



Informazioni sulla sicurezza

Catalogo di controllo AWS



Catalogo di controllo AWS: Informazioni sulla sicurezza

Copyright © 2026 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 dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è Control Catalog?	1
Panoramica dell'ontologia	1
Accesso a Control Catalog	3
Sicurezza	4
Protezione dei dati	4
Crittografia dei dati	5
Crittografia dei dati in transito	6
Gestione delle chiavi	6
Riservatezza del traffico inter-rete	6
Gestione dell'identità e degli accessi	6
Destinatari	6
Autenticazione con identità	7
Gestione dell'accesso tramite policy	8
Come funziona Control Catalog con IAM	10
Esempi di policy basate su identità	17
Risoluzione dei problemi	20
Convalida della conformità	22
Resilienza	22
Sicurezza dell'infrastruttura	22
Configurazione e vulnerabilità	23
Monitoraggio	24
CloudTrail registri	24
Controlla le informazioni del catalogo in CloudTrail	24
Informazioni sulle voci dei file di registro di Control Catalog	25
AWS PrivateLink	27
Considerazioni	27
Creazione di un endpoint di interfaccia	27
Creazione di una policy dell'endpoint	28
Cronologia dei documenti	30
.....	xxxi

Cos'è Control Catalog?

Benvenuto nella guida alle informazioni sulla sicurezza di Control Catalog. Il Control Catalog fa parte di AWS Control Tower, che elenca i controlli per diversi AWS servizi. È un catalogo consolidato di AWS controlli. Non è necessario configurarlo per AWS Control Tower utilizzare il Control Catalog.

Con Control Catalog, puoi visualizzare i controlli in base a casi d'uso comuni, tra cui sicurezza, costi, durata e operazioni.

In questo documento, puoi trovare le informazioni sulla sicurezza e la conformità che devi conoscere, poiché utilizzi quelle APIs fornite da Control Catalog.

Il Control Catalog incorpora una Control Ontology, che è un sistema di classificazione standard per i controlli.

Panoramica dell'ontologia

AWS ha sviluppato un sistema di classificazione standard per aiutare a classificare, organizzare e creare mappature tra i controlli. Questa ontologia può essere utilizzata per mappare i controlli in base a standard normativi esistenti e nuovi, inclusi 24 framework, nonché standard normativi come PCI, HIPAA e altri. Ci basiamo anche su standard di settore come NIST e ISO e su framework specifici di Amazon, incluso il framework Well-Architected.

L'ontologia ha quattro aspetti fondamentali

- Classificazione dei controlli per dominio di controllo, obiettivo di controllo e controlli comuni.

L'ontologia aiuta a organizzare e raggruppare i controlli correlati in tre livelli:

- L1: dominio di controllo,
- L2: obiettivo di controllo,
- L3: controllo comune.

Questi livelli hanno una stretta relazione gerarchica. Cioè, ogni dominio ha più obiettivi di controllo, ma ogni obiettivo di controllo deve avere un unico dominio principale. Ogni obiettivo di controllo ha più controlli comuni, ma ogni controllo comune ha un unico obiettivo principale.

- Mappatura agli standard normativi. L'ontologia ha un concetto chiamato controllo standard (L4) che rappresenta un requisito specifico all'interno di uno standard normativo o di settore. Questi controlli standard sono mappati su controlli comuni che aiutano a soddisfare tali requisiti specifici.

Ad esempio, PCI-DSS v3.2.1. ID 4.1 Utilizza protocolli di crittografia e sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte e NIST 800.53.r5 ID SC-16 Gli attributi di trasmissione di sicurezza e privacy sono due controlli standard, entrambi mappati al controllo comune Encrypt data in transit.

- Implementazioni di controllo ed evidenze di controllo. L'ontologia ha un concetto di implementazioni di controllo (L6) che possono rappresentare sia un'implementazione di controllo specifica in AWS, ad esempio, un controllo, un AWS Control Tower controllo, una AWS Security Hub CSPM AWS Config regola e così via, sia un'implementazione non tecnica esterna AWS, come una guida al processo. Un concetto separato di Control Evidence (L7) rappresenta le fonti di dati che possono essere utilizzate come prove per i controlli da strumenti di terze parti o dai AWS Audit Manager clienti stessi. Queste fonti di evidenza potrebbero essere AWS fonti come AWS CloudTrail eventi, registri delle chiamate API e risultati della valutazione delle AWS Config regole. In alternativa, potrebbero essere fonti esterne come la documentazione dei clienti.
- Il concetto di controllo Core (L5). Il controllo Core è un livello di mappatura che consolida tutte le implementazioni di controllo (L6), le fonti di evidenza corrispondenti (L7), i controlli standard correlati (L4) e i controlli comuni (L3) in un unico oggetto olistico. Il controllo Core è più un documento di mappatura che un controllo stesso. Aiuta a rispondere alla domanda di mostrarmi tutte le informazioni relative al controllo X. Ogni controllo principale può avere più implementazioni di controllo (L6) e più fonti di evidenza (L7).

In sintesi, l'ontologia del catalogo AWS di controllo contiene sette livelli. Tre sono livelli di classificazione gerarchici (domini di controllo, obiettivi di controllo, controlli comuni). Un altro livello (controlli standard) descrive i requisiti normativi o standard di settore. Un livello di mappatura (Core control) descrive un risultato di controllo per un determinato tipo di risorsa. Due livelli (implementazioni di controllo, evidenze di controllo) descrivono le implementazioni di controllo specifiche e le fonti di evidenza.

Questa ontologia è stata progettata da un AWS team di revisori certificati, sulla base della loro esperienza di lavoro con centinaia di clienti per i controlli di conformità. I concetti di domini di controllo, obiettivi di controllo, controlli comuni e controlli standard (L1-L4) vengono utilizzati in tutto il settore. Corrispondono ai modelli di settore comuni e alle raccomandazioni del NIST. I tre livelli rimanenti (L5-L7) sono stati progettati sulla base di AWS concetti esistenti, come i tipi di risorse e i controlli gestiti.

Accesso a Control Catalog

Control Catalog è disponibile tramite la console e tramite l'interfaccia di programmazione dell'applicazione (API) Control Catalog. Questa API fornisce un modo programmatico per identificare e filtrare i controlli comuni e i relativi metadati disponibili come AWS cliente. Per ulteriori informazioni, consulta il riferimento all'[API Control Catalog](#).

Sicurezza in Control Catalog

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 ulteriori informazioni sui programmi di conformità che si applicano a Control Catalog, consulta [AWS Servizi rientranti nell'ambito del programma di conformità Servizi AWS](#) .
- Sicurezza nel cloud: la tua responsabilità è determinata da Servizio AWS ciò che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Control Catalog;. I seguenti argomenti mostrano come configurare Control Catalog; per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altre risorse Servizi AWS che ti aiutano a monitorare e proteggere Control Catalog.

Argomenti

- [Protezione dei dati in Control Catalog](#)
- [Gestione delle identità e degli accessi per Control Catalog](#)
- [Convalida della conformità per Control Catalog](#)
- [Resilienza in Control Catalog](#)
- [Sicurezza dell'infrastruttura in Control Catalog](#)

Protezione dei dati in Control Catalog

Il modello di [responsabilità AWS condivisa modello](#) di di si applica alla protezione dei dati in AWS Control Catalog. 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 maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. 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 AWS Control Catalog o altro Servizi AWS utilizzando la console AWS CLI, l'API o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati

AWS Control Catalog non memorizza i dati dei clienti.

Crittografia dei dati a riposo

AWS Control Catalog non crittografa i dati dei clienti. Poiché i dati dei clienti non vengono mantenuti o conservati da AWS Control Catalog, non esistono linee guida specifiche per la crittografia inattiva.

Crittografia dei dati in transito

AWS Control Catalog non crittografa i dati dei clienti. Poiché nessun dato sensibile viene scambiato o reso persistente da AWS Control Catalog, non esistono linee guida specifiche per la crittografia in transito.

Gestione delle chiavi

La gestione delle chiavi di crittografia non si applica a AWS Control Catalog.

Riservatezza del traffico inter-rete

La privacy del traffico tra reti non si applica a AWS Control Catalog.

Gestione delle identità e degli accessi per Control Catalog

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di AWS Control Catalog. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come funziona Control Catalog con IAM](#)
- [Esempi di policy basate sull'identità per Control Catalog](#)
- [Risoluzione dei problemi di identità e accesso a Control Catalog](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi di identità e accesso a Control Catalog](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come funziona Control Catalog con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [Esempi di policy basate sull'identità per Control Catalog](#))

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.

- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Come funziona Control Catalog con IAM

Prima di utilizzare IAM per gestire l'accesso ad AWS Control Catalog, scopri quali funzionalità IAM sono disponibili per l'uso con AWS Control Catalog.

Funzionalità IAM che puoi utilizzare con Control Catalog

Funzionalità IAM	Supporto per AWS Control Catalog
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	No

Funzionalità IAM	Supporto per AWS Control Catalog
● Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come AWS Control Catalog e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta [AWS i servizi che funzionano con IAM nella IAM User Guide](#).

Policy basate sull'identità per AWS Control Catalog

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'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. 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 IAM.

Esempi di policy basate sull'identità per AWS Control Catalog

Per visualizzare esempi di policy basate sull'identità di AWS Control Catalog, consulta [Esempi di policy basate sull'identità per Control Catalog](#)

Policy basate sulle risorse all'interno di AWS Control Catalog

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 di 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.

In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni politiche per AWS Control Catalog

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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 in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di AWS Control Catalog, consulta [Azioni definite da AWS Control Catalog](#) nel Service Authorization Reference.

Le azioni politiche in AWS Control Catalog utilizzano il seguente prefisso prima dell'azione:

```
controlcatalog
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "controlcatalog:ListCommonControls",  
    "controlcatalog:ListDomains"  
]
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola List, includi la seguente operazione.

```
"Action": "controlcatalog:List*"
```

Per visualizzare esempi di policy basate sull'identità di AWS Control Catalog, consulta. [Esempi di policy basate sull'identità per Control Catalog](#)

Risorse relative alle policy per AWS Control Catalog

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse di AWS Control Catalog e relativi ARNs, consulta [Resources defined by AWS Control Catalog](#) nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta [Azioni definite da AWS Control Catalog](#).

Un dominio AWS Control Catalog ha il seguente formato Amazon Resource Name (ARN):

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

Un obiettivo di AWS Control Catalog ha il seguente formato ARN:

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

Un controllo comune di AWS Control Catalog ha il seguente formato ARN:

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

Per ulteriori informazioni sul formato di ARNs, consulta [Amazon Resource Names \(ARNs\)](#).

Ad esempio, per specificare il `i-1234567890abcdef0` dominio nella dichiarazione, utilizzare il seguente ARN.

```
"Resource": "arn:aws:controlcatalog:::domain/i-1234567890abcdef0" 
```

Per specificare tutte le istanze database che appartengono a un account specifico, utilizza il carattere jolly (*).

```
"Resource": "arn:aws:controlcatalog:::domain/*"
```

Alcune azioni di AWS Control Catalog, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Alcune azioni dell'API AWS Control Catalog supportano più risorse. Ad esempio, `ListCommonControls` accede a un controllo comune, a un obiettivo e a un dominio, quindi un principale deve disporre delle autorizzazioni per accedere a ciascuna di queste risorse. Per specificare più risorse in un'unica istruzione, separale ARNs con virgole.

```
"Resource": [  
    "commonControl",  
    "objective",  
    "domain"
```

Per visualizzare esempi di policy basate sull'identità di AWS Control Catalog, consulta [Esempi di policy basate sull'identità per Control Catalog](#)

Chiavi delle condizioni delle policy per AWS Control Catalog

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 entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. 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 visualizzare un elenco delle chiavi di condizione di AWS Control Catalog, consulta [Condition keys for AWS Control Catalog](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Actions defined by AWS Control Catalog](#).

Per visualizzare esempi di policy basate sull'identità di AWS Control Catalog, consulta [Esempi di policy basate sull'identità per Control Catalog](#)

ACLs in AWS Control Catalog

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.

ABAC con AWS Control Catalog

Supporta ABAC (tag nelle policy): No

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS Control Catalog

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per AWS Control Catalog

Supporta l'inoltro delle sessioni di accesso (FAS): no

Le sessioni di accesso diretto (FAS) utilizzano le autorizzazioni del principale chiamante al Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per AWS Control Catalog

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 [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di AWS Control Catalog. Modifica i ruoli di servizio solo quando AWS Control Catalog fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per AWS Control Catalog

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta [Servizi AWS supportati da IAM](#). Trova un servizio nella tabella che include un Yes nella colonna Service-linked

role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Control Catalog

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse di AWS Control Catalog. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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 di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da AWS Control Catalog, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per AWS Control Catalog](#) nel Service Authorization Reference.

Argomenti

- [Best practice per le policy](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Consenti agli utenti di visualizzare le risorse da AWS Control Catalog](#)

Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di AWS Control Catalog nel tuo account. Queste azioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy 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 maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere 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 privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente.

Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

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

```

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

```

Consenti agli utenti di visualizzare le risorse da AWS Control Catalog

La seguente policy concede le autorizzazioni per elencare domini, obiettivi e controlli comuni da AWS Control Catalog.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageControlCatalogAccess",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",

```

```
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
    ],
    "Resource": "*"
}
]
```

Risoluzione dei problemi di identità e accesso a Control Catalog

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere problemi comuni che potresti riscontrare quando lavori con AWS Control Catalog e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in Control Catalog](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Desidero consentire a persone esterne a me di Account AWS accedere alle risorse del mio Control Catalog](#)

Non sono autorizzato a eseguire un'azione in Control Catalog

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 `controlcatalog:GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
controlcatalog: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 `controlcatalog:GetWidget`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'iam:PassRoleazione, le tue policy devono essere aggiornate per consentirti di trasferire un ruolo ad AWS Control Catalog.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato marymajor tenta di utilizzare la console per eseguire un'azione in AWS Control Catalog. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione iam:PassRole.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne a me di Account AWS accedere alle risorse del mio Control Catalog

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 concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Control Catalog supporta queste funzionalità, consulta [Come funziona Control Catalog con IAM](#).
- 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 di IAM.

Convalida della conformità per Control Catalog

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta [AWS la documentazione sulla sicurezza](#).

Resilienza in Control Catalog

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Sicurezza dell'infrastruttura in Control Catalog

In quanto servizio gestito, Control Catalog è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper [Amazon Web Services: Overview of Security Processes](#).

Utilizzi chiamate API AWS pubblicate per accedere a Control Catalog attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Analisi della configurazione e delle vulnerabilità in Control Catalog

La configurazione e i controlli IT sono una responsabilità condivisa tra te AWS e te, nostro cliente. Per ulteriori informazioni, consulta il [modello di responsabilità AWS condivisa](#).

Monitoraggio di AWS Control Catalog

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Control Catalog e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per guardare AWS Control Catalog, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la [Guida per l'utente AWS CloudTrail](#).

Registrazione delle chiamate API di Control Catalog utilizzando AWS CloudTrail

Come parte di AWS Control Tower Control Catalog è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio. CloudTrail acquisisce tutte le chiamate API per Control Catalog come eventi. Le chiamate acquisite includono chiamate direttamente dalla AWS Control Tower console, ad esempio per abilitare o disabilitare un controllo, e chiamate di codice alle operazioni dell'API Control Catalog. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi relativi ai controlli in Control Catalog. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata a Control Catalog (tramite AWS Control Tower), l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

Controlla le informazioni del catalogo in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Control Catalog, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare

eventi recenti in Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo Account AWS, inclusi gli eventi per Control Catalog, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte le azioni del Control Catalog vengono registrate CloudTrail e documentate nel [Control Catalog API](#) Reference. . Ad esempio, le chiamate a `ListCommonControlsListObjectives`, e `ListDomains` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Informazioni sulle voci dei file di registro di Control Catalog

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni

sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ListDomains` azione.

```
{
  eventVersion:"1.05",
  userIdentity:{
    type:"IAMUser",
    principalId:"principalId",
    arn:"arn:aws:iam::accountId:user/userName",
    accountId:"111122223333",
    accessKeyId:"accessKeyId",
    userName:"userName",
    sessionContext:{
      sessionIssuer:{
      },
      webIdFederationData:{
      },
      attributes:{
        mfaAuthenticated:"false",
        creationDate:"2020-11-19T07:32:06Z"
      }
    }
  },
  eventTime:"2020-11-19T07:32:36Z",
  eventSource:"controlcatalog.amazonaws.com",
  eventName:"ListDomains",
  awsRegion:"us-west-2",
  sourceIPAddress:"sourceIPAddress",
  userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  requestParameters: null,
  responseElements: null,
  requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
  eventID:"a782029a-959e-4549-81df-9f6596775cb0",
  readOnly:false,
  eventType:"AwsApiCall",
  recipientAccountId:"recipientAccountId"
}
```

Access Control Catalog utilizzando un endpoint di interfaccia ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e Control Catalog. Puoi accedere a AWS Control Catalog come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere a Control Catalog.

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 Control Catalog.

Per ulteriori informazioni, consulta [Access Servizi AWS through AWS PrivateLink](#) nella Guida.AWS PrivateLink

Considerazioni per AWS Control Catalog

Prima di configurare un endpoint di interfaccia per Control Catalog, consulta [le considerazioni nella Guida](#).AWS PrivateLink

Control Catalog supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per Control Catalog

Puoi creare un endpoint di interfaccia per Control Catalog utilizzando la console Amazon VPC o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per Control Catalog utilizzando il seguente nome di servizio:

```
com.amazonaws.region.controlcatalog
```

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API a Control Catalog utilizzando il nome DNS regionale predefinito. Ad esempio, `service-name.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo a Control Catalog tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito a Control Catalog dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di 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.

Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

Esempio: policy degli endpoint VPC per le azioni di Control Catalog

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleggi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni elencate di AWS Control Catalog a tutti i principali su tutte le risorse.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

 Note

Le operazioni `GetControl` e `ListControls` API richiedono un'autorizzazione diversa, l'autorizzazione completa predefinita. Per un esempio, consulta [la politica degli endpoint predefinita](#).

Cronologia dei documenti per la guida alle informazioni sulla sicurezza di Control Catalog

La tabella seguente descrive le versioni della documentazione per Control Catalog.

Modifica	Descrizione	Data
Versione iniziale	Versione iniziale di Control Catalog APIs e guida alle informazioni sulla sicurezza.	8 aprile 2024

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.