizzazione, Macie continua a essere abilitato per l'account. L'account diventa un account Macie indipendente.

Risposta e gestione degli inviti all'iscrizione

Come destinatario di un invito o membro di un'organizzazione basata sugli inviti, tieni presente quanto segue quando rispondi e gestisci gli inviti che ricevi:

- Prima di accettare un invito, assicurati di aver compreso la [relazione tra l'amministratore di Macie](#) e gli account dei membri.
- Il tuo account può essere associato a un solo account amministratore Macie alla volta. Se accetti un invito e successivamente desideri entrare a far parte di un'altra organizzazione (su invito o tramite AWS Organizations), devi prima dissociare il tuo account dall'attuale account amministratore Macie. Potrai quindi entrare a far parte dell'altra organizzazione.
- Per accettare o rifiutare un invito, devi abilitare Macie nella cartella da Regione AWS cui è stato inviato l'invito. L'account che ha inviato l'invito non può abilitare Macie in quella regione per te. Il rifiuto di un invito è facoltativo. Se rifiuti un invito, puoi opzionalmente disabilitare Macie nella regione applicabile dopo aver rifiutato l'invito.
- Se sei un amministratore di Macie, non puoi accettare un invito a diventare un account membro: un account non può essere un amministratore Macie e un account membro allo stesso tempo. Per diventare un account membro, devi prima dissociare il tuo account da tutti i suoi account membro rimuovendo tutti gli account membro dalla tua attuale organizzazione.
- Macie è un servizio regionale. Se accetti un invito, l'associazione tra il tuo account e l'account amministratore di Macie è regionale: l'associazione esiste solo nel paese da Regione AWS cui l'invito è stato inviato e accettato.
- Se usi Macie in più regioni, l'account amministratore Macie del tuo account deve essere lo stesso in tutte le regioni. Tuttavia, l'amministratore di Macie deve inviarti gli inviti separatamente in ciascuna regione e tu devi accettarli separatamente in ciascuna regione.
- Puoi dissociare il tuo account da un account amministratore di Macie in qualsiasi momento. Allo stesso modo, l'amministratore Macie può rimuovere il tuo account dalla sua organizzazione in qualsiasi momento. In entrambi i casi:
 - Macie continua a essere abilitata per il tuo account. Il tuo account diventa un account Macie indipendente.
 - L'individuazione automatica dei dati sensibili è disabilitata per il tuo account, se era abilitata. Ciò disabilita anche l'accesso ai dati statistici esistenti, ai dati di inventario e ad altre informazioni che

Macie ha prodotto e fornito direttamente durante l'esecuzione del rilevamento automatico del tuo account. Puoi abilitare nuovamente il rilevamento automatico per il tuo account. Tuttavia, ciò non ripristina l'accesso ai dati esistenti. Invece, Macie genera e mantiene nuovi dati mentre esegue il rilevamento automatico del tuo account.

Passaggio a AWS Organizations

Dopo aver creato un'organizzazione basata su inviti in Macie, puoi passare a utilizzare invece. AWS Organizations Per semplificare la transizione, ti consigliamo di designare l'account amministratore esistente basato su invito come account amministratore Macie per l'organizzazione in. AWS Organizations

Se lo fai, tutti gli account membro attualmente associati continuano a esserlo. Se un account membro fa parte dell'organizzazione in AWS Organizations, l'associazione dell'account cambia automaticamente da Su invito a Via AWS Organizations in Macie. Se un account membro non fa parte dell'organizzazione in AWS Organizations, l'associazione dell'account continua a essere Su invito. In entrambi i casi, gli account continuano ad essere associati all'account amministratore Macie come account membri. Per quanto riguarda l'individuazione di dati sensibili, ciò significa anche che gli account possono continuare ad accedere a dati statistici e di altro tipo che Macie ha prodotto e fornito direttamente durante il rilevamento automatico dei dati sensibili per gli account. Inoltre, se l'amministratore di Macie ha configurato processi di rilevamento di dati sensibili per analizzare i dati relativi agli account, le esecuzioni successive continueranno a includere risorse di proprietà degli account.

Consigliamo questo approccio perché un account membro può essere associato a un solo account amministratore Macie alla volta. Se si designa un account diverso come account amministratore Macie per un'organizzazione in AWS Organizations, l'amministratore designato non sarà in grado di gestire gli account che sono già associati a un altro account amministratore Macie tramite invito. Ogni account membro deve prima dissociarsi dal suo attuale account amministratore basato su invito. Solo allora l'amministratore Macie dell'organizzazione può aggiungere l'account membro alla propria AWS Organizations organizzazione e iniziare a gestire Macie per l'account.

Dopo aver integrato Macie AWS Organizations e configurato l'organizzazione in Macie, puoi facoltativamente designare un account amministratore Macie diverso per l'organizzazione. Puoi anche continuare a utilizzare gli inviti per associare e gestire gli account dei membri che non fanno parte della tua organizzazione. AWS Organizations

Per informazioni sull'integrazione di Macie con AWS Organizations, consulta [Gestione di più account Macie con AWS Organizations](#)

Creazione e gestione di un'organizzazione basata su inviti in Macie

Note

Ti consigliamo di utilizzare gli inviti AWS Organizations al posto di Macie per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione di più account Macie con AWS Organizations](#).

Per creare un'organizzazione basata su inviti in Amazon Macie, devi innanzitutto determinare quale account desideri utilizzare come account amministratore Macie per l'organizzazione. Quindi usi quell'account per aggiungere account membro: invii inviti di iscrizione ad altri Account AWS, invitando gli account a entrare a far parte dell'organizzazione come account membri di Macie nell'attuale. Regione AWS Per creare l'organizzazione in più regioni, invia gli inviti di iscrizione da ciascuna regione in cui gli altri account utilizzano o intendono utilizzare Macie.

Quando un account accetta un invito, diventa un account membro Macie associato all'account amministratore Macie nella regione applicabile. L'account amministratore Macie può quindi accedere a determinate impostazioni, dati e risorse di Macie per l'account membro in quella regione.

In qualità di amministratore Macie di un'organizzazione basata su inviti, puoi consultare i dati di inventario e i risultati delle policy di Amazon Simple Storage Service (Amazon S3) per gli account dei membri. Puoi anche abilitare il rilevamento automatico dei dati sensibili ed eseguire processi di rilevamento dei dati sensibili per rilevare i dati sensibili nei bucket S3 di proprietà degli account membri. Per un elenco dettagliato delle attività che puoi eseguire, consulta [Relazioni tra amministratore e account membro di Macie](#)

Per impostazione predefinita, Macie ti offre la visibilità dei dati e delle risorse pertinenti per l'intera organizzazione. Puoi anche approfondire i dati e le risorse per i singoli account della tua organizzazione. Ad esempio, se [utilizzi la dashboard Summary](#) per valutare il livello di sicurezza di Amazon S3 della tua organizzazione, puoi filtrare i dati per account. Allo stesso modo, se [monitorate i costi di utilizzo stimati](#), potete accedere alle suddivisioni dei costi stimati per i singoli account membri.

Oltre alle attività comuni agli account amministratore e membro, è possibile eseguire centralmente varie attività amministrative per l'organizzazione. Prima di eseguire queste attività, è consigliabile esaminare le [considerazioni e i consigli](#) per la gestione delle organizzazioni basate su inviti in Macie.

Attività

- [Aggiungere gli account dei membri di Macie a un'organizzazione basata su inviti](#)
- [Sospensione di Macie per gli account dei membri di un'organizzazione basata su inviti](#)
- [Rimuovere gli account dei membri di Macie da un'organizzazione basata su inviti](#)
- [Eliminazione delle associazioni con altri account](#)

Aggiungere gli account dei membri di Macie a un'organizzazione basata su inviti

In qualità di amministratore di Amazon Macie per un'organizzazione basata su inviti, aggiungi account membro alla tua organizzazione eseguendo due passaggi principali:

1. Aggiungi gli account all'inventario del tuo account in Macie. In questo modo gli account vengono associati al tuo account.
2. Invia inviti di iscrizione agli account.

Quando un account accetta il tuo invito, diventa un account membro della tua organizzazione.

Passaggio 1: aggiungi gli account

Per aggiungere uno o più account all'inventario del tuo account, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Con la console Amazon Macie, puoi aggiungere un account alla volta o aggiungere più account contemporaneamente caricando un file con valori separati da virgole (CSV). Segui questi passaggi per aggiungere uno o più account utilizzando la console.

Per aggiungere un account

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri aggiungere un account.
3. Dal riquadro di navigazione, selezionare Accounts (Account). Si apre la pagina Account e mostra una tabella degli account attualmente associati al tuo account.
4. Scegliere Add accounts (Aggiungi account).

5. Nella sezione Inserisci i dettagli dell'account, scegli Aggiungi account. Quindi, esegui queste operazioni:
 - Per ID account, inserisci l'ID dell'account a 12 cifre Account AWS da aggiungere.
 - Per Indirizzo e-mail, inserisci l'indirizzo e-mail Account AWS da aggiungere.
6. Scegli Aggiungi.
7. Nella parte inferiore della pagina scegli Next (Avanti).

Macie aggiunge l'account all'inventario del tuo account. Il tipo di account è Su invito e il suo stato è Creato. Per aggiungere l'account in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Per aggiungere più account

1. Utilizzando un editor di testo, crea un file CSV come segue:
 - a. Aggiungi l'intestazione seguente come prima riga del file: Account ID,Email
 - b. Per ogni account, crea una nuova riga contenente l'ID account a 12 cifre Account AWS da aggiungere e l'indirizzo e-mail dell'account. Separa le voci con una virgola, ad esempio: 111111111111,janedoe@example.com

L'indirizzo e-mail deve corrispondere all'indirizzo e-mail associato a Account AWS.

- c. Verifica che il contenuto del file sia formattato come mostrato nell'esempio seguente, che contiene l'intestazione e le informazioni richieste per tre account:

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

- d. Salva il file sul computer.
2. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
3. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri aggiungere gli account.
4. Dal riquadro di navigazione, selezionare Accounts (Account). Si apre la pagina Account e mostra una tabella degli account attualmente associati al tuo account.
5. Scegliere Add accounts (Aggiungi account).

6. Nella sezione Inserisci i dettagli dell'account, scegli Carica elenco (CSV).
7. Scegli Sfoglia, quindi seleziona il file CSV creato nel passaggio 1.
8. Scegliere Add accounts (Aggiungi account).
9. Nella parte inferiore della pagina scegli Next (Avanti).

Macie aggiunge gli account all'inventario del tuo account. Il loro tipo è Su invito e il loro stato è Creato. Per aggiungere gli account in altre regioni, ripeti i passaggi da 3 a 8 in ciascuna regione aggiuntiva.

API

Per aggiungere uno o più account a livello di codice, utilizza il [CreateMember](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza i parametri supportati per specificare l'ID dell'account a 12 cifre e l'indirizzo e-mail per ciascuno di essi da aggiungere. Account AWS Specificate anche la regione a cui si riferisce la richiesta. Per aggiungere account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per aggiungere account utilizzando AWS Command Line Interface (AWS CLI), esegui il comando [create-member](#). Utilizzate il `region` parametro per specificare la regione in cui aggiungere gli account. Utilizzate i `account` parametri per specificare l'ID dell'account e l'indirizzo e-mail per ciascuno Account AWS di essi da aggiungere. Per esempio:

```
C:\> aws macie2 create-member --region us-east-1 --account="{\"accountId\":  
\"111111111111\",\"email\": \"janedoe@example.com\"}"
```

us-east-1 Dov'è la regione in cui aggiungere l'account (la regione Stati Uniti orientali (Virginia settentrionale)) e account i parametri specificano l'ID dell'account (**111111111111**) e l'indirizzo e-mail (**janedoe@example.com**) per l'account da aggiungere.

Se la tua richiesta ha esito positivo, Macie aggiunge ogni account all'inventario del tuo account con uno stato di Created e ricevi un output simile al seguente:

```
{  
  "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"  
}
```

arn Dov'è l'Amazon Resource Name (ARN) della risorsa che è stata creata per l'associazione tra il tuo account e l'account che hai aggiunto. In questo esempio, 123456789012 è l'ID dell'account che ha creato l'associazione e l'ID dell'account che 111111111111 è stato aggiunto.

Passaggio 2: inviare gli inviti di iscrizione agli account

Dopo aver aggiunto un account all'inventario del tuo account, puoi invitare l'account a entrare a far parte della tua organizzazione come account membro Macie. A tale scopo, invia un invito all'iscrizione all'account. Quando invii un invito, sulla console Amazon Macie vengono visualizzati un badge Account e una notifica per l'account del destinatario, se Macie è abilitato per l'account. Macie crea anche un AWS Health evento per l'account.

A seconda che utilizzi la console o l'API di Amazon Macie per inviare l'invito, Macie invia l'invito anche all'indirizzo e-mail che hai specificato per l'account del destinatario quando hai aggiunto l'account. Il messaggio e-mail indica che desideri diventare l'amministratore di Macie per il loro account e include l'ID dell'account tuo Account AWS e del destinatario. Account AWS Il messaggio spiega anche come accedere all'invito. Facoltativamente, puoi aggiungere testo personalizzato al messaggio.

Per inviare un invito all'iscrizione a uno o più account, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per inviare un invito all'iscrizione utilizzando la console Amazon Macie.

Per inviare un invito all'iscrizione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri inviare l'invito.
3. Dal riquadro di navigazione, selezionare Accounts (Account). Si apre la pagina Account e mostra una tabella degli account attualmente associati al tuo account.
4. Nella tabella Account esistenti, seleziona la casella di controllo per ogni account a cui desideri inviare l'invito.

Tip

Per identificare più facilmente gli account che hai aggiunto e a cui non hai ancora inviato inviti, puoi filtrare la tabella. A tale scopo, posiziona il cursore nella casella del filtro sopra la tabella, quindi scegli Stato. Quindi scegli Stato = Creato.

5. Nel menu Azioni, scegli Invita.

6. (Facoltativo) Nella casella Messaggio, inserisci il testo personalizzato che desideri includere nel messaggio e-mail che contiene l'invito. Il testo può contenere fino a 80 caratteri alfanumerici.
7. Seleziona Invite (Invita).

Per inviare l'invito in un altro formato Regioni AWS, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Dopo aver inviato l'invito, lo stato dell'account del destinatario cambia in Verifica e-mail in corso nell'inventario dell'account. Se Macie è in grado di verificare l'indirizzo e-mail di un account, lo stato dell'account passa successivamente a Invitato. Se Macie non riesce a verificare l'indirizzo, lo stato dell'account cambia in Verifica e-mail non riuscita. In tal caso, contatta il proprietario dell'account per ottenere l'indirizzo email corretto. Quindi [elimina l'associazione tra i tuoi account, aggiungi nuovamente l'account](#) e invia nuovamente l'invito.

Quando un destinatario accetta un invito, lo stato dell'account del destinatario cambia in Abilitato nell'inventario dell'account. Se un destinatario rifiuta un invito, l'account del destinatario viene dissociato dal tuo account e rimosso dall'inventario del tuo account.

API

Per inviare un invito a livello di codice, utilizza il [CreateInvitations](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza i parametri supportati per specificare l'ID dell'account a 12 cifre a cui Account AWS inviare l'invito. L'ID dell'account deve corrispondere all'ID dell'account presente nell'inventario dell'account. In caso contrario, si verifica un errore. Specificate anche la regione da cui inviare l'invito. Per inviare l'invito da altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Nella richiesta, puoi anche specificare se inviare l'invito come messaggio di posta elettronica e se includere testo personalizzato in quel messaggio. Se scegli di inviare un messaggio e-mail, Macie invia l'invito all'indirizzo email che hai specificato per un account quando hai aggiunto l'account all'inventario del tuo account. Per inviare l'invito come messaggio e-mail, ometti il `disableEmailNotification` parametro o imposta il valore del parametro su `false`. Il valore predefinito è `false`. Per aggiungere testo personalizzato al messaggio, utilizzate il `message` parametro per specificare il testo da aggiungere. Il testo può contenere fino a 80 caratteri alfanumerici.

[Per inviare inviti utilizzando il AWS CLI, esegui il comando `create-invitations`](#). Utilizzate il `region` parametro per specificare la regione da cui inviare l'invito. Utilizzate il `account-ids` parametro per specificare l'ID dell'account Account AWS a cui inviare l'invito. Per esempio:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-ids=["111111111111", "222222222222", "333333333333"]
```

us-east-1 Dov'è la regione da cui inviare l'invito (la regione Stati Uniti orientali (Virginia settentrionale)) e il `account-ids` parametro specifica l'account IDs per tre account a cui inviare l'invito. Per inviare un invito anche come messaggio di posta elettronica, includi anche il `no-disable-email-notification` parametro e, facoltativamente, includi il `message` parametro per specificare il testo personalizzato da aggiungere al messaggio.

Dopo aver inviato l'invito, lo stato di ogni account destinatario cambia in `EmailVerificationInProgress`. Se Macie è in grado di verificare l'indirizzo e-mail di un account, lo stato dell'account cambia successivamente in `Invited`. Se Macie non riesce a verificare l'indirizzo, lo stato dell'account diventa `EmailVerificationFailed`. In tal caso, contatta il proprietario dell'account per ottenere l'indirizzo corretto. Quindi [elimina l'associazione tra i tuoi account](#), [aggiungi nuovamente l'account](#) e invia nuovamente l'invito.

Quando un destinatario accetta un invito, lo stato dell'account del destinatario diventa `Enabled`. Nell'inventario del tuo account. Se un destinatario rifiuta un invito, l'account del destinatario viene dissociato dal tuo account e rimosso dall'inventario del tuo account.

Sospensione di Macie per gli account dei membri di un'organizzazione basata su inviti

In qualità di amministratore di Amazon Macie di un'organizzazione, puoi sospendere Macie in modo specifico Regione AWS per gli account dei singoli membri della tua organizzazione. Tieni presente, tuttavia, che non puoi riattivare Macie per un account membro dopo averlo sospeso. Solo un utente dell'account può successivamente riattivare Macie per l'account.

Quando sospendi Macie per un account utente:

- Macie perde l'accesso e smette di fornire i metadati relativi ai dati Amazon S3 dell'account nella regione.
- Macie interrompe l'esecuzione di tutte le attività relative all'account nella regione. Ciò include il monitoraggio dei bucket S3 per la sicurezza e il controllo degli accessi, l'esecuzione del

rilevamento automatico di dati sensibili e l'esecuzione di processi di rilevamento di dati sensibili attualmente in corso.

- Macie annulla tutti i processi di rilevamento di dati sensibili creati dall'account nella regione. Un lavoro non può essere ripreso o riavviato dopo essere stato annullato. Se hai creato offerte di lavoro per analizzare i dati di proprietà dell'account utente, Macie non annulla le tue offerte di lavoro. Invece, le offerte di lavoro ignorano le risorse di proprietà dell'account.

Mentre è sospeso, Macie conserva l'identificatore di sessione Macie, le impostazioni e le risorse che archivia o gestisce per l'account nella regione applicabile. Macie conserva inoltre determinati dati dell'account nella Regione. Ad esempio, i risultati dell'account rimangono intatti e non vengono modificati per un massimo di 90 giorni. Se l'individuazione automatica dei dati sensibili è stata abilitata per l'account, anche i risultati esistenti rimangono intatti e non vengono modificati per un massimo di 30 giorni. All'account non viene addebitato alcun costo per l'utilizzo di Macie nella regione applicabile, mentre Macie è sospeso per l'account in quella regione.

Per sospendere Macie per un account membro in un'organizzazione basata su inviti

Per sospendere Macie per un account membro in un'organizzazione basata su inviti, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per sospendere Macie per un account membro utilizzando la console Amazon Macie.

Per sospendere Macie per un account utente

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri sospendere Macie per un account membro.
3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account attualmente associati al tuo account.
4. Nella tabella Account esistenti, seleziona la casella di controllo relativa all'account per cui desideri sospendere Macie.
5. Nel menu Azioni, scegli Sospendi Macie.
6. Conferma di voler sospendere Macie per l'account selezionato.

Dopo aver confermato la sospensione, lo stato dell'account cambia in Sospeso (sospeso) nell'inventario dell'account.

Per sospendere Macie per l'account in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Per sospendere Macie for a member account a livello di codice, utilizza il [UpdateMemberSession](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza il `id` parametro per specificare l'ID dell'account a 12 cifre per Account AWS cui desideri sospendere Macie. Per il `status` parametro, specifica `PAUSED` come nuovo stato per Macie. Specificate anche la regione a cui si riferisce la richiesta. Per sospendere Macie in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per recuperare l'ID dell'account membro, puoi utilizzare il [ListMembers](#) funzionamento dell'API Amazon Macie. In tal caso, valuta la possibilità di filtrare i risultati includendo il `onlyAssociated` parametro nella richiesta. Se imposti il valore di questo parametro su `true`, Macie restituisce un `members` array che fornisce dettagli solo sugli account che attualmente sono account membri del tuo account amministratore.

Per sospendere Macie per un account membro utilizzando il AWS CLI, esegui il comando. [update-member-session](#) Utilizzate il `region` parametro per specificare la regione in cui sospendere Macie. Usa il `id` parametro per specificare l'ID dell'account per cui sospendere Macie. Per il parametro `status`, specifica `PAUSED`. Per esempio:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status PAUSED
```

us-east-1 Dov'è la regione in cui sospendere Macie (regione Stati Uniti orientali (Virginia settentrionale)), **123456789012** è l'ID dell'account per cui sospendere Macie e il nuovo stato di Macie per `PAUSED` l'account.

Se la richiesta ha esito positivo, Macie restituisce una risposta vuota e lo stato dell'account specificato viene modificato nell'inventario dell'account. `Paused`

Rimuovere gli account dei membri di Macie da un'organizzazione basata su inviti

In qualità di amministratore di Amazon Macie, puoi rimuovere un account membro dalla tua organizzazione. Puoi farlo dissociando l'account dall'account amministratore di Macie.

Se rimuovi un account membro, Macie continua a essere abilitato per l'account e l'account continua a comparire nell'inventario del tuo account. Tuttavia, l'account diventa un account Macie indipendente. Macie non notifica al proprietario dell'account quando rimuovi l'account. Pertanto, valuta la possibilità di contattare il proprietario dell'account per assicurarti che inizi a gestire le impostazioni e le risorse del suo account.

Quando rimuovi un account membro, perdi l'accesso a tutte le impostazioni, le risorse e i dati di Macie relativi all'account. Ciò include i risultati delle politiche e i metadati per i bucket S3 di proprietà dell'account. Inoltre, non puoi più usare Macie per scoprire dati sensibili nei bucket S3 di proprietà dell'account. Se hai già creato processi di rilevamento di dati sensibili a tale scopo, i lavori ignorano i bucket di proprietà dell'account. Se hai abilitato l'individuazione automatica dei dati sensibili per l'account, sia tu che l'account perderete l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni che Macie ha prodotto e fornito direttamente durante l'individuazione automatica dell'account.

Dopo aver rimosso un account membro, puoi successivamente aggiungerlo nuovamente alla tua organizzazione inviando un nuovo invito all'account. Se l'account accetta il nuovo invito e abilita l'individuazione automatica dei dati sensibili entro 30 giorni, potrai inoltre accedere nuovamente ai dati e alle informazioni che Macie aveva precedentemente prodotto e fornito direttamente durante l'individuazione automatica dell'account. Inoltre, le esecuzioni successive dei job esistenti ricominciano a includere i bucket S3 dell'account.

Se rimuovi un account membro e non intendi aggiungerlo nuovamente, puoi rimuoverlo completamente dall'inventario del tuo account. Per scoprire come, consulta [Eliminazione delle associazioni con altri account](#).

Per rimuovere un account membro da un'organizzazione basata su inviti

Per rimuovere un account membro dalla tua organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per rimuovere un account membro utilizzando la console Amazon Macie.

Per rimuovere un account membro

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri rimuovere un account membro.

3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account attualmente associati al tuo account.
4. Nella tabella Account esistenti, seleziona la casella di controllo relativa all'account che desideri rimuovere.
5. Nel menu Azioni, scegli Dissocia account.
6. Conferma di voler rimuovere l'account selezionato come account membro.

Dopo aver confermato la selezione, lo stato dell'account cambia in Rimosso (dissociato) nell'inventario dell'account.

Per rimuovere l'account membro in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Per rimuovere un account membro a livello di codice, utilizza il [DisassociateMember](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza il `id` parametro per specificare l' Account AWS ID a 12 cifre dell'account membro da rimuovere. Specificate anche la regione a cui si riferisce la richiesta. Per rimuovere l'account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per recuperare l'ID dell'account da rimuovere, puoi utilizzare il [ListMembers](#) funzionamento dell'API Amazon Macie. In tal caso, valuta la possibilità di filtrare i risultati includendo il `onlyAssociated` parametro nella richiesta. Se imposti il valore di questo parametro su `true`, Macie restituisce un `members` array che fornisce dettagli solo sugli account attualmente membri del tuo account.

Per rimuovere un account membro utilizzando il AWS CLI, esegui il comando [disassociate-member](#). Utilizzate il `region` parametro per specificare la regione in cui rimuovere l'account. Utilizzate il `id` parametro per specificare l'ID dell'account da rimuovere. Per esempio:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

us-east-1 Dov'è la regione in cui rimuovere l'account (la regione Stati Uniti orientali (Virginia settentrionale)) e **123456789012** l'ID dell'account da rimuovere.

Se la richiesta ha esito positivo, Macie restituisce una risposta vuota e lo stato dell'account specificato viene modificato `Removed` nell'inventario dell'account.

Eliminazione delle associazioni con altri account

Dopo aver aggiunto un account all'inventario del tuo account in Amazon Macie, puoi eliminare l'associazione tra il tuo account e l'altro account. Puoi eseguire questa operazione per qualsiasi account presente nel tuo inventario, ad eccezione di:

- Un account che fa parte della tua organizzazione in AWS Organizations. Questo tipo di associazione AWS Organizations non è controllata da Macie.
- Un account membro che ha accettato un invito a iscriversi a Macie per entrare a far parte della tua organizzazione. In tal caso, è necessario [rimuovere l'account membro](#) prima di poter eliminare l'associazione.

Quando elimini un'associazione, Macie rimuove l'account dall'inventario del tuo account. Se desideri ripristinare successivamente l'associazione, devi aggiungere nuovamente l'account come se fosse un account completamente nuovo.

Per eliminare un'associazione con un altro account

Per eliminare un'associazione tra il tuo account e un altro account, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Per utilizzare la console Amazon Macie per eliminare un'associazione con un altro account, segui questi passaggi.

Per eliminare un'associazione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri eliminare un'associazione.
3. Dal riquadro di navigazione, selezionare Accounts (Account). La pagina Account si apre e mostra una tabella degli account attualmente associati al tuo account.
4. Nella tabella Account esistenti, seleziona la casella di controllo relativa all'account di cui desideri eliminare l'associazione.
5. Dal menu Actions (Operazioni), scegli Delete (Elimina).
6. Conferma di voler eliminare l'associazione selezionata.

Per eliminare l'associazione in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Per eliminare un'associazione con un altro account a livello di codice, utilizza il [DeleteMember](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, utilizza il `id` parametro per specificare l'ID dell'account a 12 cifre con cui Account AWS eliminare l'associazione. Specificate anche la regione a cui si riferisce la richiesta. Per eliminare l'associazione in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per recuperare l'ID dell'account, puoi utilizzare il [ListMembers](#) funzionamento dell'API Amazon Macie. In tal caso, includi il `onlyAssociated` parametro nella richiesta e imposta il valore del parametro su `false`. Se l'operazione ha esito positivo, Macie restituisce un `members` array che fornisce dettagli su tutti gli account associati al tuo account, inclusi gli account che attualmente non sono account membri.

Per eliminare un'associazione con un altro account utilizzando il AWS CLI, esegui il comando [delete-member](#). Utilizzate il `region` parametro per specificare la regione in cui eliminare l'associazione. Utilizzate il `id` parametro per specificare l'ID dell'account. Per esempio:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

us-east-1 Dov'è la regione in cui eliminare l'associazione con l'altro account (la regione Stati Uniti orientali (Virginia settentrionale)) e *123456789012* l'ID dell'account.

Se la richiesta ha esito positivo, Macie restituisce una risposta vuota e l'associazione tra il tuo account e l'altro account viene eliminata. L'account precedentemente associato viene rimosso dall'inventario dell'account.

Revisione degli account Macie per un'organizzazione basata su inviti

Note

Ti consigliamo di utilizzare gli inviti AWS Organizations al posto di Macie per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione di più account Macie con AWS Organizations](#).

Se sei l'amministratore di Amazon Macie di un'organizzazione basata su inviti, Macie ti fornisce un inventario degli account associati al tuo account Macie in ognuno dei quali utilizzi Macie. Regione AWS Puoi utilizzare questo inventario per esaminare le statistiche e i dettagli dell'account per la tua organizzazione. Puoi anche utilizzarlo per [eseguire determinate attività di gestione](#) degli account dei membri e gestire lo stato della relazione tra il tuo account e gli altri account.

Per esaminare gli account di un'organizzazione basata su inviti

Per esaminare gli account della tua organizzazione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per rivedere gli account della tua organizzazione utilizzando la console Amazon Macie.

Per esaminare gli account della tua organizzazione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri esaminare gli account della tua organizzazione.
3. Dal riquadro di navigazione, selezionare Accounts (Account).

La pagina Account si apre e mostra statistiche aggregate e una tabella degli account associati al tuo account Macie nell'attuale. Regione AWS

Nella parte superiore della pagina Account, troverai le seguenti statistiche aggregate.

Tramite AWS Organizations

Se sei l'amministratore Macie di un'organizzazione in AWS Organizations, Active riporta il numero totale di account associati al tuo account tramite AWS Organizations e che sono attualmente membri Macie della tua organizzazione. Macie è abilitato per questi account e tu sei l'amministratore Macie degli account.

Tutto riporta il numero totale di account associati al tuo account tramite. AWS Organizations Ciò include gli account che attualmente non sono account membri di Macie. Include anche gli account dei membri per i quali Macie è attualmente sospeso.

Su invito

Active riporta il numero totale di account attualmente membri di Macie nella tua organizzazione basata sugli inviti. Macie è abilitato per questi account e tu sei l'amministratore Macie degli account perché hanno accettato un tuo invito a iscriversi.

Tutto riporta il numero totale di account associati al tuo account su invito di Macie, inclusi gli account che non hanno risposto a un tuo invito.

Attivi/Tutti

Active riporta il numero totale di account per i quali Macie è attualmente abilitato nell'organizzazione, incluso il proprio account. Sei l'amministratore Macie di questi account tramite AWS Organizations o su invito di Macie.

Tutto riporta il numero totale di account associati al tuo account, tramite AWS Organizations o su invito, più il tuo account. Sono inclusi gli account che non hanno risposto a un tuo invito di iscrizione a Macie. Include anche gli account che sono associati al tuo account tramite account Macie AWS Organizations e che attualmente non sono membri di Macie.

Nella tabella, troverai i dettagli su ogni account nella regione corrente. La tabella include tutti gli account associati al tuo account Macie su invito o tramite Macie. AWS Organizations

ID account

L'ID dell'account e l'indirizzo e-mail di Account AWS

Nome

Il nome dell'account per Account AWS. Questo valore è generalmente N/A per il tuo account e per gli account associati al tuo account su invito.

Tipo

In che modo l'account viene associato al tuo account, su invito o tramite AWS Organizations. Per il tuo account, questo valore è Conto corrente.

Stato

Lo stato della relazione tra il tuo account e l'account. Per un account in un'organizzazione basata su inviti (Tipo è Per invito), i valori possibili sono:

- Account sospeso: Account AWS è sospeso.
- Creato (invito): hai aggiunto l'account ma non hai inviato un invito all'iscrizione.

- Verifica e-mail non riuscita: hai provato a inviare un invito all'iscrizione all'account ma l'indirizzo email specificato non è valido per l'account.
- Verifica e-mail in corso: hai inviato un invito all'iscrizione all'account e Macie sta elaborando la richiesta.
- Abilitato: l'account è un account membro. Macie è abilitato per l'account e tu sei l'amministratore Macie dell'account.
- Invitato: hai inviato un invito all'iscrizione all'account e l'account non ha risposto al tuo invito.
- Membro dimesso: l'account era precedentemente un account membro. Tuttavia, l'account si è dimesso dall'organizzazione in seguito alla dissociazione dall'account.
- In pausa (sospeso): l'account è un account membro, ma Macie è attualmente sospeso per l'account.
- Regione disattivata: la regione corrente è disabilitata per Account AWS
- Rimosso (dissociato): l'account era precedentemente un account membro. Tuttavia, l'hai rimosso come account membro dissociandolo dal tuo account.

Ultimo aggiornamento dello stato

L'ultima volta che tu o l'account associato avete eseguito un'azione che ha influito sulla relazione tra i vostri account.

Rilevamento automatico di dati sensibili

Se il rilevamento automatico dei dati sensibili è attualmente abilitato o disabilitato per l'account.

Per ordinare la tabella in base a un campo specifico, scegli l'intestazione di colonna del campo. Per modificare l'ordinamento, scegli nuovamente l'intestazione della colonna. Per filtrare la tabella, posiziona il cursore nella casella del filtro, quindi aggiungi una condizione di filtro per un campo. Per perfezionare ulteriormente i risultati, aggiungi condizioni di filtro per campi aggiuntivi.

API

Per esaminare gli account della tua organizzazione a livello di codice, utilizza il [ListMembers](#) funzionamento dell'API Amazon Macie e specifica la regione a cui si riferisce la richiesta. Per esaminare i dettagli in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Quando invii la richiesta, utilizza il `onlyAssociated` parametro per specificare quali account includere nella risposta. Per impostazione predefinita, Macie restituisce i dettagli solo sugli account che sono account membri nella regione specificata, su invito o tramite AWS Organizations. Per recuperare i dettagli di tutti gli account associati, compresi gli account che non

sono account membri, includi il `onlyAssociated` parametro nella richiesta e imposta il valore del parametro su `false`.

Per esaminare gli account dell'organizzazione utilizzando il comando [AWS Command Line Interface \(AWS CLI\)](#), esegui il comando [list-members](#). Per il `only-associated` parametro, specificate se includere tutti gli account associati o solo gli account dei membri. Per includere solo gli account dei membri, ometti questo parametro o imposta il valore del parametro su `true`. Per includere tutti gli account, imposta questo valore su `false`. Per esempio:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

us-east-1 Dov'è la regione a cui si riferisce la richiesta, la regione Stati Uniti orientali (Virginia settentrionale).

Se la richiesta ha esito positivo, Macie restituisce un array. `members` L'array contiene un `member` oggetto per ogni account che soddisfa i criteri specificati nella richiesta. In quell'oggetto, il `relationshipStatus` campo indica lo stato corrente dell'associazione tra il tuo account e l'altro account nella regione specificata. Per un account in un'organizzazione basata su inviti, i valori possibili sono:

- **AccountSuspended**— Account AWS È sospeso.
- **Created**— Hai aggiunto l'account ma non hai inviato un invito all'iscrizione.
- **EmailVerificationFailed**— Hai provato a inviare un invito all'iscrizione all'account ma l'indirizzo email specificato non è valido per l'account.
- **EmailVerificationInProgress**— Hai inviato un invito all'iscrizione all'account e Macie sta elaborando la richiesta.
- **Enabled**— L'account è un account membro. Macie è abilitato per l'account e tu sei l'amministratore Macie dell'account.
- **Invited**— Hai inviato un invito all'iscrizione all'account e l'account non ha risposto al tuo invito.
- **Paused**— L'account è un account membro, ma Macie è attualmente sospeso (in pausa) per l'account.
- **RegionDisabled**— La regione corrente è disabilitata per. Account AWS
- **Removed**— L'account era precedentemente un account membro. Tuttavia, l'hai rimosso come account membro dissociandolo dal tuo account.
- **Resigned**— L'account era precedentemente un account membro. Tuttavia, l'account si è dimesso dall'organizzazione in seguito alla dissociazione dall'account.

Per informazioni sugli altri campi dell'oggetto, consulta [Members](#) in the Amazon Macie API Reference.

Modifica dell'account amministratore Macie per un'organizzazione basata su inviti

Note

Ti consigliamo di utilizzare gli inviti AWS Organizations al posto di Macie per gestire gli account dei membri. Per ulteriori informazioni, consulta [Gestione di più account Macie con AWS Organizations](#).

Dopo aver creato e stabilito un'organizzazione basata su inviti, puoi modificare l'account amministratore di Amazon Macie per l'organizzazione. A tale scopo, gli amministratori e i membri dell'organizzazione devono adottare le seguenti misure:

1. L'attuale amministratore di Macie esporta facoltativamente l'inventario corrente degli account dei membri dell'organizzazione. Ciò semplifica la transizione aiutandoti a identificare gli account che dovrebbero continuare a far parte dell'organizzazione.
2. L'attuale amministratore di Macie [rimuove tutti gli account dei membri](#) dall'organizzazione corrente. Questo dissocia gli account dall'account amministratore corrente. Macie continua a essere abilitato per gli account, ma gli account diventano account Macie indipendenti.

Important

Quando l'attuale amministratore Macie rimuove gli account dei membri, Macie disabilita automaticamente l'individuazione automatica dei dati sensibili per gli account. Ciò disabilita anche l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni prodotte e fornite direttamente da Macie durante l'individuazione automatica degli account. Una volta completata la transizione verso la nuova organizzazione, il nuovo amministratore di Macie non può accedere a questi dati.

3. Il nuovo amministratore Macie [aggiunge gli account dei membri precedenti](#) alla nuova organizzazione. Questo associa gli account al nuovo account amministratore.

4. Ogni account membro accetta l'invito a entrare a far parte della nuova organizzazione. Quando un account accetta l'invito, diventa un account membro della nuova organizzazione. Il nuovo amministratore Macie può quindi accedere alle impostazioni, ai dati e alle risorse di Macie per l'account. Se l'individuazione automatica dei dati sensibili era stata precedentemente abilitata per l'account, ciò non include i dati che Macie aveva precedentemente prodotto e fornito direttamente durante l'esecuzione del rilevamento automatico dell'account. Macie genera e mantiene invece nuovi dati per l'account, se il nuovo amministratore Macie abilita il rilevamento automatico dell'account.

Se la tua organizzazione utilizza Macie in più di un'area Regioni AWS, esegui i passaggi precedenti in ciascuna di queste regioni.

Per esportare l'inventario corrente degli account dei membri, l'attuale amministratore Macie può utilizzare la console Amazon Macie o l'API Amazon Macie. Con la console, l'attuale amministratore può esportare i dati in un file con valori separati da virgole (CSV). Il nuovo amministratore può quindi utilizzare la console per caricare il file CSV e aggiungere tutti gli account (in blocco) alla nuova organizzazione.

Per esportare i dati degli account dei membri utilizzando la console

1. Accedi AWS Management Console utilizzando l'attuale account amministratore di Macie.
2. Utilizzando il Regione AWS selettore nell'angolo in alto a destra della pagina, scegli la regione in cui desideri esportare i dati.
3. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
4. Dal riquadro di navigazione, selezionare Accounts (Account). Si apre la pagina Account e visualizza una tabella degli account associati all'attuale account amministratore di Macie.
5. (Facoltativo) Per filtrare la tabella e mostrare solo gli account che sono attualmente account membri dell'organizzazione, utilizza la casella di filtro sopra la tabella per aggiungere le seguenti condizioni di filtro:
 - Tipo = Invito
 - Stato = Abilitato
 - Stato = In pausa
6. Nella tabella, seleziona la casella di controllo per ogni account membro da includere nei dati esportati.
7. Scegli Esporta CSV.

8. Specificate un nome e una posizione per il file.

Con l'API Amazon Macie, l'attuale amministratore di Macie può recuperare i dati in formato JSON. Il nuovo amministratore Macie può quindi utilizzare tali dati per generare l'elenco di account IDs e indirizzi e-mail per gli account da aggiungere e invitare alla nuova organizzazione. Per recuperare i dati in formato JSON, utilizza il [ListMembers](#) funzionamento dell'API Amazon Macie. Se l'operazione ha esito positivo, Macie restituisce un `members` array che fornisce dettagli su tutti gli account associati all'account dell'amministratore. Se un account è attualmente un account membro, il valore della `relationshipStatus` proprietà dell'account è `Enabled` o `Paused` e la `invitedAt` proprietà specifica una data e un'ora.

Gestire l'appartenenza a un'organizzazione in Macie

Note

Ti consigliamo di utilizzare AWS Organizations invece degli inviti Macie per gestire centralmente Macie per più account. Per ulteriori informazioni, consulta [Gestione di più account Macie con AWS Organizations](#).

Se sei invitato a far parte di un'organizzazione in Amazon Macie, puoi facoltativamente accettare o rifiutare l'invito. In Macie, un'organizzazione è un insieme di account gestiti centralmente come gruppo di account correlati. Un'organizzazione è composta da un account amministratore Macie designato e da uno o più account membro associati.

Se accetti un invito, il tuo account diventa un account membro dell'organizzazione. Quando accetti, l'account che ha inviato l'invito diventa l'account amministratore Macie del tuo account: associ il tuo account all'altro account e abiliti una relazione amministratore-membro tra gli account. L'account amministratore Macie può quindi accedere a determinate impostazioni, dati e risorse di Macie per il tuo account, se necessario. Regione AWS Per informazioni dettagliate sulle attività che l'account amministratore può eseguire, consulta. [Relazioni tra amministratore e account membro di Macie](#)

Se rifiuti un invito, lo stato e le impostazioni correnti del tuo account Macie non vengono modificati.

Argomenti

- [Rispondere agli inviti di iscrizione per le organizzazioni](#)
- [Dissociarsi da un account amministratore di Macie](#)

Rispondere agli inviti di iscrizione per le organizzazioni

Quando ricevi un invito a entrare a far parte di un'organizzazione, Amazon Macie ti avvisa in diversi modi. Per impostazione predefinita, Macie ti invia l'invito come messaggio e-mail. Macie crea anche un AWS Health evento per te. Account AWS Se usi già Macie Regione AWS da cui è stato inviato l'invito, Macie visualizza anche il badge Accounts e una notifica sulla console Macie.

Dopo aver ricevuto un invito, puoi facoltativamente accettarlo o rifiutarlo. Prima di rispondere, tieni presente quanto segue:

- Puoi essere membro di una sola organizzazione alla volta. Se ricevi più inviti, puoi accettarne solo uno. Oppure, se sei già membro di un'organizzazione, devi dissociare il tuo account dall'attuale account amministratore di Macie prima di poter entrare a far parte di un'altra organizzazione.
- Se usi Macie in più regioni, il tuo account deve avere lo stesso account amministratore Macie in tutte queste regioni. L'amministratore di Macie deve inviarti gli inviti separatamente da ciascuna regione e tu devi accettarli separatamente in ciascuna regione.
- Per accettare o rifiutare un invito, devi abilitare Macie nella regione da cui è stato inviato l'invito. Il rifiuto di un invito è facoltativo. Se consenti a Macie di rifiutare un invito, puoi [disabilitare Macie](#) nella regione dopo aver rifiutato l'invito. Questo aiuta a evitare costi inutili per l'utilizzo di Macie nella regione.
- Se il rilevamento automatico dei dati sensibili è abilitato per il tuo account e accetti un invito, perdi l'accesso ai dati statistici, ai dati di inventario e ad altre informazioni che Macie ha prodotto e fornito direttamente durante l'esecuzione del rilevamento automatico del tuo account. Dopo aver accettato un invito, l'amministratore di Macie può abilitare il rilevamento automatico per il tuo account. Tuttavia, ciò non ripristina l'accesso ai dati esistenti. Invece, Macie genera e mantiene nuovi dati mentre esegue il rilevamento automatico del tuo account.

Per ulteriori considerazioni, consulta. [Risposta e gestione degli inviti all'iscrizione](#)

Per rispondere a un invito a diventare membro di un'organizzazione

Per rispondere a un invito all'iscrizione, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per rispondere a un invito di iscrizione utilizzando la console Amazon Macie.

Per rispondere a un invito di iscrizione

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui hai ricevuto l'invito.
3. Se non hai abilitato Macie nella regione, scegli Inizia, quindi scegli Abilita Macie. Devi abilitare Macie prima di poter accettare o rifiutare un invito.
4. Dal riquadro di navigazione, selezionare Accounts (Account).
5. In Account amministratore, esegui una delle seguenti operazioni:
 - Per accettare l'invito, attiva Accept  accanto all'invito. Quindi scegli Accetta invito o Aggiorna, a seconda che tu abbia accettato in precedenza un altro invito.
 - Per rifiutare l'invito, scegli Rifiuta invito accanto all'invito, quindi conferma che desideri rifiutare l'invito.

Se hai ricevuto e desideri rispondere all'invito in altre regioni, ripeti i passaggi precedenti in ciascuna regione aggiuntiva.

API

Per rispondere a un invito in modo programmatico, utilizza [AcceptInvitation](#) o [DeclineInvitations](#) utilizza l'API Amazon Macie, a seconda che tu voglia accettare o rifiutare l'invito. Quando invii la richiesta, assicurati di specificare la regione da cui è stato inviato l'invito. Per rispondere all'invito in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

In una `AcceptInvitation` richiesta, utilizza il `administratorAccountId` parametro per specificare l'ID dell'account a 12 cifre per chi ha inviato Account AWS l'invito. Utilizzate il `invitationId` parametro per specificare l'ID univoco dell'invito da accettare.

In una `DeclineInvitations` richiesta, utilizzate il `accountIds` parametro per specificare l'ID dell'account a 12 cifre dell'utente Account AWS che ha inviato l'invito da rifiutare.

Per recuperare gli ID, puoi utilizzare il [ListInvitations](#) funzionamento dell'API Amazon Macie. Se l'operazione ha esito positivo, Macie restituisce un `invitations` array che fornisce dettagli sugli inviti che hai ricevuto, incluso l'ID dell'account che ha inviato ogni invito e l'ID univoco per ogni

invito. Se il valore della `relationshipStatus` proprietà di un invito è `Invited`, non hai ancora risposto all'invito.

Per rispondere a un invito utilizzando [AWS Command Line Interface \(AWS CLI\)](#), esegui il comando [accept-invitation](#) o [decline-invitations](#), a seconda che tu voglia accettare o rifiutare l'invito. Utilizzate il `region` parametro per specificare la regione da cui è stato inviato l'invito. Per esempio:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

Dov'è la regione da cui `us-east-1` è stato inviato l'invito (la regione Stati Uniti orientali (Virginia settentrionale)), `123456789012` è l'ID account dell'account che ha inviato l'invito ed `d8bdad0e203fd1242e0a4721bexample` è l'ID univoco dell'invito da accettare.

Se una richiesta di accettazione di un invito ha esito positivo, Macie restituisce una risposta vuota. Se una richiesta di rifiuto di un invito ha esito positivo, Macie restituisce un array vuoto. `unprocessedAccounts`

Dopo aver rifiutato un invito, l'invito persiste come risorsa per il tuo account Macie. [Facoltativamente, puoi eliminarlo utilizzando l'DeleteInvitationsoperazione o, per il AWS CLI, il comando delete-invitations.](#)

Dissociarsi da un account amministratore di Macie

Se accetti un invito a entrare a far parte di un'organizzazione in Amazon Macie, puoi successivamente dimetterti dall'organizzazione dissociando il tuo account dall'account amministratore Macie corrente. Tieni presente che non puoi farlo se il tuo account è un account membro di un'organizzazione. AWS Organizations Per dimetterti da un' AWS Organizations organizzazione, contatta l'amministratore di Macie per rimuovere il tuo account come account membro di Macie.

Se dissocii il tuo account dall'account amministratore Macie, l'amministratore Macie perde l'accesso a tutte le impostazioni, i dati e le risorse del tuo account Macie. Ciò include i metadati e i risultati delle policy per i dati di Amazon S3 di tua proprietà. Ciò significa anche che l'amministratore non può più analizzare i dati di Amazon S3 eseguendo il rilevamento automatico di dati sensibili o eseguendo processi di rilevamento di dati sensibili.

Quando annulli l'associazione del tuo account, Macie continua a essere abilitato per il tuo account nella regione applicabile. Tuttavia, il tuo account diventa un account Macie autonomo nella regione. Lo stato del tuo account cambia in Membro dimesso nell'inventario degli account dell'amministratore.

Per dissociarsi da un account amministratore di Macie

Per dissociare il tuo account dall'attuale account amministratore Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie.

Console

Segui questi passaggi per dissociare il tuo account dall'account amministratore Macie utilizzando la console Amazon Macie.

Per dissociarsi da un account amministratore

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri dissociare il tuo account dall'account amministratore.
3. Dal riquadro di navigazione, selezionare Accounts (Account).
4. In Account amministratore, disattiva Accept
()
accanto all'invito, quindi scegli Aggiorna.

L'account continua a essere visualizzato nella pagina Account. Se decidi di rientrare nell'organizzazione, puoi utilizzare questa pagina per accettare nuovamente l'invito originale. In alternativa, puoi rifiutare ed eliminare l'invito, eliminando anche l'associazione tra il tuo account e l'altro account. Per fare ciò, scegli Rifiuta l'invito.

Se desideri dissociare il tuo account dall'account amministratore Macie in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

API

Per dissociare il tuo account dall'account amministratore Macie a livello di codice, usa il [DisassociateFromAdministratorAccount](#) funzionamento dell'API Amazon Macie. Quando invii la richiesta, assicurati di specificare la regione a cui si riferisce la richiesta. Per dissociarti dall'account in altre regioni, invia la richiesta in ciascuna regione aggiuntiva.

Per dissociare il tuo account dall'account amministratore di Macie utilizzando il AWS CLI, esegui il comando. [disassociate-from-administrator-account](#) Utilizza il `region` parametro per specificare la regione in cui dissociarsi dall'account.

Se la richiesta ha esito positivo, Macie restituisce una risposta vuota.

Dopo la dissociazione dall'account, l'invito originale rimane una risorsa per il tuo account Macie, a meno che tu non lo elimini. Se decidi di rientrare nell'organizzazione, puoi utilizzare questa risorsa per accettare nuovamente l'invito originale. In alternativa, puoi eliminare l'invito utilizzando l'[DeleteInvitations](#) operazione o, per il AWS CLI, il comando [delete-invitations](#). Se elimini l'invito, elimini anche l'associazione tra il tuo account e l'altro account.

Etichettare le risorse di Macie

Un tag è un'etichetta che puoi definire e assegnare alle AWS risorse, inclusi alcuni tipi di risorse Amazon Macie. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Ad esempio, puoi utilizzare i tag per: applicare politiche, allocare i costi, distinguere tra le versioni delle risorse o identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità.

Puoi assegnare tag ai seguenti tipi di risorse Macie: elenchi di autorizzazioni, identificatori di dati personalizzati, regole di filtro e regole di soppressione per i risultati e i processi di scoperta di dati sensibili. Se sei l'amministratore Macie di un'organizzazione, puoi anche assegnare tag agli account dei membri della tua organizzazione.

Una risorsa può avere fino a 50 tag. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Una chiave tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

Ad esempio, se si creano identificatori di dati personalizzati e processi di individuazione di dati sensibili per analizzare i dati in diversi punti di un flusso di lavoro (un set per i dati staged e un altro per i dati di produzione), è possibile assegnare una chiave di Stack tag a tali risorse. Il valore del tag per questa chiave di tag potrebbe riguardare Staging gli identificatori di dati personalizzati e i processi che analizzano i dati staged e per gli altri. Production

Argomenti

- [Nozioni fondamentali sull'etichettatura per le risorse di Macie](#)
- [Aggiungere tag alle risorse Macie](#)
- [Controllo dell'accesso alle risorse di Macie tramite tag](#)
- [Revisione e modifica dei tag per le risorse Macie](#)
- [Rimozione dei tag dalle risorse di Macie](#)

Nozioni fondamentali sull'etichettatura per le risorse di Macie

Per identificare, classificare e gestire le risorse Amazon Macie per il tuo account, puoi assegnare tag alle risorse. Un tag è un'etichetta che definisci e assegni alle AWS risorse, inclusi determinati tipi di risorse Macie. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale.

Una chiave tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag. Una risorsa può avere fino a 50 tag.

Puoi assegnare tag ai seguenti tipi di risorse Macie:

- Consenti elenchi
- Identificatori di dati personalizzati
- Regole di filtro e regole di soppressione per i risultati
- Lavori di individuazione di dati sensibili

Se sei l'amministratore Macie di un'organizzazione, puoi anche assegnare tag agli account dei membri della tua organizzazione.

Assegnando tag alle risorse Macie, puoi identificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Questo può aiutarti a eseguire attività come applicare politiche, allocare i costi, distinguere tra le risorse o identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità. Ad esempio, se si creano identificatori di dati personalizzati e processi di individuazione di dati sensibili per analizzare i dati in diversi punti di un flusso di lavoro (un set per i dati staged e un altro per i dati di produzione), è possibile assegnare una Stack chiave di tag a tali risorse. Il valore del tag per questa chiave di tag potrebbe riguardare Staging gli identificatori di dati personalizzati e i processi che analizzano i dati staged e per gli altri. Production

Quando definisci e assegni i tag alle risorse di Macie, tieni presente quanto segue:

- Ogni risorsa può avere un massimo di 50 tag.
- Per ogni risorsa, ogni chiave di tag deve essere unica e può avere un solo valore di tag.
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Come best practice, ti consigliamo di definire una strategia per utilizzare i tag in maiuscolo e di implementarla in modo coerente tra le tue risorse.
- Una chiave tag può contenere un massimo di 128 caratteri UTF-8. Il valore di un tag può contenere un massimo di 256 caratteri UTF-8. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: `_ . : / = + - @`
- Il `aws :` prefisso è riservato all'uso di AWS. Non puoi usarlo in nessuna chiave o valore di tag che definisci. Inoltre, non è possibile modificare o rimuovere le chiavi o i valori dei tag che utilizzano questo prefisso. I tag che utilizzano questo prefisso non vengono conteggiati nella quota di 50 tag per una risorsa.

- Tutti i tag che assegni sono disponibili solo per te Account AWS e solo nel gruppo Regione AWS in cui li assegni.
- Se si elimina una risorsa, vengono eliminati anche tutti i tag assegnati alla risorsa.

Per ulteriori restrizioni, suggerimenti e best practice, consulta la [Tagging AWS Resources User Guide](#).

 Important

Non archiviate dati riservati o di altro tipo nei tag. I tag sono accessibili da molti Servizi AWS, tra cui AWS Billing and Cost Management. Non sono destinati a essere utilizzati per dati sensibili.

Per aggiungere e gestire i tag per le risorse Macie, puoi usare Macie o. AWS Resource Groups AWS Resource Groups è un servizio progettato per aiutarti a raggruppare e gestire AWS le risorse come una singola unità anziché individualmente. Se usi Macie, puoi aggiungere tag a una risorsa quando la crei. Puoi anche aggiungere e gestire tag per singole risorse esistenti. Se lo utilizzi AWS Resource Groups, puoi aggiungere e gestire i tag in blocco per più risorse esistenti che si estendono su più risorse Servizi AWS, incluso Macie. Per ulteriori informazioni, consulta la sezione [Taggi AWS nella Guida all'uso delle risorse](#).

Aggiungere tag alle risorse Macie

Un tag è un'etichetta che puoi definire e assegnare alle AWS risorse, inclusi alcuni tipi di risorse Amazon Macie. Utilizzando i tag, puoi identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Ad esempio, puoi utilizzare i tag per: applicare politiche, allocare i costi, distinguere tra versioni delle risorse o identificare risorse che supportano determinati requisiti o flussi di lavoro di conformità.

Puoi aggiungere tag ai seguenti tipi di risorse Macie:

- Consenti elenchi
- Identificatori di dati personalizzati
- Regole di filtro e regole di soppressione per i risultati
- Lavori di individuazione di dati sensibili

Se sei l'amministratore Macie di un'organizzazione, puoi anche aggiungere tag agli account dei membri della tua organizzazione.

Una risorsa può avere fino a 50 tag. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Una chiave tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag. Per ulteriori informazioni sulle opzioni e sui requisiti di etichettatura, consulta [Nozioni fondamentali sull'etichettatura](#).

Puoi aggiungere tag alle risorse di Macie in diversi modi. Puoi usare direttamente Macie. Puoi anche utilizzare il Tag Editor sulla AWS Resource Groups console o le operazioni di tagging dell'API AWS Resource Groups Tagging. AWS Resource Groups è un servizio progettato per aiutarti a raggruppare e gestire AWS le risorse come una singola unità anziché individualmente. Se usi Macie, puoi aggiungere tag a una risorsa quando la crei. Puoi anche aggiungere tag a singole risorse esistenti. Con AWS Resource Groups, puoi aggiungere tag in blocco per più risorse esistenti che si estendono su più risorse Servizi AWS, incluso Macie.

Per aggiungere tag a una risorsa Macie

Per aggiungere tag a una singola risorsa Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Per aggiungere tag a più risorse Macie contemporaneamente, usa la AWS Resource Groups console o l'API Tagging. AWS Resource Groups Per ulteriori informazioni, consulta la sezione [Taggi AWS nella Guida all'uso delle risorse](#).

 Important

L'aggiunta di tag a una risorsa può influire sull'accesso alla risorsa. Prima di aggiungere un tag a una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare i tag per controllare l'accesso alle risorse. Per ulteriori informazioni, consulta [Controllo dell'accesso alle risorse AWS mediante i tag delle risorse](#) nella Guida per l'utente IAM.

Console

Quando crei un elenco di dati consentiti, un identificatore di dati personalizzato o un processo di rilevamento di dati sensibili, la console Amazon Macie offre opzioni per aggiungere tag alla risorsa. Segui le istruzioni sulla console per aggiungere tag a questi tipi di risorse al

momento della creazione delle risorse. Per aggiungere tag a una regola di filtro, a una regola di soppressione o a un account membro, devi creare la risorsa prima di poterti aggiungere tag.

Per aggiungere uno o più tag a una risorsa esistente utilizzando la console Amazon Macie, segui questi passaggi.

Per aggiungere un tag a una risorsa

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. A seconda del tipo di risorsa a cui desideri aggiungere un tag, esegui una delle seguenti operazioni:
 - Per un elenco consentito, scegli Consenti elenchi nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa all'elenco. Quindi scegli Gestisci tag nel menu Azioni.
 - Per un identificatore di dati personalizzato, scegli Identificatori di dati personalizzati nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo per l'identificatore di dati personalizzato. Quindi scegli Gestisci tag nel menu Azioni.
 - Per una regola di filtro o di soppressione, scegli Risultati nel riquadro di navigazione. Nell'elenco Regole salvate, scegliete l'icona di modifica  accanto alla regola. Scegli, quindi, Gestisci tag.
 - Per un account membro della tua organizzazione, scegli Account nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa all'account. Quindi scegli Gestisci tag nel menu Azioni.
 - Per un processo di rilevamento di dati sensibili, scegli Jobs nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa al lavoro. Quindi scegli Gestisci tag nel menu Azioni.

La finestra Gestisci tag elenca tutti i tag attualmente assegnati alla risorsa.

3. Nella finestra Gestisci tag, scegli Modifica tag.
4. Seleziona Aggiungi tag.
5. Nella casella Chiave, inserisci la chiave del tag da aggiungere alla risorsa. Quindi, nella casella Valore, inserite facoltativamente un valore di tag per la chiave.

Una chiave di tag può contenere fino a un massimo di 128 caratteri. Un valore di tag può contenere fino a un massimo di 256 caratteri. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: `_`:`/`= `+` `-` `@`

6. Per aggiungere un altro tag alla risorsa, scegliete **Aggiungi tag**, quindi ripetete il passaggio precedente. Puoi assegnare fino a 50 tag a una risorsa.
7. Quando hai finito di aggiungere i tag, scegli **Salva**.

API

Per creare una risorsa e aggiungervi uno o più tag a livello di codice, utilizzate l'Createoperazione appropriata per il tipo di risorsa che desiderate creare:

- Elenco consentiti: utilizza l'operazione. [CreateAllowList](#) Oppure, se stai usando il AWS Command Line Interface (AWS CLI), esegui il [create-allow-list](#) comando.
- Identificatore di dati personalizzato: utilizza l'[CreateCustomDataIdentifier](#) operazione. Oppure, se utilizzi il AWS CLI, esegui il [create-custom-data-identifier](#) comando.
- Regola di filtro o soppressione: utilizza l'[CreateFindingsFilter](#) operazione. Oppure, se utilizzi il AWS CLI, esegui il [create-findings-filter](#) comando.
- Account membro: utilizza l'[CreateMember](#) operazione. In alternativa, se utilizzi il AWS CLI, esegui il comando [create-member](#).
- Processo di rilevamento di dati sensibili: utilizza l'[CreateClassificationJob](#) operazione. Oppure, se utilizzi il AWS CLI, esegui il [create-classification-job](#) comando.

Nella richiesta, utilizzate il `tags` parametro per specificare la chiave del tag (`key`) e il valore del tag opzionale (`value`) per ogni tag da aggiungere alla risorsa. Il `tags` parametro specifica una string-to-string mappa delle chiavi dei tag e dei valori dei tag associati.

Per aggiungere uno o più tag a una risorsa esistente, utilizza l'[TagResource](#) operazione dell'API Amazon Macie o, se utilizzi la AWS CLI, esegui il comando [tag-resource](#). Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa a cui desideri aggiungere un tag. Utilizza il `tags` parametro per specificare il tag `key` (`key`) e il tag `value` opzionale (`value`) per ogni tag da aggiungere alla risorsa. Come nel caso delle `Create` operazioni e dei comandi, il `tags` parametro specifica una string-to-string mappa delle chiavi dei tag e dei valori dei tag associati.

Ad esempio, il AWS CLI comando seguente aggiunge una chiave di Stack tag con un valore di Production tag al processo specificato. Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={"Stack":"Production"}
```

Dove:

- **resource-arn** specifica l'ARN del lavoro a cui aggiungere un tag.
- **Stack** è la chiave del tag da aggiungere al lavoro.
- **Production** è il valore del tag per la chiave del tag specificata (**Stack**).

Nell'esempio seguente, il comando aggiunge diversi tag al job:

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={"Stack":"Production", "CostCenter":"12345", "Owner":"jane-doe"}
```

Per ogni tag in una tags mappa, sono obbligatori key sia gli value argomenti che. Tuttavia, il valore dell'valueargomento può essere una stringa vuota. Se non desiderate associare un valore di tag a una chiave di tag, non specificate un valore per l'valueargomento. Ad esempio, il AWS CLI comando seguente aggiunge una chiave di Owner tag senza alcun valore di tag associato:

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={"Owner":""}
```

Se un'operazione di tagging ha esito positivo, Macie restituisce una risposta HTTP 204 vuota. Altrimenti, Macie restituisce una risposta HTTP 4xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Controllo dell'accesso alle risorse di Macie tramite tag

Dopo aver iniziato a etichettare le risorse di Amazon Macie, puoi definire autorizzazioni basate su tag a livello di risorsa nelle policy (IAM). AWS Identity and Access Management Utilizzando i tag in questo modo, puoi implementare un controllo granulare su quali utenti e ruoli all'interno della tua azienda Account AWS sono autorizzati a creare ed etichettare le risorse Macie e quali utenti e ruoli sono autorizzati ad aggiungere, modificare e rimuovere tag più in generale. Per controllare l'accesso in base ai tag, puoi utilizzare le [chiavi di condizione relative ai tag](#) per Macie nell'elemento [Condition](#) delle politiche IAM.

Ad esempio, puoi creare una policy che consenta a un utente di avere pieno accesso a tutte le risorse Macie, se il Owner tag della risorsa specifica il suo nome utente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "macie2:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

Se vengono definite autorizzazioni a livello di risorsa basate su tag, le autorizzazioni diventano subito effettive. Ciò significa che le tue risorse sono più sicure non appena vengono create. Significa anche che puoi iniziare rapidamente a far rispettare l'uso dei tag per nuove risorse. È inoltre possibile utilizzare le autorizzazioni a livello di risorsa per controllare quali chiavi e valori di tag possono essere associati a risorse nuove ed esistenti. Per ulteriori informazioni, consulta [Controllare l'accesso alle AWS risorse utilizzando i tag](#) nella Guida per l'utente IAM.

Revisione e modifica dei tag per le risorse Macie

Man mano che il tuo ambiente o i tuoi requisiti cambiano nel tempo, puoi valutare i tag esistenti per le tue risorse Amazon Macie e modificarli se necessario. Un tag è un'etichetta che definisci e assegna a

una o più AWS risorse, inclusi determinati tipi di risorse Macie. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. Una chiave tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Ad esempio, puoi utilizzare i tag per: applicare politiche, allocare i costi, distinguere tra le versioni delle risorse o identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità.

Puoi assegnare tag ai seguenti tipi di risorse Macie:

- Consenti elenchi
- Identificatori di dati personalizzati
- Regole di filtro e regole di soppressione per i risultati
- Lavori di individuazione di dati sensibili

Se sei l'amministratore Macie di un'organizzazione, puoi anche assegnare tag agli account dei membri della tua organizzazione. Una risorsa può avere fino a 50 tag.

Argomenti

- [Revisione dei tag per le risorse Macie](#)
- [Modifica dei tag per le risorse Macie](#)

Revisione dei tag per le risorse Macie

Puoi esaminare i tag di una risorsa Amazon Macie utilizzando Macie o AWS Resource Groups. AWS Resource Groups è un servizio progettato per aiutarti a raggruppare e gestire AWS le risorse come una singola unità anziché individualmente. Se usi Macie, puoi controllare i tag di una risorsa alla volta. Con AWS Resource Groups, puoi rivedere i tag in blocco per più risorse esistenti che coprono più risorse, tra cui Macie. Servizi AWS

Per esaminare i tag di una risorsa Macie

Per esaminare i tag di una singola risorsa Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Per esaminare i tag di più risorse Macie contemporaneamente, utilizza il Tag Editor sulla AWS Resource Groups console o le operazioni di tagging dell'API Tagging. AWS Resource Groups Per ulteriori informazioni, consulta la sezione [Taggi AWS nella Guida all'uso delle risorse](#).

Console

Segui questi passaggi per esaminare i tag di una risorsa utilizzando la console Amazon Macie.

Per esaminare i tag di una risorsa

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. A seconda del tipo di risorsa di cui desideri esaminare i tag, esegui una delle seguenti operazioni:
 - Per un elenco consentito, scegli Consenti elenchi nel pannello di navigazione. Nella tabella, seleziona la casella di controllo relativa all'elenco. Quindi scegli Gestisci tag nel menu Azioni.
 - Per un identificatore di dati personalizzato, scegli Identificatori di dati personalizzati nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo per l'identificatore di dati personalizzato. Quindi scegli Gestisci tag nel menu Azioni.
 - Per una regola di filtro o di soppressione, scegli Risultati nel riquadro di navigazione. Nell'elenco Regole salvate, scegliete l'icona di modifica  accanto alla regola. Scegli, quindi, Gestisci tag.
 - Per un account membro della tua organizzazione, scegli Account nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa all'account. Quindi scegli Gestisci tag nel menu Azioni.
 - Per un processo di rilevamento di dati sensibili, scegli Jobs nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa al lavoro. Quindi scegli Gestisci tag nel menu Azioni.

La finestra Gestisci tag elenca tutti i tag attualmente assegnati alla risorsa. Ad esempio, l'immagine seguente mostra i tag assegnati a un identificatore di dati personalizzato.

Manage tags ✕

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Name: Former Surnames - Basic Latin

Key	Value
CostCenter	12345
Owner	-
Stack	Production

[Edit tags](#)

[Cancel](#) [Ok](#)

In questo esempio, all'identificatore di dati personalizzato vengono assegnati tre tag: la chiave CostCenter tag con 12345 come valore del tag associato, la chiave del tag Owner senza valore di tag associato (—) e la chiave del tag Stack con Production come valore del tag associato.

3. Al termine della revisione dei tag, scegli Annulla per chiudere la finestra.

API

Per recuperare e rivedere i tag di una risorsa esistente a livello di codice, puoi utilizzare l'Describeoperazione Get OR appropriata per il tipo di risorsa di cui desideri esaminare i tag. Ad esempio, se si utilizza l'[GetCustomDataIdentifier](#)operazione o si esegue il [get-custom-data-identifier](#)comando da AWS Command Line Interface (AWS CLI), la risposta include un oggetto. tags L'oggetto elenca tutti i tag (sia chiavi che valori dei tag) attualmente assegnati alla risorsa.

Puoi anche utilizzare il [ListTagsForResource](#)funzionamento dell'API Amazon Macie. Nella tua richiesta, utilizza il resourceArn parametro per specificare l'Amazon Resource Name (ARN) della risorsa. Se si utilizza il AWS CLI, eseguire il [list-tags-for-resource](#)comando e utilizzare il resource-arn parametro per specificare l'ARN della risorsa. Per esempio:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

Nell'esempio precedente, *arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample* è l'ARN di un processo di rilevamento di dati sensibili esistente.

Se l'operazione ha esito positivo, Macie restituisce un `tags` oggetto che elenca tutti i tag (sia le chiavi che i valori dei tag) attualmente assegnati alla risorsa. Per esempio:

```
{
  "tags": {
    "Stack": "Production",
    "CostCenter": "12345",
    "Owner": ""
  }
}
```

Dove `Stack`, `CostCenter`, e `Owner` sono le chiavi dei tag assegnate alla risorsa. `Production` è il valore del tag associato alla chiave del `Stack` tag. `12345` è il valore del tag associato alla chiave del `CostCenter` tag. La chiave `Owner` tag non ha un valore di tag associato.

Per recuperare un elenco di tutte le risorse Macie dotate di tag e di tutti i tag assegnati a ciascuna di tali risorse, utilizza il [GetResources](#) funzionamento dell'API AWS Resource Groups Tagging. Nella richiesta, imposta il valore del parametro su `ResourceTypeFilters macie2`. A tale scopo AWS CLI, eseguite il comando [get-resources](#) e impostate il valore del `resource-type-filters` parametro su `macie2`. Per esempio:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

Se l'operazione ha esito positivo, Resource Groups restituisce un `ResourceTagMappingList` array che contiene tutte le risorse Macie dotate ARNs di tag e le chiavi e i valori dei tag assegnati a ciascuna di tali risorse.

Modifica dei tag per le risorse Macie

Per modificare i tag (chiavi o valori dei tag) per una risorsa Amazon Macie, puoi usare Macie o AWS Resource Groups. Se usi Macie, puoi modificare i tag per una risorsa alla volta. Se lo usi AWS Resource Groups, puoi modificare i tag in blocco per più risorse esistenti che si estendono su più risorse, incluso Macie. Servizi AWS

Per modificare i tag di una risorsa Macie

Per modificare i tag per una singola risorsa Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. [Per modificare i tag per più risorse Macie contemporaneamente, utilizza il Tag Editor sulla AWS Resource Groups console o le operazioni di tagging dell'API Tagging.AWS Resource Groups](#)

 Important

La modifica dei tag di una risorsa può influire sull'accesso alla risorsa. Prima di modificare la chiave o il valore di un tag per una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse. Per ulteriori informazioni, consulta [Controlling access to AWS resources using tags](#) nella IAM User Guide.

Console

Segui questi passaggi per modificare i tag di una risorsa utilizzando la console Amazon Macie.

Per modificare i tag di una risorsa

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. A seconda del tipo di risorsa di cui desideri modificare i tag, esegui una delle seguenti operazioni:
 - Per un elenco consentito, scegli Consenti elenchi nel pannello di navigazione. Nella tabella, seleziona la casella di controllo relativa all'elenco. Quindi scegli Gestisci tag nel menu Azioni.
 - Per un identificatore di dati personalizzato, scegli Identificatori di dati personalizzati nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo per l'identificatore di dati personalizzato. Quindi scegli Gestisci tag nel menu Azioni.
 - Per una regola di filtro o di soppressione, scegli Risultati nel riquadro di navigazione. Nell'elenco Regole salvate, scegliete l'icona di modifica  accanto alla regola. Scegli, quindi, Gestisci tag.
 - Per un account membro della tua organizzazione, scegli Account nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa all'account. Quindi scegli Gestisci tag nel menu Azioni.

- Per un processo di rilevamento di dati sensibili, scegli Jobs nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa al lavoro. Quindi scegli Gestisci tag nel menu Azioni.

La finestra Gestisci tag elenca tutti i tag attualmente assegnati alla risorsa.

3. Nella finestra Gestisci tag, scegli Modifica tag.
4. Effettua una delle seguenti operazioni:
 - Per aggiungere un valore di tag a una chiave di tag, inserisci il valore nella casella Valore accanto alla chiave del tag.
 - Per modificare una chiave di tag esistente, scegliete Rimuovi accanto al tag. Quindi scegli Aggiungi tag. Nella casella Chiave che appare, inserisci la nuova chiave del tag. Facoltativamente, inserite un valore di tag associato nella casella Valore.
 - Per modificare il valore di un tag esistente, scegliete X nella casella Valore che contiene il valore. Quindi inserite il nuovo valore del tag nella casella Valore.
 - Per rimuovere un valore di tag esistente, scegliete X nella casella Valore che contiene il valore.
 - Per rimuovere un tag esistente (sia la chiave che il valore del tag), scegliete Rimuovi accanto al tag.

Una risorsa può avere fino a 50 tag. Una chiave di tag può contenere fino a un massimo di 128 caratteri. Un valore di tag può contenere fino a un massimo di 256 caratteri. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: `_./=: + - @`

5. Quando hai finito di modificare i tag, scegli Salva.

API

Quando modificate un tag per una risorsa a livello di codice, sovrascrivete il tag esistente con nuovi valori. Pertanto, il modo migliore per modificare un tag dipende dal fatto che si desideri modificare una chiave di tag, un valore di tag o entrambi. Per modificare una chiave di tag, [rimuovi il tag corrente](#) e [aggiungi un nuovo tag](#).

Per modificare o rimuovere solo il valore del tag associato a una chiave di tag, sovrascrivi il valore esistente utilizzando il [TagResource](#) funzionamento dell'API Amazon Macie. Se utilizzi AWS Command Line Interface (AWS CLI), puoi farlo eseguendo il comando [tag-resource](#). Nella

richiesta, specifica l'Amazon Resource Name (ARN) della risorsa di cui desideri modificare o rimuovere il valore del tag.

Per modificare il valore di un tag per una chiave di tag, usa il `tags` parametro per specificare la chiave di tag di cui desideri modificare il valore del tag e specifica il nuovo valore del tag per la chiave. Ad esempio, il comando seguente modifica il valore del tag da `Production` a `Staging` per la chiave di `Stack` tag assegnata al processo di rilevamento dei dati sensibili specificato. Questo esempio è formattato per Microsoft Windows e utilizza il carattere di continuazione di riga (^) per migliorare la leggibilità.

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={"Stack":"Staging"}
```

Dove:

- `resource-arn` specifica l'ARN del lavoro.
- **Stack** è la chiave del tag associata al valore del tag da modificare.
- **Staging** è il nuovo valore del tag per la chiave di tag specificata (**Stack**).

Per rimuovere un valore di tag da una chiave di tag, non specificate un valore per l'`value` argomento nel `tags` parametro. Per esempio:

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={"Stack":""}
```

Se l'operazione ha esito positivo, Macie restituisce una risposta HTTP 204 vuota. Altrimenti, Macie restituisce una risposta HTTP 4xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Rimozione dei tag dalle risorse di Macie

Se aggiungi tag a una risorsa Amazon Macie, puoi successivamente rimuoverne uno o più. Un tag è un'etichetta che definisci e assegni alle AWS risorse, inclusi determinati tipi di risorse Macie. Puoi

aggiungere, modificare e rimuovere tag dai seguenti tipi di risorse Macie: elenchi di autorizzazioni, identificatori di dati personalizzati, regole di filtro e regole di soppressione per i risultati, account membri di un'organizzazione e processi di rilevamento di dati sensibili.

È possibile rimuovere i tag da una risorsa Macie utilizzando Macie o AWS Resource Groups. AWS Resource Groups è un servizio progettato per aiutarti a raggruppare e gestire AWS le risorse come una singola unità anziché individualmente. Se usi Macie, puoi rimuovere i tag da una risorsa alla volta. Con AWS Resource Groups, puoi rimuovere i tag in blocco per più risorse esistenti che si estendono su più risorse, incluso Macie. Servizi AWS

Per rimuovere i tag da una risorsa Macie

Per rimuovere i tag da una risorsa Macie, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Per eseguire questa operazione per più risorse Macie contemporaneamente, utilizza il Tag Editor sulla AWS Resource Groups console o le operazioni di tagging dell'API Tagging. AWS Resource Groups Per ulteriori informazioni, consulta la [Tagging AWS](#) Resources User Guide.

Important

La rimozione di tag da una risorsa può influire sull'accesso alla risorsa. Prima di rimuovere un tag, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse. Per ulteriori informazioni, consulta [Controllo dell'accesso alle risorse AWS mediante i tag delle risorse](#) nella Guida per l'utente IAM.

Console

Segui questi passaggi per rimuovere uno o più tag da una risorsa utilizzando la console Amazon Macie.

Per rimuovere un tag da una risorsa

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. A seconda del tipo di risorsa da cui desideri rimuovere un tag, esegui una delle seguenti operazioni:
 - Per un elenco consentito, scegli Consenti elenchi nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa all'elenco. Quindi scegli Gestisci tag nel menu Azioni.

- Per un identificatore di dati personalizzato, scegli Identificatori di dati personalizzati nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo per l'identificatore di dati personalizzato. Quindi scegli Gestisci tag nel menu Azioni.
- Per una regola di filtro o di soppressione, scegli Risultati nel riquadro di navigazione. Nell'elenco Regole salvate, scegliete l'icona di modifica  accanto alla regola. Scegli, quindi, Gestisci tag.
- Per un account membro della tua organizzazione, scegli Account nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa all'account. Quindi scegli Gestisci tag nel menu Azioni.
- Per un processo di rilevamento di dati sensibili, scegli Jobs nel riquadro di navigazione. Nella tabella, seleziona la casella di controllo relativa al lavoro. Quindi scegli Gestisci tag nel menu Azioni.

La finestra Gestisci tag elenca tutti i tag attualmente assegnati alla risorsa.

3. Nella finestra Gestisci tag, scegli Modifica tag.
4. Effettua una delle seguenti operazioni:
 - Per rimuovere solo il valore del tag, scegli X nella casella Valore che contiene il valore da rimuovere.
 - Per rimuovere sia la chiave che il valore del tag (in coppia) per un tag, scegliete Rimuovi accanto al tag da rimuovere.
5. Per rimuovere tag aggiuntivi dalla risorsa, ripeti il passaggio precedente per ogni tag aggiuntivo da rimuovere.
6. Al termine della rimozione dei tag, scegli Salva.

API

Per rimuovere uno o più tag da una risorsa a livello di codice, utilizza il [UntagResource](#) funzionamento dell'API Amazon Macie. Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa da cui rimuovere un tag. Usa il `tagKeys` parametro per specificare la chiave del tag da rimuovere. Per rimuovere solo un valore di tag specifico (non una chiave di tag) da una risorsa, [modifica il tag](#) anziché rimuoverlo.

Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando [untag-resource](#) e usa il `resource-arn` parametro per specificare l'ARN della risorsa da cui rimuovere un tag. Utilizzate il `tag-keys` parametro per specificare la chiave del tag da rimuovere. Ad esempio, il comando seguente rimuove il `Stack` tag (sia la chiave del tag che il valore del tag) dal processo di rilevamento dei dati sensibili specificato:

```
C:\> aws macie2 untag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tag-keys Stack
```

Dove `resource-arn` specifica l'ARN del lavoro da cui rimuovere un tag **Stack** ed è la chiave del tag da rimuovere.

Per rimuovere più tag da una risorsa, aggiungete ogni chiave di tag aggiuntiva come argomento per il `tag-keys` parametro. Per esempio:

```
C:\> aws macie2 untag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tag-keys Stack Owner
```

Dove `resource-arn` specifica l'ARN del lavoro da cui rimuovere i tag **Stack** e **Owner** e sono le chiavi dei tag da rimuovere.

Se l'operazione ha esito positivo, Macie restituisce una risposta HTTP 204 vuota. Altrimenti, Macie restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Sicurezza in Macie

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS su Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per informazioni sui programmi di conformità applicabili ad Amazon Macie, consulta [AWS Services in Scope by Compliance Program](#) Program.
- **Sicurezza nel cloud:** la tua responsabilità è determinata dall'uso Servizi 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 ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon Macie. I seguenti argomenti mostrano come configurare Macie per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a usarne altri Servizi AWS che possono aiutarti a monitorare e proteggere le tue risorse Macie.

Argomenti

- [Protezione dei dati in Macie](#)
- [Gestione delle identità e degli accessi per Macie](#)
- [Convalida della conformità per Macie](#)
- [Resilienza a Macie](#)
- [Sicurezza dell'infrastruttura in Macie](#)
- [Accedere a Macie con un endpoint di interfaccia \(\)AWS PrivateLink](#)

Protezione dei dati in Macie

Il [modello di responsabilità AWS condivisa](#) si applica alla protezione dei dati in Amazon Macie.

Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center 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.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Macie o altri utenti che Servizi AWS utilizzano la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per 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.

Crittografia dei dati a riposo

Amazon Macie archivia in modo sicuro i dati archiviati utilizzando AWS soluzioni di crittografia. Macie crittografa i dati, come i risultati, utilizzando una chiave gestita da AWS form (). AWS Key Management Service AWS KMS

Se disabiliti Macie, elimina definitivamente tutte le risorse che archivia o gestisce per te, come i processi di rilevamento di dati sensibili, gli identificatori di dati personalizzati e i risultati.

Crittografia in transito

Amazon Macie crittografa tutti i dati in transito tra di loro. Servizi AWS

Macie analizza i dati da Amazon S3 ed esporta i risultati della scoperta di dati sensibili in un bucket S3 generico. Dopo che Macie ottiene le informazioni di cui ha bisogno dagli oggetti S3, gli oggetti vengono scartati.

Macie accede ad Amazon S3 utilizzando un endpoint VPC fornito da AWS PrivateLink. Pertanto, il traffico tra Macie e Amazon S3 rimane sulla rete Amazon e non passa attraverso la rete Internet pubblica. Per ulteriori informazioni, consulta [AWS PrivateLink](#).

Gestione delle identità e degli accessi per Macie

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Macie. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona Macie con AWS Identity and Access Management](#)
- [Esempi di politiche basate sull'identità per Macie](#)
- [AWS politiche gestite per Macie](#)

- [Utilizzo di ruoli collegati ai servizi per Macie](#)
- [Risoluzione dei problemi di gestione delle identità e degli accessi per Macie](#)

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in Macie.

Utente del servizio: se utilizzi il servizio Macie per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Macie per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Macie, consulta [Risoluzione dei problemi di gestione delle identità e degli accessi per Macie](#)

Amministratore del servizio: se sei responsabile delle risorse Macie della tua azienda, probabilmente hai pieno accesso a Macie. È tuo compito determinare a quali funzionalità e risorse di Macie devono accedere gli utenti del servizio. 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 saperne di più su come la tua azienda può utilizzare IAM con Macie, consulta [Come funziona Macie con AWS Identity and Access Management](#)

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a Macie. Per visualizzare esempi di policy basate sull'identità di Macie che puoi utilizzare in IAM, consulta [Esempi di politiche basate sull'identità per Macie](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta [Signature Version 4 AWS per le richieste API](#) nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\)AWS in IAM](#) nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 [Casi d'uso per utenti IAM](#) nella Guida per l'utente IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi [passare da un ruolo utente a un ruolo IAM \(console\)](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Create a role for a third-party identity provider \(federation\)](#) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.

- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso inoltrato (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon](#) nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'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 [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica della lista di controllo degli accessi \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente IAM.
- **Politiche di controllo del servizio (SCPs):** SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell'Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- **Politiche di controllo delle risorse (RCPs):** RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere [Resource control policies \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la [logica di valutazione delle policy](#) nella IAM User Guide.

Come funziona Macie con AWS Identity and Access Management

Prima di utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso ad Amazon Macie, scopri quali funzionalità IAM sono disponibili per l'uso con Macie.

Funzionalità IAM che puoi usare con Macie

Funzionalità IAM	Supporto per Macie
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi () ACLs	No
Controllo degli accessi basato sugli attributi (ABAC): tag nelle politiche	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per una panoramica di alto livello su come Macie e altri Servizi AWS funzionano con la maggior parte delle funzionalità IAM, consulta Servizi AWS la sezione dedicata alla compatibilità con IAM nella [IAM User Guide](#).

Politiche basate sull'identità per Macie

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le 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 [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

Amazon Macie supporta politiche basate sull'identità. Per alcuni esempi, consulta [Esempi di politiche basate sull'identità per Macie](#).

Politiche basate sulle risorse all'interno di Macie

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Amazon Macie non supporta politiche basate sulle risorse. Vale a dire, non è possibile collegare una policy direttamente a una risorsa Macie.

Azioni politiche per Macie

Supporta le operazioni di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni 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 azioni politiche per Amazon Macie utilizzano il seguente prefisso prima dell'azione:

```
macie2
```

Ad esempio, per concedere a qualcuno l'autorizzazione ad accedere alle informazioni su tutti gli identificatori di dati gestiti forniti da Macie, che è un'azione che corrisponde al `ListManagedDataIdentifiers` funzionamento dell'API Amazon Macie, includi `macie2:ListManagedDataIdentifiers` l'azione nella sua politica:

```
"Action": "macie2:ListManagedDataIdentifiers"
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Per esempio:

```
"Action": [  
    "macie2:ListManagedDataIdentifiers",  
    "macie2:ListCustomDataIdentifiers"  
]
```

Puoi anche specificare più operazioni utilizzando i caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

```
"Action": "macie2:List*"
```

Tuttavia, è consigliabile definire policy in grado di seguire il principio del privilegio minimo. In altre parole, è necessario creare policy che includano solo le autorizzazioni necessarie per eseguire un'attività specifica.

Per un elenco delle azioni Macie, consulta [Azioni definite da Amazon Macie](#) nel Service Authorization Reference. Per esempi di politiche che specificano le azioni di Macie, consulta. [Esempi di politiche basate sull'identità per Macie](#)

Risorse politiche per Macie

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `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 \(ARN\)](#). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni 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": "*"
```

Amazon Macie definisce i seguenti tipi di risorse:

- Elenco di indirizzi consentiti
- Identificatore dati personalizzato
- Regola di filtro o soppressione, nota anche come filtro dei risultati
- Account membro
- Processo di individuazione di dati sensibili, noto anche come processo di classificazione

È possibile specificare questi tipi di risorse nelle politiche utilizzando ARNs.

Ad esempio, per creare una policy per il processo di rilevamento di dati sensibili con l'ID di lavoro 3ce05dbb7ec5505def334104bexample, è possibile utilizzare il seguente ARN:

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

Oppure, per specificare tutti i processi di rilevamento di dati sensibili per un determinato account, utilizza un carattere jolly (*):

```
"Resource": "arn:aws:macie2:*:*:123456789012:classification-job/*"
```

123456789012 Dov'è l'ID dell'account Account AWS che ha creato i lavori. Tuttavia, è consigliabile creare politiche che seguano il principio del privilegio minimo. In altre parole, è necessario creare politiche che includano solo le autorizzazioni necessarie per eseguire un'attività specifica su una risorsa specifica.

Alcune azioni di Macie possono essere applicate a più risorse. Ad esempio, l'azione `macie2:BatchGetCustomDataIdentifier` può recuperare i dettagli di più identificatori di dati personalizzati. In questi casi, un principale deve disporre delle autorizzazioni per accedere a tutte le risorse a cui si applica l'azione. Per specificare più risorse in una singola istruzione, separale ARNs con una virgola:

```
"Resource": [  
  "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",  
  "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",  
  "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"  
]
```

Per un elenco dei tipi di risorse Macie e la sintassi ARN per ciascuno di essi, [consulta Tipi di risorse definiti da Amazon Macie nel Service Authorization Reference](#). Per sapere quali azioni è possibile specificare con ogni tipo di risorsa, consulta [Azioni definite da Amazon Macie](#) nel Service Authorization Reference. Per esempi di politiche che specificano le risorse, consulta [Esempi di politiche basate sull'identità per Macie](#).

Chiavi relative alle condizioni delle politiche per Macie

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. OR Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile 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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per un elenco delle chiavi di condizione di Amazon Macie, consulta [Condition keys for Amazon Macie](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Amazon Macie](#). Per esempi di politiche che utilizzano chiavi condizionali, consulta [Esempi di politiche basate sull'identità per Macie](#).

Accedi alle liste di controllo (ACLs) in Macie

Supporti ACLs: No

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) è un esempio di Servizio AWS supporto. ACLs Per ulteriori informazioni, consulta la [panoramica dell'elenco di controllo degli accessi \(ACL\)](#) nella Guida per l'utente di Amazon Simple Storage Service.

Amazon Macie non supporta. ACLs Vale a dire, non è possibile collegare un ACL a una risorsa Macie.

Controllo degli accessi basato sugli attributi (ABAC) con Macie

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Puoi allegare tag alle risorse Amazon Macie: elenchi di autorizzazioni, identificatori di dati personalizzati, regole di filtro e regole di soppressione, account dei membri e processi di rilevamento di dati sensibili. Puoi anche controllare l'accesso a questi tipi di risorse fornendo informazioni sui tag nell'elemento di una policy. `Condition` Per informazioni su come allegare tag alle risorse, consulta [Etichettare le risorse di Macie](#). Per un esempio di politica basata sull'identità che controlla l'accesso a una risorsa in base ai tag, vedi. [Esempi di politiche basate sull'identità per Macie](#)

Utilizzo di credenziali temporanee con Macie

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi usando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla [Servizi AWS compatibilità con IAM nella IAM](#) User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Passaggio da un ruolo utente a un ruolo IAM \(console\)](#) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API `or`. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Amazon Macie supporta l'uso di credenziali temporanee.

Sessioni di accesso diretto per Macie

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle

autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Amazon Macie invia richieste FAS a valle Servizi AWS quando esegui le seguenti attività:

- Crea o aggiorna le impostazioni di Macie per un elenco di contenuti consentiti archiviato in un bucket S3.
- Controlla lo stato di un elenco consentito archiviato in un bucket S3.
- Recupera campioni di dati sensibili da un oggetto S3 interessato utilizzando le credenziali utente IAM.
- Crittografa campioni di dati sensibili recuperati utilizzando le credenziali utente IAM o un ruolo IAM.
- Consenti a Macie di integrarsi con. AWS Organizations
- Designare l'account amministratore delegato Macie per un'organizzazione in. AWS Organizations

Per altre attività, Macie utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per informazioni dettagliate su questo ruolo, consulta. [Utilizzo di ruoli collegati ai servizi per Macie](#)

Ruoli di servizio per Macie

Supporta i ruoli di servizio: no

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Amazon Macie non assume né utilizza ruoli di servizio. Per eseguire azioni per tuo conto, Macie utilizza principalmente un ruolo collegato al servizio. Per informazioni dettagliate su questo ruolo, consulta. [Utilizzo di ruoli collegati ai servizi per Macie](#)

Ruoli collegati ai servizi per Macie

Supporta ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Amazon Macie utilizza un ruolo collegato al servizio per eseguire azioni per tuo conto. Per dettagli su questo ruolo, consulta [Utilizzo di ruoli collegati ai servizi per Macie](#)

Esempi di politiche basate sull'identità per Macie

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse Macie. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l'AWS API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Macie, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per Amazon Macie](#) nel Service Authorization Reference.

Quando crei una policy, assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti di AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) prima di salvare la policy. [IAM Access Analyzer esegue controlli sulle policy per convalidare una policy rispetto alla grammatica e alle best practice delle policy IAM](#). Questi controlli generano risultati e forniscono raccomandazioni attuabili per aiutarti a creare policy funzionali e conformi alle best practice di sicurezza. Per ulteriori informazioni sulla convalida delle policy utilizzando IAM Access Analyzer, consulta la convalida delle policy di [IAM Access Analyzer nella IAM User Guide](#). Per esaminare un elenco degli avvisi, degli errori e dei suggerimenti che IAM Access Analyzer può restituire, consulta il riferimento per il [controllo delle politiche di IAM Access Analyzer nella IAM User Guide](#).

Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console Amazon Macie](#)
- [Esempio: consentire agli utenti di rivedere le proprie autorizzazioni](#)
- [Esempio: consenti agli utenti di creare processi di rilevamento di dati sensibili](#)
- [Esempio: consentire agli utenti di gestire un processo di rilevamento di dati sensibili](#)
- [Esempio: consenti agli utenti di esaminare i risultati](#)

- [Esempio: consenti agli utenti di esaminare gli identificatori di dati personalizzati in base ai tag](#)

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse Macie nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Protezione dell'accesso API con MFA](#) nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo della console Amazon Macie

Per accedere alla console Amazon Macie, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Macie presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS AI contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano utilizzare la console Amazon Macie, crea policy IAM che forniscano loro l'accesso alla console. Per ulteriori informazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.

Se crei una policy che consente agli utenti o ai ruoli di utilizzare la console Amazon Macie, assicurati che la policy consenta l'azione `macie2:GetMacieSession`. In caso contrario, tali utenti o ruoli non saranno in grado di accedere alle risorse o ai dati Macie sulla console.

Assicurati inoltre che la policy consenta `macie2:List` le azioni appropriate per le risorse a cui tali utenti o ruoli devono accedere sulla console. In caso contrario, non saranno in grado di navigare o visualizzare i dettagli su tali risorse sulla console. Ad esempio, per esaminare i dettagli di un processo di rilevamento di dati sensibili utilizzando la console, a un utente deve essere consentito di eseguire l'azione `macie2:DescribeClassificationJob` relativa al lavoro e all'azione `macie2:ListClassificationJobs`. Se un utente non è autorizzato a eseguire l'azione `macie2:ListClassificationJobs`, non sarà in grado di visualizzare un elenco di lavori nella pagina Processi della console e pertanto non potrà scegliere il lavoro per visualizzarne i dettagli. Affinché i dettagli includano informazioni su un identificatore di dati personalizzato utilizzato dal processo, all'utente deve inoltre essere consentito di eseguire l'azione `macie2:BatchGetCustomDataIdentifiers` per l'identificatore di dati personalizzato.

Esempio: consentire agli utenti di rivedere le proprie autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica

include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam: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": "*"
    }
  ]
}
```

Esempio: consenti agli utenti di creare processi di rilevamento di dati sensibili

Questo esempio mostra come è possibile creare una politica che consenta a un utente di creare processi di rilevamento di dati sensibili.

Nell'esempio, la prima istruzione concede `macie2:CreateClassificationJob` le autorizzazioni all'utente. Queste autorizzazioni consentono all'utente di creare lavori. La dichiarazione concede

anche le `macie2:DescribeClassificationJob` autorizzazioni. Queste autorizzazioni consentono all'utente di accedere ai dettagli dei lavori esistenti. Sebbene queste autorizzazioni non siano necessarie per creare lavori, l'accesso a questi dettagli può aiutare l'utente a creare lavori con impostazioni di configurazione uniche.

La seconda istruzione dell'esempio consente all'utente di creare, configurare e rivedere i lavori utilizzando la console Amazon Macie. Le `macie2:ListClassificationJobs` autorizzazioni consentono all'utente di visualizzare i lavori esistenti nella pagina Lavori della console. Tutte le altre autorizzazioni contenute nell'istruzione consentono all'utente di configurare e creare un lavoro utilizzando le pagine Crea lavoro sulla console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndReviewJobs",
      "Effect": "Allow",
      "Action": [
        "macie2:CreateClassificationJob",
        "macie2:DescribeClassificationJob"
      ],
      "Resource": "arn:aws:macie2:*:*:classification-job/*"
    },
    {
      "Sid": "CreateAndReviewJobsOnConsole",
      "Effect": "Allow",
      "Action": [
        "macie2:ListClassificationJobs",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListManagedDataIdentifiers",
        "macie2:SearchResources",
        "macie2:DescribeBuckets"
      ],
      "Resource": "*"
    }
  ]
}
```


Esempio: consentire agli utenti di gestire un processo di rilevamento di dati sensibili

Questo esempio mostra come è possibile creare una politica che consenta a un utente di accedere ai dettagli di un particolare processo di rilevamento di dati sensibili, il lavoro il cui ID è `3ce05dbb7ec5505def334104bexample`. L'esempio consente inoltre all'utente di modificare lo stato del job, se necessario.

La prima istruzione dell'esempio concede `macie2:DescribeClassificationJob` e `macie2:UpdateClassificationJob` autorizzazioni all'utente. Queste autorizzazioni consentono all'utente di recuperare rispettivamente i dettagli del lavoro e modificarne lo stato. La seconda istruzione concede `macie2:ListClassificationJobs` le autorizzazioni all'utente, il che consente all'utente di accedere al lavoro utilizzando la pagina Lavori sulla console Amazon Macie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageOneJob",
      "Effect": "Allow",
      "Action": [
        "macie2:DescribeClassificationJob",
        "macie2:UpdateClassificationJob"
      ],
      "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
    },
    {
      "Sid": "ListJobsOnConsole",
      "Effect": "Allow",
      "Action": "macie2:ListClassificationJobs",
      "Resource": "*"
    }
  ]
}
```

Puoi anche consentire all'utente di accedere ai dati di registrazione (eventi di registro) che Macie pubblica su Amazon CloudWatch Logs per il lavoro. A tale scopo, puoi aggiungere istruzioni che concedono le autorizzazioni per eseguire azioni CloudWatch Logs (logs) sul gruppo di log e sullo stream per il processo. Per esempio:

```
"Statement": [
```

```
{
  "Sid": "AccessLogGroupForMacieJobs",
  "Effect": "Allow",
  "Action": [
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams"
  ],
  "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
},
{
  "Sid": "AccessLogEventsForOneMacieJob",
  "Effect": "Allow",
  "Action": "logs:GetLogEvents",
  "Resource": [
    "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
    "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-stream:3ce05dbb7ec5505def334104bexample"
  ]
}
]
```

Per informazioni sulla gestione dell'accesso ai CloudWatch log, consulta [Panoramica della gestione delle autorizzazioni di accesso alle risorse Logs nella Amazon CloudWatch CloudWatch Logs](#) User Guide.

Esempio: consenti agli utenti di esaminare i risultati

Questo esempio mostra come è possibile creare una politica che consenta a un utente di accedere ai dati dei risultati.

In questo esempio, le `macie2:GetFindingStatistics` autorizzazioni `macie2:GetFindings` and consentono all'utente di recuperare i dati utilizzando l'API Amazon Macie o la console Amazon Macie. Le `macie2:ListFindings` autorizzazioni consentono all'utente di recuperare e rivedere i dati utilizzando la dashboard di riepilogo e le pagine Findings sulla console Amazon Macie.

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

```

        "macie2:GetFindings",
        "macie2:GetFindingStatistics",
        "macie2:ListFindings"
    ],
    "Resource": "*"
}
]
}

```

Puoi anche consentire all'utente di creare e gestire regole di filtro e regole di soppressione per i risultati. A tale scopo, è possibile includere un'istruzione che conceda le seguenti autorizzazioni: `macie2:CreateFindingsFilter`, `macie2:GetFindingsFilter`, `macie2:UpdateFindingsFilter` e `macie2>DeleteFindingsFilter`. Per consentire all'utente di gestire le regole utilizzando la console Amazon Macie, includi anche `macie2:ListFindingsFilters` le autorizzazioni nella policy. Per esempio:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewFindings",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindings",
        "macie2:GetFindingStatistics",
        "macie2:ListFindings"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ManageRules",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindingsFilter",
        "macie2:UpdateFindingsFilter",
        "macie2:CreateFindingsFilter",
        "macie2>DeleteFindingsFilter"
      ],
      "Resource": "arn:aws:macie2:*:*:findings-filter/*"
    },
    {
      "Sid": "ListRulesOnConsole",

```

```

        "Effect": "Allow",
        "Action": "macie2:ListFindingsFilters",
        "Resource": "*"
    }
]
}

```

Esempio: consenti agli utenti di esaminare gli identificatori di dati personalizzati in base ai tag

Nelle politiche basate sull'identità, puoi utilizzare le condizioni per controllare l'accesso alle risorse di Amazon Macie in base ai tag. Questo esempio mostra come creare una policy che consenta a un utente di esaminare gli identificatori di dati personalizzati utilizzando la console Amazon Macie o l'API Amazon Macie. Tuttavia, l'autorizzazione viene concessa solo se il valore del Owner tag è il nome utente dell'utente.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewCustomDataIdentifiersIfOwner",
      "Effect": "Allow",
      "Action": "macie2:GetCustomDataIdentifier",
      "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    },
    {
      "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
      "Effect": "Allow",
      "Action": "macie2:ListCustomDataIdentifiers",
      "Resource": "*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}

```

In questo esempio, se un utente con il nome utente `richard-roe` tenta di esaminare i dettagli di un identificatore di dati personalizzato, l'identificatore di dati personalizzato deve essere contrassegnato

con `Owner=richard-roe` o `owner=richard-roe`. In caso contrario, a questo utente viene negato l'accesso. La chiave del tag `condition Owner` corrisponde a entrambi `Owner` e `owner` perché i nomi delle chiavi di condizione non fanno distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.

AWS politiche gestite per Macie

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

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Amazon Macie fornisce diverse policy AWS gestite: la `AmazonMacieFullAccess` policy, la `AmazonMacieReadOnlyAccess` policy e la `AmazonMacieServiceRolePolicy` policy.

Politiche e aggiornamenti

- [AWS politica gestita: AmazonMacieFullAccess](#)
- [AWS politica gestita: AmazonMacieReadOnlyAccess](#)
- [AWS politica gestita: AmazonMacieServiceRolePolicy](#)
- [Aggiornamenti alle politiche AWS gestite per Macie](#)

AWS politica gestita: AmazonMacieFullAccess

Puoi collegare la policy AmazonMacieFullAccess anche alle tue entità IAM.

Questa policy concede autorizzazioni amministrative complete che consentono a un'identità IAM (principale) di creare il ruolo [collegato al servizio Amazon Macie](#) ed eseguire tutte le azioni di lettura e scrittura per Amazon Macie. Le autorizzazioni includono funzioni mutanti come creazione, aggiornamento ed eliminazione. Se questa politica è associata a un'entità, quest'ultima può creare, recuperare e accedere in altro modo a tutte le risorse, i dati e le impostazioni di Macie per il proprio account.

Questa politica deve essere associata a un'entità prima che quest'ultima possa abilitare Macie per il proprio account. Una persona principale deve essere autorizzata a creare il ruolo collegato al servizio Macie per abilitare Macie per il proprio account.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- **macie2**— Consente ai mandanti di eseguire tutte le azioni di lettura e scrittura per Amazon Macie.
- **iam**— Consente ai dirigenti di creare ruoli collegati ai servizi. L'**Resourceelemento** specifica il ruolo collegato al servizio per Macie. L'**Conditionelemento** utilizza la [chiave di `iam:AWSServiceName` condizione](#) e l'[operatore di `StringLike` condizione](#) per limitare le autorizzazioni al ruolo collegato al servizio per Macie.
- **pricing**— Consente ai mandanti di recuperare i dati sui prezzi da loro. Account AWS AWS Billing and Cost Management Macie utilizza questi dati per calcolare e visualizzare i costi stimati quando i responsabili creano e configurano lavori di rilevamento di dati sensibili.

Per esaminare le autorizzazioni relative a questa politica, consulta [AmazonMacieFullAccess](#) la AWS Managed Policy Reference Guide.

AWS politica gestita: AmazonMacieReadOnlyAccess

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

Questa policy concede autorizzazioni di sola lettura che consentono a un'identità IAM (principale) di eseguire tutte le azioni di lettura per Amazon Macie. Le autorizzazioni non includono funzioni mutanti come la creazione, l'aggiornamento o l'eliminazione. Se questa policy è associata a un'entità, quest'ultima può recuperare ma non accedere in altro modo a tutte le risorse, i dati e le impostazioni di Macie per il proprio account.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

`macie2`— Consente ai mandanti di eseguire tutte le azioni di lettura per Amazon Macie.

Per esaminare le autorizzazioni relative a questa politica, consulta [AmazonMacieReadOnlyAccess](#) la AWS Managed Policy Reference Guide.

AWS politica gestita: `AmazonMacieServiceRolePolicy`

Non è possibile allegare la policy `AmazonMacieServiceRolePolicy` alle entità IAM.

Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon Macie di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Macie](#).

Per esaminare le autorizzazioni relative a questa politica, consulta la AWS Managed Policy [AmazonMacieServiceRolePolicy](#) Reference Guide.

Aggiornamenti alle politiche AWS gestite per Macie

La tabella seguente fornisce dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon Macie da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sugli aggiornamenti delle politiche, iscriviti al feed RSS nella pagina della cronologia dei documenti di [Macie](#).

Modifica	Descrizione	Data
AmazonMacieReadOnlyAccess — Aggiunta una nuova politica	Macie ha aggiunto una nuova politica, la AmazonMacieReadOnlyAccess politica. Questa politica concede autorizzazioni di sola lettura che consentono ai responsabili di recuperare e tutte le risorse, i dati e le impostazioni di Macie per il proprio account.	15 giugno 2023
AmazonMacieFullAccess — Aggiornamento di una politica esistente	Nella AmazonMacieFullAccess policy, Macie ha aggiornato l'Amazon Resource Name (ARN) del ruolo Macie collegato al servizio (). <code>aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie</code>	30 giugno 2022
AmazonMacieServiceRolePolicy — Ha aggiornato una policy esistente	Macie ha rimosso azioni e risorse per Amazon Macie Classic dalla AmazonMacieServiceRolePolicy policy. Amazon Macie Classic non è più disponibile e non è più disponibile. Più specificamente, Macie ha rimosso tutte le azioni. AWS CloudTrail Macie ha inoltre rimosso tutte le azioni di Amazon S3 per le	20 maggio 2022

Modifica	Descrizione	Data
	seguenti risorse <code>arn:aws:s3:::awsmacie-*</code>, <code>arn:aws:s3:::awsmacietrail-*</code>, e <code>arn:aws:s3:::*-awsmacietrail-*</code>.	
AmazonMacieFullAccess— Ha aggiornato una politica esistente	Macie ha aggiunto un'azione AWS Billing and Cost Management (pricing) alla <code>AmazonMacieFullAccess</code> policy. Questa azione consente ai mandanti di recuperare i dati sui prezzi del proprio account. Macie utilizza questi dati per calcolare e visualizzare i costi stimati quando i responsabili creano e configurano lavori di rilevamento di dati sensibili. Macie ha inoltre rimosso le azioni di Amazon Macie Classic (<code>macie</code>) dalla <code>AmazonMacieFullAccess</code> policy.	7 marzo 2022

Modifica	Descrizione	Data
AmazonMacieServiceRolePolicy — Ha aggiornato una politica esistente	Macie ha aggiunto le azioni di Amazon CloudWatch Logs alla AmazonMacieServiceRolePolicy policy. Queste azioni consentono a Macie di pubblicare eventi di registro su CloudWatch Logs per lavori di rilevamento di dati sensibili.	13 aprile 2021
Macie ha iniziato a tenere traccia delle modifiche	Macie ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	13 aprile 2021

Utilizzo di ruoli collegati ai servizi per Macie

Amazon Macie utilizza un ruolo collegato al [servizio AWS Identity and Access Management \(IAM\) denominato](#) `AWSServiceRoleForAmazonMacie`. Questo ruolo collegato al servizio è un ruolo IAM collegato direttamente a Macie. È predefinito da Macie e include tutte le autorizzazioni necessarie a Macie per chiamare altri Servizi AWS utenti e monitorare le risorse per tuo conto. AWS Macie utilizza questo ruolo collegato al servizio in tutti i luoghi in cui Macie è disponibile. Regioni AWS

Un ruolo collegato al servizio semplifica la configurazione di Macie perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Macie definisce le autorizzazioni di questo ruolo collegato al servizio e, se non diversamente definito, solo Macie può assumere il ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli un Sì con un link per consultare la documentazione del ruolo collegato al servizio per quel servizio.

Argomenti

- [Autorizzazioni di ruolo collegate al servizio per Macie](#)

- [Creazione del ruolo collegato al servizio per Macie](#)
- [Modifica del ruolo collegato al servizio per Macie](#)
- [Eliminazione del ruolo collegato al servizio per Macie](#)
- [Supportato Regioni AWS per il ruolo Macie collegato al servizio](#)

Autorizzazioni di ruolo collegate al servizio per Macie

Amazon Macie utilizza il ruolo collegato al servizio denominato.

`AWSServiceRoleForAmazonMacie` Questo ruolo collegato al servizio si fida che il servizio assuma il `macie.amazonaws.com` ruolo.

La politica di autorizzazione per il ruolo, che è denominato `AmazonMacieServiceRolePolicy`, consente a Macie di eseguire attività come le seguenti sulle risorse specificate:

- Utilizzare le operazioni di Amazon S3 per recuperare informazioni su bucket e oggetti S3.
- Usa le azioni di Amazon S3 per recuperare oggetti S3.
- Utilizza AWS Organizations le azioni per recuperare informazioni sugli account associati.
- Usa le azioni di Amazon CloudWatch Logs per registrare gli eventi per i lavori di rilevamento di dati sensibili.

Per esaminare le autorizzazioni relative a questa politica, consulta [AmazonMacieServiceRolePolicy](#) la AWS Managed Policy Reference Guide.

Per dettagli sugli aggiornamenti a questa politica, consulta [Aggiornamenti alle politiche AWS gestite per Macie](#). Per avvisi automatici sulle modifiche a questa politica, iscriviti al feed RSS nella pagina della cronologia dei [documenti di Macie](#).

È necessario configurare le autorizzazioni per un'entità IAM (come un utente o un ruolo) per consentire all'entità di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione del ruolo collegato al servizio per Macie

Non è necessario creare manualmente il ruolo `AWSServiceRoleForAmazonMacie` collegato al servizio per Amazon Macie. Quando abiliti Macie per il tuo account Account AWS, Macie crea automaticamente il ruolo collegato al servizio per te.

Se elimini il ruolo Macie collegato al servizio e poi devi crearlo di nuovo, puoi utilizzare la stessa procedura per ricreare il ruolo nel tuo account. Quando abiliti nuovamente Macie, Macie crea nuovamente il ruolo collegato al servizio per te.

Modifica del ruolo collegato al servizio per Macie

Amazon Macie non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonMacie` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché diverse entità potrebbero fare riferimento al ruolo. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Aggiornamento di un ruolo collegato ai servizi nella Guida](#) per l'utente IAM.

Eliminazione del ruolo collegato al servizio per Macie

È possibile eliminare un ruolo collegato al servizio solo dopo aver eliminato le relative risorse. Questa procedura protegge le risorse di perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Se non hai più bisogno di utilizzare Amazon Macie, ti consigliamo di eliminare manualmente il ruolo collegato al `AWSServiceRoleForAmazonMacie` servizio. Quando disabiliti Macie, Macie non elimina il ruolo per te.

Prima di eliminare il ruolo, devi disabilitare Macie in ogni posizione in Regione AWS cui lo hai abilitato. È inoltre necessario pulire manualmente le risorse per il ruolo. Per eliminare il ruolo, puoi utilizzare la console IAM AWS CLI, o l' AWS API. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Note

Se Macie utilizza il `AWSServiceRoleForAmazonMacie` ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In tal caso, attendi qualche minuto e poi riprova a eseguire l'operazione.

Se elimini il ruolo `AWSServiceRoleForAmazonMacie` collegato al servizio e devi crearlo di nuovo, puoi crearlo di nuovo abilitando Macie per il tuo account. Quando abiliti nuovamente Macie, Macie crea nuovamente il ruolo collegato al servizio per te.

Supportato Regioni AWS per il ruolo Macie collegato al servizio

Amazon Macie supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonMacie` collegato al servizio in tutti i paesi in Regioni AWS cui Macie è disponibile. Per un elenco delle regioni in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

Risoluzione dei problemi di gestione delle identità e degli accessi per Macie

Le seguenti informazioni possono aiutarti a diagnosticare e risolvere problemi comuni che potresti riscontrare quando lavori con Amazon Macie AWS Identity and Access Management e (IAM).

Argomenti

- [Non sono autorizzato a eseguire un'azione in Macie](#)
- [Voglio consentire a persone esterne a me Account AWS di accedere alle mie risorse Macie](#)

Non sono autorizzato a eseguire un'azione in Macie

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *my-example-widget* fittizia ma non dispone di autorizzazioni `macie2:GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
macie2:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *my-example-widget* utilizzando l'azione `macie2:GetWidget`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me Account AWS di accedere alle mie risorse Macie

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Macie supporta queste funzionalità, consulta [Come funziona Macie con AWS Identity and Access Management](#)
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Convalida della conformità per Macie

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta [Servizi AWS Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Governance e conformità per la sicurezza](#): queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- [Riferimenti sui servizi conformi ai requisiti HIPAA](#): elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.

- [AWS Risorse per](#) la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- [Valutazione delle risorse con regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza a Macie

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. 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 tradizionali. Per ulteriori informazioni sulle zone Regioni AWS di disponibilità, vedere [AWS Global Infrastructure](#).

Oltre all'infrastruttura AWS globale, Amazon Macie offre diverse funzionalità per supportare le tue esigenze di resilienza e backup dei dati. Ad esempio, quando esegui un processo di rilevamento di dati sensibili o Macie esegue un rilevamento automatico di dati sensibili, Macie crea automaticamente un record di analisi per ogni oggetto Amazon Simple Storage Service (Amazon S3) incluso

nell'ambito dell'analisi. Questi record, denominati risultati di scoperta di dati sensibili, registrano dettagli sull'analisi che Macie esegue su singoli oggetti S3. Ciò include oggetti in cui Macie non rileva dati sensibili e oggetti che Macie non può analizzare a causa di errori o problemi. Macie archivia questi risultati in un bucket S3 specificato dall'utente. Per ulteriori informazioni, consulta [Archiviazione e mantenimento dei risultati di rilevamento dei dati sensibili](#).

Macie pubblica anche i risultati relativi alle politiche e ai dati sensibili su Amazon sotto EventBridge forma di eventi. Ciò include nuove scoperte e aggiornamenti ai risultati delle politiche esistenti. (Non include i risultati che vengono archiviati automaticamente utilizzando le regole di soppressione). Utilizzando EventBridge, puoi inviare i dati dei risultati alla tua piattaforma di storage preferita e archivarli per tutto il tempo che desideri. A seconda delle impostazioni di pubblicazione scelte, Macie può anche pubblicare i risultati delle policy e dei dati sensibili su AWS Security Hub. Per ulteriori informazioni, consulta [Monitoraggio ed elaborazione dei risultati](#).

Hai anche la possibilità di utilizzare le operazioni dell'API Macie per recuperare i risultati e altri tipi di dati in modo programmatico. È quindi possibile elaborare e inviare i dati alla piattaforma di archiviazione preferita o a un altro servizio, applicazione o sistema. Per informazioni sulle operazioni API che potresti utilizzare a tale scopo, consulta [Amazon Macie API](#) Reference.

Sicurezza dell'infrastruttura in Macie

In quanto servizio gestito, Amazon Macie è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Macie attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi chiamare queste operazioni API da una qualsiasi posizione di rete. Tuttavia, se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi stabilire una connessione privata tra il tuo VPC e Macie creando un endpoint di interfaccia. Gli endpoint di interfaccia sono alimentati da [AWS PrivateLink](#), una tecnologia che consente di accedere privatamente a Macie senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Creiamo un'interfaccia di rete endpoint in ogni sottorete abilitata per un endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che possono fungere da punto di ingresso per il traffico destinato a Macie. Per ulteriori informazioni, consulta la sezione [Accesso a Servizi AWS tramite AWS PrivateLink](#) nella Guida di AWS PrivateLink .

Accedere a Macie con un endpoint di interfaccia ()AWS PrivateLink

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo cloud privato virtuale (VPC) e Amazon Macie. Puoi accedere a Macie come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere a Macie.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato a Macie.

Per ulteriori informazioni, consulta la sezione [Accesso a Servizi AWS tramite AWS PrivateLink](#) nella Guida di AWS PrivateLink .

Argomenti

- [Considerazioni sugli endpoint dell'interfaccia Macie](#)
- [Creazione di un endpoint di interfaccia per Macie](#)
- [Creazione di una policy per gli endpoint per Macie](#)

Considerazioni sugli endpoint dell'interfaccia Macie

Amazon Macie supporta gli endpoint di interfaccia in tutti i paesi in Regioni AWS cui è attualmente disponibile. Per un elenco di queste regioni, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS Macie supporta le chiamate a tutte le sue operazioni API tramite endpoint di interfaccia.

Se crei un endpoint di interfaccia per Macie, valuta la possibilità di fare lo stesso per altri dispositivi Servizi AWS che si integrano con Macie e con AWS PrivateLink, ad esempio, Amazon e. EventBridge AWS Security Hub Macie e questi servizi possono quindi utilizzare gli endpoint dell'interfaccia per l'integrazione. Ad esempio, se crei un endpoint di interfaccia per Macie e un endpoint di interfaccia per Security Hub, Macie può utilizzare il suo endpoint di interfaccia quando pubblica i risultati su Security Hub. Security Hub può utilizzare il suo endpoint di interfaccia quando riceve i risultati. Per informazioni sui servizi supportati, consulta [Servizi AWS la sezione dedicata all'integrazione con AWS PrivateLink](#) nella AWS PrivateLink Guida.

Creazione di un endpoint di interfaccia per Macie

Puoi creare un endpoint di interfaccia per Amazon Macie utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint VPC](#) nella Guida di AWS PrivateLink .

Quando crei un endpoint di interfaccia per Macie, usa il seguente nome di servizio:

`com.amazonaws.region.macie2`

region Dov'è il codice regionale applicabile. Regione AWS

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API a Macie utilizzando il nome DNS regionale predefinito, ad esempio `macie2.us-east-1.amazonaws.com` per la regione Stati Uniti orientali (Virginia settentrionale).

Creazione di una policy per gli endpoint per Macie

Una policy per gli endpoint è una risorsa AWS Identity and Access Management (IAM) che puoi collegare a un endpoint di interfaccia. La policy predefinita per gli endpoint consente l'accesso completo ad Amazon Macie tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito a Macie dal tuo VPC, collega una policy endpoint personalizzata all'endpoint dell'interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Si tratta di una policy separata per controllare l'accesso dall'endpoint al servizio specificato. Per ulteriori informazioni, consulta [Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint](#) nella Guida.AWS PrivateLink

Esempio: policy degli endpoint VPC per le azioni di Macie

Di seguito è riportato un esempio di policy personalizzata per gli endpoint per Macie. Se colleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni Macie elencate per tutti i principali su tutte le risorse. Consente agli utenti che si connettono a Macie tramite il VPC di accedere ai dati dei risultati utilizzando l'API Amazon Macie.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindings",
        "macie2:GetFindingStatistics",
        "macie2:ListFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Per consentire inoltre agli utenti di accedere ai dati dei risultati o eseguire altre azioni utilizzando la console Amazon Macie, la policy dovrebbe anche concedere l'accesso all'`macie2:GetMacieSessionazione`, ad esempio:

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "macie2:GetMacieSession",
        "macie2:GetFindings",
        "macie2:GetFindingStatistics",
        "macie2:ListFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}  
  ]  
}
```

Registrazione delle chiamate all'API Macie con AWS CloudTrail

Amazon Macie si integra con [AWS CloudTrail](#), un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un. Servizio AWS CloudTrail acquisisce tutte le chiamate API per Macie come eventi di gestione. Le chiamate acquisite includono chiamate dalla console Amazon Macie e chiamate programmatiche alle operazioni dell'API Amazon Macie. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Macie, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

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 root o utente.
- Se la richiesta è stata effettuata per conto di un AWS IAM Identity Center utente.
- 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.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente AWS CloudTrail. Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrail Lake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella

Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail [Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC](#). ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail](#)

Eventi manageriali di Macie in AWS CloudTrail

[Gli eventi](#) di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse di Account AWS Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Amazon Macie registra tutte le operazioni del piano di controllo Macie come eventi di gestione. CloudTrail Ad esempio, le chiamate a `ListFindingsDescribeBuckets`, e le `CreateClassificationJob` operazioni generano eventi di gestione in. CloudTrail Ogni evento include un `eventSource` campo. Questo campo indica Servizio AWS il destinatario della richiesta. Per gli eventi Macie, il valore di questo campo è: `macie2.amazonaws.com`.

Per un elenco delle operazioni del piano di controllo a cui Macie accede CloudTrail, consulta [Operazioni](#) nell'Amazon Macie API Reference.

Esempi di eventi Macie in AWS CloudTrail

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Gli esempi seguenti mostrano CloudTrail eventi che dimostrano il funzionamento di Amazon Macie. Per i dettagli sulle informazioni che un evento potrebbe contenere, consulta il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

Esempio: elenco dei risultati

L'esempio seguente mostra un CloudTrail evento per l'operazione Amazon Macie [ListFindings](#). In questo esempio, un utente AWS Identity and Access Management (IAM) (Mary_Major) ha utilizzato la console Amazon Macie per recuperare un sottoinsieme di informazioni sui risultati delle politiche correnti per il proprio account.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "attributes": {
        "creationdate": "2023-11-14T15:49:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-11-14T16:09:56Z",
  "eventSource": "macie2.amazonaws.com",
  "eventName": "ListFindings",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36",
  "requestParameters": {
```

```
    "sortCriteria": {
      "attributeName": "updatedAt",
      "orderBy": "DESC"
    },
    "findingCriteria": {
      "criterion": {
        "archived": {
          "eq": [
            "false"
          ]
        },
        "category": {
          "eq": [
            "POLICY"
          ]
        }
      }
    },
    "maxResults": 25,
    "nextToken": ""
  },
  "responseElements": null,
  "requestID": "d58af6be-1115-4a41-91f8-ace03example",
  "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}
```

Esempio: recupero di campioni di dati sensibili per una scoperta

Questo esempio mostra CloudTrail gli eventi per il recupero e la rivelazione di campioni di dati sensibili segnalati da Amazon Macie in un risultato. In questo esempio, un utente AWS Identity and Access Management (IAM) (JohnDoe) ha utilizzato la console Amazon Macie per recuperare e rivelare campioni di dati sensibili. L'account dell'utente è configurato per assumere un ruolo IAM (MacieReveal) per recuperare e rivelare campioni di dati sensibili dagli oggetti Amazon Simple Storage Service (Amazon S3) interessati.

L'evento seguente mostra i dettagli sulla richiesta dell'utente di recuperare e rivelare campioni di dati sensibili eseguendo l'operazione Amazon [GetSensitiveDataOccurrences](#) Macie.


```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "UU4MH70YK5ZCOAEXAMPLE:JohnDoe",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "UU4MH70YK5ZCOAEXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-12-12T14:40:23Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-12-12T17:04:47Z",
  "eventSource": "macie2.amazonaws.com",
  "eventName": "GetSensitiveDataOccurrences",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "198.51.100.252",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.0.0 Safari/537.36",
  "requestParameters": {
    "findingId": "3ad9d8cd61c5c390bede45cd2example"
  },
  "responseElements": null,
  "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
  "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

L'evento successivo mostra i dettagli su come Macie assuma il ruolo IAM specificato (MacieReveal) eseguendo l' AWS Security Token Service operazione ([AssumeRole](#)).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "reveal-samples.macie.amazonaws.com"
  },
  "eventTime": "2023-12-12T17:04:47Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
  "userAgent": "reveal-samples.macie.amazonaws.com",
  "requestParameters": {
    "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
    "roleSessionName": "RevealCrossAccount"
  },
  "responseElements": {
    "credentials": {
      "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
      "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
      "expiration": "Dec 12, 2023, 6:04:47 PM"
    },
    "assumedRoleUser": {
      "assumedRoleId": "AROAX0TKAR0CSNEXAMPLE:RevealCrossAccount",
      "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
    }
  },
  "requestID": "d905cea8-2dc8-44c1-948e-19419example",
  "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::IAM::Role",
      "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
    }
  ],
}
```

```
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "111122223333",  
"eventCategory": "Management"  
}
```

Per informazioni sul contenuto degli CloudTrail eventi, consultate il [contenuto dei CloudTrail record nella Guida](#) per l'AWS CloudTrail utente.

Creazione di risorse Macie con AWS CloudFormation

Amazon Macie si integra con [AWS CloudFormation](#), un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come identificatori di dati personalizzati) e fornisce e AWS CloudFormation configura tali risorse per te.

Quando lo usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Macie in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS e. Regioni AWS

Macie e modelli AWS CloudFormation

Per fornire e configurare le risorse per Amazon Macie e i servizi correlati, devi conoscere AWS CloudFormation i modelli. I modelli descrivono le risorse che desideri fornire nei tuoi AWS CloudFormation stack. Sono file di testo in formato JSON o YAML. Se non conosci JSON o YAML, AWS Infrastructure Composer Designer può aiutarti a iniziare. AWS CloudFormation Per ulteriori informazioni, consulta [Lavorare con i CloudFormation modelli](#) nella Guida per l'utente.AWS CloudFormation

È possibile creare AWS CloudFormation modelli per i seguenti tipi di risorse Macie:

- Consenti elenchi
- Identificatori di dati personalizzati
- Regole di filtro e regole di soppressione per i risultati, note anche come filtri di risultati

Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per questi tipi di risorse, consulta il [riferimento al tipo di risorsa Amazon Macie](#) nella Guida per l'utente.AWS CloudFormation

Risorse di apprendimento aggiuntive per AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guida per l'utente](#)
- [AWS CloudFormation Documentazione di riferimento delle API](#)

- [AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando](#)

Sospendere Macie per te Account AWS

Puoi mettere temporaneamente in pausa Amazon Macie per Account AWS il tuo computer. Regione AWS Puoi farlo sospendendo Macie nella regione. Macie interrompe quindi l'esecuzione di tutte le attività relative al tuo account in quella regione. Le attività includono: monitoraggio dei dati di Amazon Simple Storage Service (Amazon S3), esecuzione di rilevazione automatica di dati sensibili ed esecuzione di processi di rilevamento di dati sensibili attualmente in corso. Macie annulla anche tutti i tuoi lavori di rilevamento di dati sensibili nella regione. Non ti viene addebitato alcun costo per l'utilizzo di Macie nella Regione mentre è sospeso.

Se sospendi Macie in una Regione, Macie conserva l'identificatore di sessione, le impostazioni e le risorse che archivia o gestisce per il tuo account nella Regione. Macie conserva anche alcuni dati che archivia o conserva per l'account dell'utente nella Regione. Ad esempio, i risultati esistenti rimangono intatti e vengono conservati per un massimo di 90 giorni. Se per il tuo account è stata abilitata l'individuazione automatica dei dati sensibili, anche i risultati esistenti rimangono intatti e vengono conservati per un massimo di 30 giorni.

Note

Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, tieni presente i seguenti requisiti per sospendere Macie:

- Se disponi di un account membro in un' AWS Organizations organizzazione, devi contattare l'amministratore Macie dell'organizzazione. Solo l'amministratore di Macie può sospendere Macie per il tuo account.
- Se sei l'amministratore Macie dell'organizzazione, devi rimuovere tutti gli account dei membri associati al tuo account prima di sospendere Macie per il tuo account. Il modo in cui esegui questa operazione dipende dal fatto che il tuo account sia associato agli account tramite AWS Organizations o tramite invito. Per ulteriori informazioni, consulta [Gestione di più account](#).

Dopo aver sospeso Macie in una regione, puoi riattivarlo in un secondo momento. Potrai quindi riottenere l'accesso alle impostazioni, alle risorse e ai dati di Macie nella regione. Inoltre, Macie riprende le attività per il tuo account nella Regione. Ciò include l'aggiornamento e la manutenzione delle informazioni sui bucket S3 e il monitoraggio dei bucket per motivi di sicurezza e controllo degli

accessi. Ciò non include la ripresa o il riavvio dei processi di rilevamento dei dati sensibili. I processi di rilevamento di dati sensibili non possono essere ripresi o riavviati dopo essere stati annullati.

Per sospendere Macie per il tuo account

Per sospendere Macie per il tuo account, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Segui questi passaggi per sospenderlo utilizzando la console. Per sospenderlo a livello di codice, utilizza il [UpdateMacieSession](#) funzionamento dell'API Amazon Macie.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri sospendere Macie.
3. Nel pannello di navigazione scegli Impostazioni.
4. Nella sezione Suspend Macie, scegli Sospendi Macie.
5. Quando viene richiesta la conferma, inserisci, quindi **Suspend** scegli Sospendi.
6. Per sospendere Macie in altre regioni, ripeti i passaggi da 2 a 5 in ciascuna regione aggiuntiva.

Per riattivare successivamente Macie in una regione, apri la console Amazon Macie e scegli la regione utilizzando il selettore. Regione AWS Quindi scegli Impostazioni nel pannello di navigazione. Nella sezione Suspend Macie, scegli Riattiva Macie. Puoi anche riattivare Macie a livello di codice. A tale scopo, utilizza il [UpdateMacieSession](#) funzionamento dell'API Amazon Macie.

Disabilitare Macie per il tuo Account AWS

Se desideri interrompere l'utilizzo di Amazon Macie in un determinato caso Regione AWS, puoi disattivarlo per la tua Account AWS regione.

Quando disabiliti Macie in una regione, Macie interrompe l'esecuzione di tutte le attività relative al tuo account in quella regione. Le attività includono: monitoraggio dei dati di Amazon Simple Storage Service (Amazon S3), esecuzione di rilevazione automatica di dati sensibili ed esecuzione di processi di rilevamento di dati sensibili attualmente in corso. Macie elimina anche tutte le impostazioni, le risorse e i dati esistenti che archivia o conserva per il tuo account nella Regione. Ad esempio, Macie elimina i risultati e i lavori di rilevamento dei dati sensibili. I dati che hai archiviato o pubblicato su altri Servizi AWS rimangono intatti e non sono interessati, ad esempio, i risultati del rilevamento di dati sensibili in Amazon S3 e la ricerca di eventi in Amazon. EventBridge

Se il tuo account fa parte di un'organizzazione che gestisce centralmente più account Macie, devi fare quanto segue prima di disabilitare Macie per il tuo account:

- Se hai un account membro, contatta l'amministratore di Macie per rimuovere il tuo account come account membro.
- Se sei l'amministratore Macie dell'organizzazione, rimuovi tutti gli account dei membri associati al tuo account. Elimina anche le associazioni tra il tuo account e tali account.

Il modo in cui completi le attività precedenti dipende dal fatto che il tuo account sia associato ad altri account tramite AWS Organizations o tramite invito. Per ulteriori informazioni, consulta [Gestione di più account](#).

Per disattivare Macie per il tuo account

Per disabilitare Macie per il tuo account, puoi utilizzare la console Amazon Macie o l'API Amazon Macie. Segui questi passaggi per disabilitarlo utilizzando la console. Per disabilitarlo a livello di codice, utilizza il [DisableMacie](#) funzionamento dell'API Amazon Macie.

Warning

Se disabiliti Macie in una regione, elimini definitivamente anche tutti i risultati esistenti, i processi di ricerca di dati sensibili, gli identificatori di dati personalizzati e altre risorse e dati che Macie archivia o conserva per il tuo account nella regione. Le risorse e i dati non possono

essere recuperati dopo l'eliminazione. Per conservare le risorse e i dati, [sospendi Macie](#) invece di disabilitarlo.

1. Apri la console Amazon Macie all'indirizzo. <https://console.aws.amazon.com/macie/>
2. Utilizzando il Region AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri disattivare Macie.
3. Nel pannello di navigazione scegli Impostazioni.
4. Nella sezione Disattiva Macie, scegli Disabilita Macie.
5. Quando viene richiesta la conferma, immetti **Disable**, quindi scegli Disabilita.

Per disabilitare Macie in altre regioni, ripeti i passaggi precedenti in ogni regione aggiuntiva.

Quote per Macie

Hai Account AWS determinate quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Queste quote rappresentano il numero massimo di risorse o operazioni di servizio per l'account. Questo argomento elenca le quote che si applicano alle risorse e alle operazioni di Amazon Macie per il tuo account. Salvo diversa indicazione, ogni quota si applica all'account di ciascuno di essi. Regione AWS

Alcune quote possono essere aumentate, mentre altre no. Per richiedere un aumento di una quota, usa la console [Service Quotas](#). Per informazioni su come richiedere un aumento, consulta [Richiedere un aumento della quota](#) nella Service Quotas User Guide. Se una quota non è disponibile nella console Service Quotas, utilizza il [modulo di aumento del limite di servizio](#) su AWS Support Center Console per richiedere un aumento della quota.

Risultati

- Regole di filtro e regole di soppressione per account: 1.000
- Risultati per esecuzione di un processo di rilevamento di dati sensibili: 100.000, più il 5% di tutti i risultati rimanenti dopo il raggiungimento della soglia di 100.000

Questa quota si applica solo alla console Amazon Macie e all'API Amazon Macie. Non esiste una quota per il numero di eventi di ricerca che Macie pubblica su Amazon EventBridge o il numero di risultati di scoperta di dati sensibili che Macie crea per ogni esecuzione di un lavoro.

- Luoghi di rilevamento per rilevamento di dati sensibili: 15
- Richieste di recupero e rivelazione di campioni di dati sensibili da un oggetto Amazon S3:100 al giorno

Questa quota viene ripristinata ogni 24 ore alle 00:00:01 UTC+0.

- Dimensioni di un oggetto Amazon S3 per recuperare e rivelare campioni di dati sensibili da:
 - File contenitore di oggetti Apache Avro (.avro): 70 MB
 - File Apache Parquet (.parquet): 100 MB
 - File CSV (.csv): 255 MB
 - File di archivio compresso GNU Zip (.gz o .gzip): 90 MB
 - File JSON o JSON Lines (.json o .jsonl): 25 MB
 - File della cartella di lavoro Microsoft Excel (.xlsx): 20 MB
 - Testo non binario (text/plain) file: 100 MB

- File TSV (.tsv): 75 MB
- File di archivio compresso ZIP (.zip): 355 MB

Se una scoperta si applica a un file di archivio che genera più file.gz per i corrispondenti [risultati di rilevamento dei dati sensibili](#), non è possibile recuperare e visualizzare campioni di dati sensibili dal file di archivio.

Organizations

- Account membri su invito: 1.000
- Account membri fino a AWS Organizations: 10.000

Controllo preventivo e monitoraggio

- Bucket S3 per account: 10.000

Se il tuo account supera questa quota, Macie fornisce funzionalità di monitoraggio complete per i 10.000 bucket che sono stati creati o modificati più di recente. Per tutti gli altri bucket, Macie non valuta né monitora i bucket per quanto riguarda la sicurezza e il controllo degli accessi, non genera risultati relativi alle politiche o mantiene dati di inventario completi.

Rilevamento di dati sensibili

- Analisi mensile per account in base alle attività di rilevamento di dati sensibili: 5 TB

Questa quota si applica solo ai lavori di rilevamento di dati sensibili. Per aumentare la quota fino a 1.000 TB (1 PB), usa la console [Service Quotas](#). Per richiedere un aumento per più di 1 PB, utilizza il [modulo di aumento del limite di servizio disponibile](#) su AWS Support Center Console

- Identificatori di dati personalizzati per account: 10.000
- Consenti elenchi per account: 10, 1—5 consentono elenchi che specificano testo predefinito e 1—5 consentono elenchi che specificano espressioni regolari

Le quote aggiuntive si applicano a un elenco di contenuti consentiti che specifica un testo predefinito. L'elenco non può contenere più di 100.000 voci e la dimensione di archiviazione dell'elenco non può superare i 35 MB.

- Bucket S3 da escludere dal rilevamento automatico di dati sensibili: 1.000

Se il tuo account è l'account amministratore Macie di un'organizzazione, questa quota si applica all'intera organizzazione.

- Bucket S3 per processo di rilevamento di dati sensibili: 1.000

Questa quota non si applica ai lavori che utilizzano i criteri dei bucket di runtime per determinare quali bucket analizzare. Si applica a un job solo se si configura il job per analizzare bucket specifici selezionati. Se il tuo account è l'account amministratore Macie di un'organizzazione, puoi selezionare fino a 1.000 bucket che coprono fino a 1.000 account della tua organizzazione.

- Identificatori di dati personalizzati per processo di rilevamento di dati sensibili: 30
- Consenti elenchi per processo di rilevamento di dati sensibili: 10, 1—5 consentono elenchi che specificano testo predefinito e 1—5 consentono elenchi che specificano espressioni regolari
- [CreateClassificationJob](#) operazione: 0,1 richieste al secondo
- Tempo di analisi di un singolo file: 10 ore
- Dimensioni di un singolo file da analizzare:
 - File Adobe Portable Document Format (.pdf): 1.024 MB
 - File contenitore di oggetti Apache Avro (.avro): 8 GB
 - File Apache Parquet (.parquet): 8 GB
 - File di messaggi di posta elettronica (.eml): 20 GB
 - File di archivio compresso GNU Zip (.gz o .gzip): 8 GB
 - File della cartella di lavoro di Microsoft Excel (.xls o .xlsx): 512 MB
 - Documento Microsoft Word (.doc o .docx): 512 MB
 - File di testo non binario: 20 GB
 - File di archivio TAR (.tar): 20 GB
 - File di archivio compresso ZIP (.zip): 8 GB

Se un file è più grande della quota applicabile, Macie non analizza alcun dato nel file.

- Estrazione e analisi dei dati in un file compresso o di archivio:
 - Dimensione di archiviazione (compressa): 8 GB per un file di archivio compresso GNU Zip (.gz o .gzip) o file di archivio compresso ZIP (.zip); 20 GB per un file di archivio TAR (.tar)
 - Profondità dell'archivio annidato: 10 livelli
 - File estratti: 1.000.000

- Byte estratti: complessivamente 10 GB di dati non compressi. [3 GB di dati non compressi per ogni file estratto che utilizza un tipo di file o un formato di archiviazione supportato.](#)

Se i metadati di un file compresso o di archivio indicano che il file contiene più di 10 livelli annidati o supera la quota applicabile in termini di dimensioni di archiviazione o byte estratti, Macie non estrae né analizza alcun dato nel file. Se Macie inizia a estrarre e analizzare i dati in un file compresso o di archivio e successivamente determina che il file contiene più di 1.000.000 di file o supera la quota di byte estratti, Macie interrompe l'analisi dei dati nel file e crea rilevamenti di dati sensibili e risultati di scoperta solo per i dati che sono stati elaborati.

- Analisi degli elementi annidati nei dati strutturati: 256 livelli per file

Questa quota si applica solo ai file JSON (.json) e JSON Lines (.jsonl). Se la profondità annidata di uno dei due tipi di file supera questa quota, Macie non analizza alcun dato nel file.

- Posizioni di rilevamento per risultato del rilevamento di dati sensibili: 1.000 per tipo di rilevamento di dati sensibili
- Rilevamento di nomi completi: 1.000 per file, inclusi i file di archivio

Dopo che Macie rileva le prime 1.000 occorrenze di nomi completi in un file, Macie smette di incrementare il conteggio e di riportare i dati sulla posizione per i nomi completi.

- Rilevamento degli indirizzi postali: 1.000 per file, inclusi i file di archivio

Dopo che Macie rileva le prime 1.000 occorrenze di indirizzi postali in un file, Macie smette di incrementare il conteggio e di riportare i dati sulla posizione degli indirizzi postali.

Cronologia dei documenti per la Guida per l'utente di Amazon Macie

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione di Amazon Macie. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

Ultimo aggiornamento della documentazione: 2 luglio 2025

Modifica	Descrizione	Data
Nuove funzionalità	Macie ora supporta gli endpoint dell'interfaccia VPC e le policy degli endpoint in tutti i paesi in cui Regioni AWS è attualmente disponibile.	2 luglio 2025
Nuove funzionalità	Macie ora fornisce identificatori di dati gestiti progettati per rilevare i seguenti tipi di dati sensibili: numeri di identificazione nazionali per Argentina, Cile, Colombia e Messico; numeri di carta del Sistema Único de Boleto Electrónico (SUBE) per l'Argentina; e numeri di identificazione e di riferimento dei contribuenti per Argentina, Cile, Colombia e Messico.	3 marzo 2025
Funzionalità aggiornate	Macie ora può eseguire il monitoraggio preventivo del controllo per un massimo di 10.000 bucket Amazon S3 generici per il tuo account.	6 dicembre 2024

Nuovo contenuto

Sono stati aggiunti esempi e dettagli che spiegano come [configurare e gestire il rilevamento automatico di dati sensibili in modo programmatico](#) con l'API Amazon Macie.

22 novembre 2024

Nuova caratteristica

Se disponi di un account membro in un'organizzazione, ora hai accesso in lettura a statistiche, dati di inventari o e altre informazioni che il [rilevamento automatico di dati sensibili](#) produce per i tuoi dati Amazon S3. Per dettagli sulle impostazioni di rilevamento automatico per il tuo account e la tua organizzazione, contatta l'amministratore di Macie.

22 luglio 2024

Nuova caratteristica

Se sei l'amministratore delegato di Macie di un'organizzazione, ora puoi [abilitare o disabilitare il rilevamento automatico dei dati sensibili](#) per i singoli account della tua organizzazione. Con questa opzione aggiuntiva, ora puoi definire l'ambito delle analisi in diversi modi: abilitare il rilevamento automatico per tutti gli account, abilitare selettivamente il rilevamento automatico per determinati account ed escludere determinati bucket S3.

14 giugno 2024

Nuove funzionalità

AWS Security Hub ora fornisce [controlli di sicurezza](#) che controllano lo stato di Macie e il rilevamento automatico dei dati sensibili per gli account. [Se questi controlli sono abilitati, Security Hub esegue periodicamente controlli di sicurezza per determinare se Macie è abilitato per un Account AWS \(controllo Macie.1\) e se il rilevamento automatico dei dati sensibili è abilitato per un account Macie \(controllo Macie.2\).](#)

20 febbraio 2024

Nuove funzionalità

Macie ora può [analizzare gli oggetti Amazon S3](#) crittografati utilizzando la crittografia lato server a doppio livello con (DSSE-KMS). AWS KMS keys Questi oggetti sono ora idonei per l'analisi quando Macie esegue il rilevamento automatico di dati sensibili o quando si eseguono lavori di rilevamento di dati sensibili. Inoltre, i bucket e gli oggetti S3 che utilizzano la crittografia DSSE-KMS sono ora inclusi nelle [statistiche e nei metadati](#) forniti da Macie sui tuoi dati Amazon S3.

17 gennaio 2024

Nuova caratteristica

Ora puoi configurare Macie in modo che assuma un ruolo AWS Identity and Access Management (IAM) quando scegli di [recuperare e rivelare](#) campioni di dati sensibili che Macie riporta nei risultati. Gli esempi possono aiutarti a verificare la natura dei dati sensibili trovati da Macie e a personalizzare l'indagine su un oggetto e un bucket Amazon S3 interessati.

16 novembre 2023

Nuove funzionalità

Macie ora fornisce [identificatori di dati gestiti](#) progettati per rilevare i numeri di conto bancario internazionale (IBANs) per 47 altri paesi e regioni. Ora puoi usare Macie per rilevare e segnalare ricorrenze in più IBANs di 50 paesi e regioni.

1 novembre 2023

Nuove funzionalità

Macie ora fornisce [identificatori di dati gestiti](#) progettati per rilevare i seguenti tipi di dati sensibili: chiavi API di Google Cloud, chiavi API Stripe e numeri Aadhaar, numeri di account permanenti (PANs) e numeri di identificazione della patente di guida per l'India.

25 settembre 2023

[Nuove quote](#)

Per aiutarti a verificare la natura dei dati sensibili riportati dai risultati, abbiamo aumentato le quote di dimensione per il [recupero e la rivelazione di campioni di dati sensibili dagli oggetti Amazon S3](#). Ora puoi recuperare e rivelare campioni da oggetti S3 la cui dimensione di archiviazione supera i 10 MB. Per un elenco delle nuove quote, consulta la sezione Quote di [Amazon Macie](#).

7 settembre 2023

[Disponibilità regionale](#)

Macie è ora disponibile nella regione di Israele (Tel Aviv). Per un elenco completo delle aree Regioni AWS in cui Macie è attualmente disponibile, consulta gli [endpoint e le quote di Amazon Macie](#) nel. Riferimenti generali di AWS

28 agosto 2023

Funzionalità aggiornate

Abbiamo implementato un nuovo set dinamico di [identificatori di dati gestiti predefiniti per il rilevamento automatico di dati](#) sensibili. Il set predefinito include gli identificatori di dati gestiti consigliati per il rilevamento automatico di dati sensibili. È progettato per rilevare categorie e tipi comuni di dati sensibili, ottimizzando al contempo i risultati del rilevamento automatico dei dati sensibili.

2 agosto 2023

Funzionalità aggiornate

Per aiutarti a [individuare le occorrenze di dati sensibili](#) segnalati da Macie nelle rilevazioni di dati sensibili e nei risultati della scoperta di dati sensibili, abbiamo modificato il limite di caratteri da 20 a 240 per i nomi degli elementi del percorso JSON negli oggetti. Record Questa modifica influisce sulle nuove rilevazioni di dati sensibili e sui risultati di scoperta per i contenitori di oggetti Apache Avro, i file Apache Parquet, i file JSON e i file JSON Lines.

24 luglio 2023

Funzionalità aggiornate

Se sei l'amministratore delegato di Macie per un'organizzazione in AWS Organizations, ora puoi [gestire Macie per](#) un massimo di 10.000 account della tua organizzazione.

30 giugno 2023

Nuova caratteristica

Ora puoi [creare e configurare processi di rilevamento di dati sensibili per utilizzarli automaticamente il set di identificatori di dati gestiti che consigliamo per i lavori](#). Questo [set consigliato di identificatori di dati gestiti](#) è progettato per rilevare categorie e tipi comuni di dati sensibili, ottimizzando al contempo i risultati del lavoro.

28 giugno 2023

Nuova policy

Abbiamo aggiunto una nuova [policy AWS gestita, la AmazonMacieReadOnlyAccess policy](#). Questa policy concede autorizzazioni di sola lettura che consentono a un'identità IAM (principale) di recuperare tutte le risorse, i dati e le impostazioni di Macie per il proprio account.

15 giugno 2023

Nuova caratteristica

Per aiutarti a [valutare e monitorare la copertura automatizzata del rilevamento di dati sensibili](#) dei tuoi dati Amazon S3, la console Macie ora include una pagina di copertura delle risorse. La pagina offre una visualizzazione unificata delle statistiche e dei dati di copertura per tutti i bucket S3, incluso un elenco degli eventuali problemi di analisi che si sono verificati di recente per ogni bucket. Se si sono verificati problemi, la pagina fornisce anche indicazioni per la risoluzione.

15 maggio 2023

Nuova caratteristica

Macie si integra con Notifiche all'utente AWS, che è una novità Servizio AWS che funge da posizione centrale per le AWS notifiche su. AWS Management Console Con Notifiche all'utente, puoi [configurare regole e canali di distribuzione personalizzati](#) per generare e inviare notifiche sugli EventBridge eventi di Amazon pubblicati da Macie per rilevare policy e dati sensibili.

5 maggio 2023

Contenuti aggiornati

27 febbraio 2023

Descrizioni aggiornate delle [statistiche e dei metadati](#) forniti da Macie sulle impostazioni di crittografia predefinite per i bucket S3. [È stata inoltre aggiornata la descrizione del risultato della politica. Policy: IAMUser/S3BucketEncryptionDisabled](#) Amazon S3 ora applica automaticamente la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per gli oggetti che vengono aggiunti a bucket nuovi ed esistenti. Per informazioni su questa modifica in Amazon S3, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

Nuove funzionalità

24 febbraio 2023

Macie ora può generare un ulteriore tipo di [ricerca delle policy](#) per un bucket S3: `Policy: IAMUser/S3BucketSharedWithCloudFront`. Questo tipo di risultato indica che la politica di un bucket è stata modificata per consentire la condivisione del bucket con una Amazon CloudFront Origin Access Identity (OAI), un CloudFront Origin Access Control (OAC) o entrambi. Inoltre, i bucket condivisi con CloudFront OAI o che ora OACs sono considerati condivisi esternamente nelle statistiche e nei metadati forniti da Macie sui tuoi dati Amazon S3.

Nuove funzionalità

Macie ora [supporta la classe di storage Amazon S3 Glacier Instant Retrieval](#) per il rilevamento di dati sensibili. Gli oggetti S3 che utilizzano questa classe di storage sono ora idonei per l'analisi quando Macie esegue il rilevamento automatico di dati sensibili o si eseguono lavori di rilevamento di dati sensibili. Sono anche considerati oggetti classificabili nelle statistiche e nei metadati che Macie fornisce sui tuoi dati Amazon S3.

21 dicembre 2022

Nuova caratteristica

Ora puoi configurare Macie per [eseguire il rilevamento automatico dei dati sensibili](#) per il tuo account o la tua organizzazione. Con il rilevamento automatico dei dati sensibili, Macie valuta continuamente i dati di Amazon S3 e utilizza tecniche di campionamento per identificare, selezionare e analizzare e gli oggetti rappresentativi nei bucket S3, ispezionando gli oggetti alla ricerca di dati sensibili. Puoi valutare i risultati delle analisi in statistiche, risultati e altre informazioni fornite da Macie sui tuoi dati Amazon S3.

28 novembre 2022

Nuova caratteristica

Ora puoi [creare e utilizzare elenchi di autorizzazione](#) per specificare testo e modelli di testo che desideri che Macie ignori quando ispeziona gli oggetti Amazon S3 alla ricerca di dati sensibili. Utilizzando gli elenchi consentiti, puoi definire eccezioni relative ai dati sensibili per scenari o ambienti particolari, ad esempio i nomi dei rappresentanti pubblici dell'organizzazione, numeri di telefono specifici o dati di esempio che l'organizzazione utilizza per i test.

30 agosto 2022

Nuova caratteristica

Per verificare la natura dei dati sensibili che Macie trova negli oggetti S3, ora puoi configurare e utilizzare Macie per [recuperare campioni](#) di dati sensibili riportati dai risultati.

26 luglio 2022

Funzionalità aggiornate

Nella [AmazonMacieFullAccesspolicy](#), abbiamo aggiornato l'Amazon Resource Name (ARN) del ruolo collegato al servizio Macie (). `aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

30 giugno 2022

Funzionalità aggiornate

Abbiamo aggiornato la [AmazonMacieServiceRolePolicy](#), che è la politica allegata al ruolo collegato al servizio Macie (`AWSServiceRoleForAmazonMacie`). La policy non specifica più azioni e risorse per Amazon Macie Classic. Amazon Macie Classic non è più disponibile e non è più disponibile.

20 maggio 2022

Nuove funzionalità

Macie ora include il `OriginType` campo [dei risultati relativi ai dati sensibili su cui pubblica](#). AWS Security Hub II `OriginType` campo specifica in che modo Macie ha trovato i dati sensibili che hanno prodotto una scoperta.

11 maggio 2022

Contenuti aggiornati

È stato chiarito come funzionano le impostazioni delle parole chiave e della distanza massima di corrispondenza per gli identificatori di dati [personalizzati](#).

22 aprile 2022

Nuove funzionalità

Macie ora fornisce [identificatori di dati gestiti](#) progettati per rilevare intestazioni di autorizzazione di base HTTP, cookie HTTP e token Web JSON.

21 aprile 2022

Nuovo contenuto	Sono state aggiunte descrizioni e definizioni dei concetti e dei termini chiave per Macie.	16 marzo 2022
Nuove funzionalità	Per calcolare e visualizzare i costi stimati durante la creazione e la configurazione di lavori di rilevamento di dati sensibili, Macie ora recupera i dati sui prezzi da te Account AWS forniti. AWS Billing and Cost Management Per supportare questa funzionalità, abbiamo aggiunto un'azione Billing and Cost Management AmazonMacieFullAccess alla policy.	7 marzo 2022
Nuove funzionalità	Macie ora include il Sample campo tra i risultati su cui pubblica . AWS Security Hub Sample campo specifica se un risultato è un risultato esemplificativo .	24 febbraio 2022
Nuovo contenuto	Sono state aggiunte informazioni sull' utilizzo di Amazon Virtual Private Cloud per stabilire una connessione privata tra il tuo VPC e Macie.	19 gennaio 2022

Nuove funzionalità	Ora puoi utilizzare la console Amazon Macie per assegnare e gestire tag per identificatori di dati personalizzati, regole di filtro e soppressione per risultati, processi di rilevamento di dati sensibili e, se sei l'amministratore Macie di un'organizzazione, account membri della tua organizzazione. Un tag è un'etichetta che puoi definire e assegnare facoltativamente a determinati tipi di risorse. AWS	12 gennaio 2022
Nuovo contenuto	Sono state aggiunte informazioni sull'utilizzo AWS Identity and Access Management per gestire l'accesso a Macie.	20 dicembre 2021
Nuova caratteristica	Quando crei un identificatore di dati personalizzato, ora puoi definire le impostazioni di gravità per le rilevazioni di dati sensibili che produce. Con queste impostazioni, puoi specificare la gravità da assegnare a un risultato in base al numero di occorrenze di testo che corrispondono ai criteri di rilevamento dell'identificatore di dati personalizzato.	4 novembre 2021

Nuove funzionalità

Per conoscere i diversi tipi di risultati forniti da Macie, puoi [generare risultati di esempio](#). I risultati di esempio utilizzano dati di esempio e valori segnaposto per dimostrare i tipi di informazioni che Macie potrebbe includere in ogni tipo di risultato.

28 ottobre 2021

Nuove funzionalità

Macie ora include il `OwnerAccountId` campo tra i [risultati su cui pubblica](#). AWS Security Hub Questo campo specifica l'ID dell'account del proprietario del Account AWS bucket S3 interessato.

27 ottobre 2021

Nuovo contenuto

Sono state aggiunte informazioni sulla [gestione centralizzata di più account Macie](#). Puoi farlo in due modi: integrando Macie AWS Organizations o inviando inviti all'iscrizione da Macie.

13 ottobre 2021

Nuove funzionalità

L'inventario dei bucket S3

5 ottobre 2021

ora indica se le impostazioni delle autorizzazioni di un bucket impediscono a Macie di recuperare informazioni sul bucket o sugli oggetti del bucket e di valutare e monitorare la sicurezza e la privacy dei dati del bucket. Inoltre, abbiamo aggiornato i riferimenti e le chiavi gestite dai clienti per riflettere la terminologia corrente. AWS KMS keys

Nuove funzionalità

Macie ora archivia i risultati delle policy e dei dati sensibili per 90 giorni anziché 30 giorni. Se Macie ha creato o aggiornato una scoperta a partire dal 31 agosto 2021, puoi accedere alla scoperta per un massimo di 90 giorni utilizzando la console Macie o l'API Macie. In alcuni casi Regioni AWS, Macie ha iniziato a conservare i risultati per 90 giorni già il 27 settembre 2021.

1° ottobre 2021

Nuova caratteristica	Quando crei un processo di rilevamento di dati sensibili , ora puoi specificare quali identificatori di dati gestiti desideri che il job utilizzi per l'analisi degli oggetti S3. Con questa funzionalità, puoi personalizzare l'analisi di un lavoro per concentrarti su determinati tipi di dati sensibili.	17 settembre 2021
Nuove funzionalità	I risultati relativi ai dati sensibili ora forniscono informazioni aggiuntive per aiutarti a localizzare i dati sensibili nei file JSON e JSON Lines.	6 luglio 2021
Funzionalità aggiornate	Macie ora utilizza il tipo di <code>AwsS3Bucket</code> risorsa nei risultati su cui pubblica . AWS Security Hub(Macie aveva precedentemente impostato questo valore su.) <code>AWS::S3::Bucket</code> <code>AwsS3Bucket</code> è il valore del tipo di risorsa utilizzato per i bucket S3 nel AWS Security Finding Format (ASFF).	28 giugno 2021

Nuova caratteristica

Quando [crei un processo di rilevamento di dati sensibili](#), ora puoi definire criteri di runtime che determinano i bucket S3 analizzati dal job.

Grazie a questa funzionalità, l'ambito dell'analisi di un job può adattarsi dinamicamente alle modifiche apportate all'inventario dei bucket.

15 maggio 2021

Nuove funzionalità

L'[inventario dei bucket S3](#) e la dashboard di riepilogo ora forniscono metadati di crittografia e statistiche che indicano se le policy dei bucket richiedono la crittografia lato server di nuovi oggetti. Inoltre, ora puoi eseguire aggiornamenti su richiesta dei metadati degli oggetti per singoli bucket nel tuo inventario di bucket.

30 aprile 2021

Nuova caratteristica

Ora puoi [utilizzare Amazon CloudWatch Logs per monitorare e analizzare gli eventi](#) che si verificano quando esegui processi di rilevamento di dati sensibili. [Per supportare questa funzionalità, abbiamo aggiunto le azioni CloudWatch Logs alla policy AWS gestita per il ruolo collegato al servizio Macie.](#)

14 aprile 2021

Disponibilità regionale	Macie è ora disponibile nella regione AWS Asia Pacifico (Osaka).	5 aprile 2021
Nuova caratteristica	Ora puoi configurare Macie per pubblicare i risultati relativi ai dati sensibili su . AWS Security Hub	22 marzo 2021
Nuovo contenuto	Sono state aggiunte informazioni sul monitoraggio e la previsione dei costi di Macie e sulla partecipazione alla prova gratuita.	26 febbraio 2021
Contenuti aggiornati	Abbiamo sostituito il termine account principale con il termine account amministratore. Un account amministratore viene utilizzato per gestire centralmente più account .	12 febbraio 2021
Nuove funzionalità	Ora puoi affinare l'ambito dei processi di rilevamento dei dati sensibili utilizzando i prefissi degli oggetti S3 nei criteri di inclusione ed esclusione personalizzati.	2 febbraio 2021
Contenuti aggiornati	Macie ora aderisce alla tassonomia dei tipi di ricerca del AWS Security Finding Format (ASFF) quando pubblica i risultati delle politiche su. AWS Security Hub	28 gennaio 2021

Nuovo contenuto	Sono state aggiunte informazioni sul monitoraggio dei dati di Amazon S3 e sulla valutazione della sicurezza e della privacy di tali dati.	8 gennaio 2021
Disponibilità regionale	Macie è ora disponibile nella regione AWS Africa (Città del Capo), nella regione AWS Europa (Milano) e nella regione AWS Medio Oriente (Bahrein).	21 dicembre 2020
Nuove funzionalità	Se il tuo account è un account amministratore Macie, ora puoi creare ed eseguire processi di rilevamento di dati sensibili che analizzano i dati per un massimo di 1.000 bucket che coprono fino a 1.000 account della tua organizzazione.	25 novembre 2020
Nuove funzionalità	Il tuo inventario dei bucket S3 ora indica se hai configurato processi di rilevamento di dati sensibili una tantum o periodici per analizzare i dati in un bucket. In caso affermativo, fornisce anche dettagli sul job eseguito più di recente.	23 novembre 2020
Nuovo contenuto	Sono state aggiunte informazioni sul filtraggio dei risultati .	12 novembre 2020

Nuove funzionalità	I dati sensibili ora forniscono informazioni aggiuntive per aiutarti a localizzare i dati sensibili nei contenitori di oggetti Apache Avro, nei file Apache Parquet e nelle cartelle di lavoro di Microsoft Excel.	9 novembre 2020
Nuova caratteristica	Ora puoi utilizzare i risultati dei dati sensibili per individuare singole occorrenze di dati sensibili negli oggetti S3.	22 ottobre 2020
Nuova caratteristica	Ora puoi mettere in pausa e riprendere i lavori di rilevamento dei dati sensibili .	16 ottobre 2020
Nuovo contenuto	Sono stati aggiunti dettagli sul sistema di valutazione della gravità per i risultati delle politiche e dei dati sensibili.	6 ottobre 2020
Nuove funzionalità	Ora puoi visualizzare le statistiche che indicano la quantità di dati che Macie può analizzare nei singoli bucket S3 quando esegui un processo di rilevamento di dati sensibili. Inoltre, è ora possibile visualizzare il costo stimato di un lavoro al momento della creazione di un lavoro .	3 settembre 2020

Nuovo contenuto	Sono state aggiunte informazioni sulla configurazione, l'esecuzione e la gestione dei job di rilevamento di dati sensibili .	31 agosto 2020
Nuove funzionalità	Gli identificatori di dati gestiti possono ora rilevare determinati tipi di informazioni di identificazione personale per il Brasile.	31 luglio 2020
Contenuti aggiornati	Sono state aggiunte informazioni sulla sintassi supportata per le espressioni regolari negli identificatori di dati personalizzati .	30 luglio 2020
Contenuti aggiornati	Sono stati aggiunti i requisiti relativi alle parole chiave per gli identificatori di dati gestiti e è stata aumentata la quota per il numero di risultati che ogni processo di rilevamento di dati sensibili può produrre.	17 luglio 2020
Nuovo contenuto	Sono state aggiunte informazioni sull'utilizzo di Amazon EventBridge e AWS Security Hub sul monitoraggio e l'elaborazione dei risultati . Ciò include lo schema degli EventBridge eventi per i risultati e gli esempi di eventi per i risultati delle politiche e dei dati sensibili.	22 giugno 2020

Nuovo contenuto	Sono state aggiunte informazioni sull' analisi e la soppressione dei risultati .	17 giugno 2020
Nuovo contenuto	Sono state aggiunte istruzioni per configurare Macie per archiviare i risultati di discovery dettagliati in un bucket S3.	2 giugno 2020
Nuovo contenuto	Sono state aggiunte informazioni sui tipi di dati sensibili che Macie è in grado di rilevare e sui requisiti di crittografia per il rilevamento dei dati sensibili negli oggetti Amazon S3.	28 maggio 2020
Disponibilità generale	Questa è la versione pubblica iniziale della Guida per l'utente di Amazon Macie.	13 maggio 2020

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.