aws

Guida per l'utente

AWS Elemental MediaStore

AWS Elemental MediaStore: Guida per l'utente

Table of Contents

Cos'è AWS Elemental MediaStore?

AWS Elemental MediaStore è un servizio di origine e archiviazione video che offre le alte prestazioni e la coerenza immediata necessarie per l'origine live. Con MediaStore, puoi gestire le risorse video come oggetti in contenitori per creare flussi di lavoro multimediali affidabili e basati sul cloud.

Per usare il servizio, è possibile caricare gli oggetti da una sorgente, ad esempio un codificatore o feed di dati, in un container creato in MediaStore.

MediaStore è un'ottima scelta per archiviare file video frammentati quando è necessaria una forte coerenza, letture e scritture a bassa latenza e la capacità di gestire elevati volumi di richieste simultanee. Se non offri video in streaming live, prendi in considerazione l'utilizzo di Amazon Simple Storage Service (Amazon S3).

Argomenti

MediaStore Concetti e terminologia di AWS Elemental

ARN

Un Amazon Resource Name.

Body

I dati da caricare in un oggetto.

Intervallo (Byte)

Un sottoinsieme di dati di oggetto da esaminare. Per ulteriori informazioni, consulta intervallo dalla specifica HTTP.

Container

Uno spazio dei nomi che contiene gli oggetti. Un container ha un endpoint che è possibile utilizzare per scrivere e recuperare oggetti e collegare policy di accesso.

Endpoint

Un punto di accesso al MediaStore servizio, fornito come URL root HTTPS.

ETag

Un tag di entità che è un hash dei dati di oggetto.

Cartella

Una divisione di un container. Una cartella può contenere oggetti e altre cartelle.

Elemento

Termine utilizzato per fare riferimento a oggetti e cartelle.

Oggetto

Una risorsa, simile a un oggetto Amazon S3. Gli oggetti sono le entità fondamentali archiviate in MediaStore. Il servizio accetta tutti i tipi di file.

Servizio di emissione

MediaStore è considerato un servizio di origine perché è il punto di distribuzione per la distribuzione di contenuti multimediali.

Percorso

Un identificatore univoco di un oggetto o di una cartella, che ne indica la posizione nel container.

Parte

Un sottoinsieme di dati (blocco) di un oggetto.

Policy

Una policy IAM.

Risorsa

Un'entità in AWS che è possibile utilizzare. A ogni risorsa AWS viene assegnato un Amazon Resource Name (ARN) che agisce come un identificatore unico. In MediaStore, questa è la risorsa e il suo formato ARN:

- Container: `aws:mediastore:`*`region`*`:`*`account-id`*`:container/:`*`containerName`*

Servizi correlati

- Amazon CloudFront è un servizio globale di rete per la distribuzione di contenuti (CDN) che fornisce dati e video in modo sicuro ai tuoi spettatori. Puoi usare CloudFront per distribuire contenuti con le migliori prestazioni possibili. Per ulteriori informazioni, consulta l'Amazon CloudFront Developer Guide.
- AWS CloudFormation è un servizio che consente di modellare e configurare le risorse AWS. Crei un modello che descrive tutte le AWS risorse che desideri (come i MediaStore contenitori) e AWS CloudFormation si occupa del provisioning e della configurazione di tali risorse per te. Non è necessario creare e configurare singolarmente le risorse AWS e determinare le dipendenze, perché è AWS CloudFormation a gestire tutti questi aspetti. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudFormation.
- AWS CloudTrailè un servizio che ti consente di monitorare le chiamate effettuate all' CloudTrail API per il tuo account, incluse le chiamate effettuate dalla Console di gestione AWS e altri servizi. AWS CLI Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.
- Amazon CloudWatch è un servizio di monitoraggio delle risorse AWS cloud e delle applicazioni su cui eseguiAWS. Usa CloudWatch Events per tenere traccia delle modifiche allo stato dei contenitori e degli oggetti in MediaStore. Per ulteriori informazioni, consulta la CloudWatch documentazione di Amazon.
- AWS Identity and Access Management (IAM) è un servizio Web che aiuta a controllare in modo sicuro l'accesso alle risorse AWS per gli utenti. Utilizza IAM per stabilire chi può utilizzare le tue risorse (autenticazione) AWS, quali risorse e in che modo (autorizzazione). Per ulteriori informazioni, consulta Configurazione di AWS Elemental MediaStore.
- Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) è uno storage di oggetti progettato per archiviare e recuperare qualsiasi quantità di dati da qualsiasi luogo. Per ulteriori informazioni, consulta la Documentazione di Amazon S3.

Accesso ad AWS Elemental MediaStore

È possibile accedere MediaStore utilizzando uno dei seguenti metodi:

- Console di gestione AWS: le procedure riportate in questa guida spiegano come utilizzare la Console di gestione AWS per eseguire attività per MediaStore. Per accedere MediaStore tramite la console:

```
https://<region>.console.aws.amazon.com/mediastore/home
```

- AWS Command Line Interface— Per ulteriori informazioni, consulta la Guida AWS Command Line Interface per l'utente. Per accedere MediaStore utilizzando l'endpoint CLI:

```
aws mediastore
```

- MediaStore API: se utilizzi un linguaggio di programmazione per il quale non è disponibile un SDK, consulta l'AWS Elemental MediaStoreAPI Reference per informazioni sulle azioni API e su come effettuare richieste API. Per accedere MediaStore utilizzando l'endpoint dell'API REST:

```
https://mediastore.<region>.amazonaws.com
```

- SDK AWS: se usi un linguaggio di programmazione per cui AWS fornisce un SDK, puoi utilizzare un SDK per accedere a MediaStore. Gli SDK semplificano l'autenticazione, si integrano senza difficoltà nel tuo ambiente di sviluppo e ti offrono semplice accesso ai comandi di MediaStore . Per ulteriori informazioni, consulta Strumenti per Amazon Web Services.
- AWS Tools per Windows PowerShell: per ulteriori informazioni, consulta la Guida per AWS Tools for Windows PowerShell l'utente.

Prezzi per AWS Elemental MediaStore

Come per gli altri AWS prodotti, non sono previsti contratti o impegni minimi per l'utilizzo MediaStore. Verrà addebitata una tariffa di consumo per GB quando i contenuti arrivano al servizio e una tariffa mensile per GB per i contenuti archiviati nel servizio. Per ulteriori informazioni, consulta i prezzi di AWS Elemental MediaStore .

Regioni ed endpoint per AWS Elemental MediaStore

Per ridurre la latenza dei dati nelle tue applicazioni, MediaStore offre un endpoint regionale per effettuare la tua richiesta:

```
https://mediastore.<region>.amazonaws.com
```

Per visualizzare l'elenco completo delle regioni AWS in cui MediaStore è disponibile, consulta gli MediaStore endpoint e le quote di AWS Elemental nell'AWS General Reference.

Configurazione di AWS Elemental MediaStore

Questa sezione ti guida attraverso i passaggi necessari per configurare gli utenti per accedere ad AWS MediaStore Elemental. Per informazioni di base e aggiuntive sulla gestione delle identità e degli accessi per MediaStore, consultaIdentity and Access Management per AWS Elemental MediaStore.

Per iniziare a usare AWS Elemental MediaStore, completa i seguenti passaggi.

Argomenti

Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

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

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

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

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

Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accesso come utente root della Guida per l'utente di Accedi ad AWS.
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per ricevere istruzioni, consulta Abilitazione di un dispositivo MFA virtuale per l'utente root dell'Account AWS (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita IAM Identity Center.

   Per istruzioni, consulta Enabling AWS IAM Identity Center nella Guida AWS IAM Identity Center per l'utente.
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente amministrativo.

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

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta Accedere al portale di accesso AWS nella Guida per l'utente Accedi ad AWS.

Nozioni base su AWS Elemental MediaStore

Questo tutorial introduttivo mostra come usare AWS MediaStore Elemental per creare un contenitore e caricare un oggetto.

Argomenti

Fase 1: Accedere ad AWS Elemental MediaStore

Dopo aver configurato l'account AWS e creato utenti e ruoli, accedi alla console di AWS Elemental MediaStore.

Per accedere ad AWS Elemental MediaStore

- Accedere aAWS Management Console e aprire la MediaStore console all'indirizzo https://console.aws.amazon.com/mediastore/.

> **Note**
>
> Puoi effettuare l'accesso utilizzando le credenziali IAM create per questo account. Per informazioni su come creare le credenziali IAM, consulta Configurazione di AWS Elemental MediaStore.

Fase 2: creare un container

Utilizzi i contenitori in AWS MediaStore Elemental per archiviare cartelle e oggetti. I container consentono di raggruppare oggetti correlati nello stesso modo in cui si utilizza una directory per raggruppare i file in un file system. Non ti verrà addebitato alcun costo durante la creazione dei container; ti verranno addebitati i costi solo quando caricherai un oggetto in un container.

Per creare un container

1. Nella pagina Containers (Container), scegliere Create container (Crea container).
2. In Container name (Nome container) digita un nome per il container. Per ulteriori informazioni, consulta Regole per i nomi di container.
3. Scegli Crea contenitore. AWS Elemental MediaStore aggiunge il nuovo contenitore a un elenco di contenitori. Inizialmente, lo stato del container è Creating (In fase di creazione), quindi diventa Active (Attivo).

Fase 3: caricare un oggetto

Puoi caricare gli oggetti (con dimensioni massime di 25 MB per oggetto) in un container o in una cartella all'interno di un container. Per caricare un oggetto in una cartella, devi specificare il percorso della cartella. Se la cartella esiste già, AWS Elemental MediaStore memorizza l'oggetto nella cartella. Se la cartella non esiste, il servizio la crea e quindi archivia l'oggetto nella cartella.

> **Note**
>
> I nomi di file di oggetti possono contenere solo lettere, numeri, punti (.), trattini bassi (_), tilde (~) e trattini (-).

Per caricare un oggetto

1. Nella pagina Containers scegli il nome del container appena creato. Viene visualizzata la pagina dei dettagli del container.
2. Scegli Upload object (Carica oggetto).
3. In Target path (Percorso di destinazione) digita un percorso per le cartelle. Ad esempio, `premium/canada`. Se una delle cartelle del percorso non esiste ancora, AWS Elemental le MediaStore crea automaticamente.
4. Per Object (Oggetto), scegli Browse (Sfoglia).
5. Passa alla cartella appropriata e scegli un oggetto da caricare.
6. Seleziona Open (Apri), quindi Upload (Carica).

Fase 4: accedere a un oggetto

Puoi scaricare i tuoi oggetti in un endpoint specificato.

1. Nella pagina Containers (Container), scegli il nome del container che contiene l'oggetto da scaricare.
2. Se l'oggetto che desideri scaricare si trova in una sottocartella, continua a selezionare i nomi di cartella fino a visualizzare l'oggetto.
3. Scegli il nome dell'oggetto.
4. Nella pagina dei dettagli per l'oggetto, scegli Download (Scarica).

Container in AWS ElementalMediaStore

Usa i container in MediaStore per archiviare le cartelle e gli oggetti. Gli oggetti correlati possono essere raggruppati in container come si fa con una directory per raggruppare i file in un file system. Non ti verrà addebitato alcun costo durante la creazione dei container; ti verranno addebitati i costi solo quando caricherai un oggetto in un container. Per ulteriori informazioni sui costi, consultaAWS ElementalMediaStorePrezzi.

Argomenti

Regole per i nomi di container

Quando scegli un nome per il container, ricorda quanto segue:

- Il nome deve essere univoco all'interno dell'account corrente per la regione AWS corrente.
- Il nome può contenere lettere maiuscole e minuscole, numeri e caratteri di sottolineatura (_).
- Il nome deve contenere da 1 a 255 caratteri.
- I nomi rispettano la distinzione tra lettere maiuscole e minuscole. Ad esempio, puoi avere un container denominato `myContainer` e una cartella denominata `mycontainer` perché tali nomi sono univoci.
- Un container non può essere rinominato dopo che è stato creato.

Creazione di un container

Puoi creare fino a 100 container per ogni account AWS. Puoi creare il numero di cartelle che desideri, per non più di 10 livelli all'interno di un container. Inoltre, è possibile caricare il numero di oggetti che desideri in ogni contenitore.

> **Tip**
>
> Puoi anche creare un container automaticamente utilizzando un modello AWS CloudFormation. Il modello AWS CloudFormation gestisce i dati per cinque operazioni API: creazione di un container, impostazione della registrazione degli accessi, aggiornamento della policy del container di default, aggiunta di una policy CORS e aggiunta della policy del ciclo di vita degli oggetti. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudFormation.

Per creare un container (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere Create container (Crea container).
3. In Container name (Nome container) immettere un nome per il container. Per ulteriori informazioni, consultare . Regole per i nomi di container .
4. ScegliereCreazione di container. AWS ElementalMediaStoreaggiunge il nuovo container a un elenco di container. Inizialmente, lo stato del container è Creating (In fase di creazione), quindi diventa Active (Attivo).

Per creare un container (AWS CLI)

- In AWS CLI, usa il comando `create-container`.

```
aws mediastore create-container --container-name ExampleContainer --region us-
west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "Container": {
        "AccessLoggingEnabled": false,
        "CreationTime": 1563557265.0,
        "Name": "ExampleContainer",
        "Status": "CREATING",
        "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleContainer"
    }
```

```
}
```

Visualizzazione dei dettagli di un container

I dettagli per un container includono la policy, l'endpoint, l'ARN e l'ora di creazione.

Per visualizzare i dettagli di un container (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container) scegliere il nome del container.

   Viene visualizzata la pagina dei dettagli del container. Questa pagina si articola in due sezioni:

   - La sezione Objects (Oggetti), in cui sono elencati gli oggetti e le cartelle nel container.
   - La sezione Container policy (Policy di container), che mostra la policy basata su risorse associata a questo container. Per ulteriori informazioni sulle policy basate su risorse, consultare Policy di container.

Per visualizzare i dettagli di un container (AWS CLI)

- In AWS CLI, usa il comando `describe-container`.

```
aws mediastore describe-container --container-name ExampleContainer --region us-
west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "Container": {
        "CreationTime": 1563558086.0,
        "AccessLoggingEnabled": false,
        "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleContainer",
        "Status": "ACTIVE",
        "Name": "ExampleContainer",
        "Endpoint": "https://aaabbbcccdddee.data.mediastore.us-
west-2.amazonaws.com"
    }
```

```
}
```

Visualizzazione di un elenco di container

Puoi visualizzare un elenco di tutti i container associati al tuo account.

Per visualizzare un elenco di container (console)

- Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.

  Viene visualizzata la pagina Containers (Container), con l'elenco di tutti i contenitori associati al tuo account.

Per visualizzare un elenco di container (AWS CLI)

- In AWS CLI, usa il comando `list-containers`.

```
aws mediastore list-containers --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "Containers": [
        {
            "CreationTime": 1505317931.0,
            "Endpoint": "https://aaabbbcccdddee.data.mediastore.us-
west-2.amazonaws.com",
            "Status": "ACTIVE",
            "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleLiveDemo",
            "AccessLoggingEnabled": false,
            "Name": "ExampleLiveDemo"
        },
        {
            "CreationTime": 1506528818.0,
            "Endpoint": "https://fffggghhhiiijj.data.mediastore.us-
west-2.amazonaws.com",
            "Status": "ACTIVE",
            "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleContainer",
```

```
            "AccessLoggingEnabled": false,
            "Name": "ExampleContainer"
        }
    ]
}
```

Eliminazione di un container

Puoi eliminare un container solo se non contiene oggetti.

Per eliminare un container (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere l'opzione a sinistra del nome del container.
3. Scegliere Delete (Elimina).

Per eliminare un container (AWS CLI)

- In AWS CLI, usa il comando `delete-container`.

  ```
  aws mediastore delete-container --container-name=ExampleLiveDemo --region us-west-2
  ```

  Il comando non ha un valore restituito.

Policy di AWS ElementalMediaStore

Puoi applicare una o più di queste policy al AWS ElementalMediaStorecontainer:

- Policy di container- Imposta i diritti di accesso a tutte le cartelle e gli oggetti all'interno del container. MediaStoreimposta un criterio predefinito che consente agli utenti di eseguire tuttiMediaStoreoperazioni sul contenitore. Questa policy specifica che tutte le operazioni devono essere eseguite su HTTPS. Dopo aver creato un container, puoi modificarne la policy.
- Policy CORS (CRS-Origin Resource Sharing)- Consente alle applicazioni Web client caricate da un dominio di interagire con le risorse caricate in un dominio differente. MediaStorenon imposta un criterio CORS predefinito.
- Policy di parametro- ConsenteMediaStoreper inviare parametri ad AmazonCloudWatch. MediaStorenon imposta una policy di parametro di default.
- Policy del ciclo di vita degli oggetti- Controlla la durata di permanenza degli oggetti in unMediaStorecontainer. MediaStorenon imposta una policy del ciclo di vita degli oggetti di default.

Politiche per i container in AWS ElementalMediaStore

Ogni container presenta una policy basata su risorse che gestisce i diritti di accesso a tutte le cartelle e agli oggetti in tale container. La policy di default, che viene automaticamente collegata a tutti i nuovi container, consente l'accesso a tutti i AWS ElementalMediaStoreoperazioni sul contenitore. e specifica che tale accesso ha la condizione di richiedere il protocollo HTTPS per le operazioni. Dopo aver creato un container, puoi modificare la policy collegata a tale container.

Puoi anche specificare una policy del ciclo di vita degli oggetti che regola la data di scadenza degli oggetti in un container. Dopo che gli oggetti raggiungono l'età massima specificata, il servizio elimina gli oggetti dal container.

Argomenti

- Visualizzazione di una policy di container
- Modifica di una policy di container
- Policy di container di esempio

Visualizzazione di una policy di container

Puoi utilizzare la console o la AWS CLI per visualizzare la policy basata su risorse di un container.

Per visualizzare una policy di container (console)

1. Apertura dellaMediaStoreConsole alhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere il nome del container.

   Viene visualizzata la pagina dei dettagli del container. La policy viene visualizzata nella sezione Container policy (Policy container).

Per visualizzare una policy di container (AWS CLI)

- In AWS CLI, usa il comando `get-container-policy`.

```
aws mediastore get-container-policy --container-name ExampleLiveDemo --region us-
west-2
```

L'esempio seguente mostra il valore restituito:

```
{
  "Policy": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "PublicReadOverHttps",
        "Effect": "Allow",
        "Principal": {
          "AWS": "arn:aws:iam::111122223333:root",
        },
        "Action": [
          "mediastore:GetObject",
          "mediastore:DescribeObject",
        ],
        "Resource": "arn:aws:mediastore:us-
west-2:111122223333:container/ExampleLiveDemo/*",
        "Condition": {
          "Bool": {
            "aws:SecureTransport": "true"
          }
```

```
        }
      }
    ]
  }
}
```

Modifica di una policy di container

È possibile modificare le autorizzazioni nella policy di container predefinita o crearne una nuova per sostituirla. Affinché la nuova policy diventi effettiva, sono necessari fino a cinque minuti.

Per modificare una policy di container (console)

1. Apertura dellaMediaStoreConsole alhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere il nome del container.
3. Selezionare Edit policy (Modifica policy). Esempi di impostazione di autorizzazioni diverse sono disponibili su the section called “Policy di container di esempio”.
4. Apportare le opportune modifiche e selezionare Save (Salva).

Per modificare una policy di container (AWS CLI)

1. Crea un file che definisca la policy del container:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadOverHttps",
      "Effect": "Allow",
      "Action": ["mediastore:GetObject", "mediastore:DescribeObject"],
      "Principal": "*",
      "Resource": "arn:aws:mediastore:us-
west-2:111122223333:container/ExampleLiveDemo/*",
      "Condition": {
        "Bool": {
            "aws:SecureTransport": "true"
        }
      }
    }
  ]
```

```
}
```

2. In AWS CLI, usa il comando `put-container-policy`.

```
aws mediastore put-container-policy --container-name ExampleLiveDemo --
policy file://ExampleContainerPolicy.json --region us-west-2
```

Il comando non ha un valore restituito.

Policy di container di esempio

Gli esempi seguenti mostrano policy di container costruite per diversi gruppi di utenti.

Argomenti

- Policy di container di esempio: Default (predefinito)
- Policy di container di esempio: Accesso in lettura pubblico su HTTPS
- Policy di container di esempio: Accesso in lettura pubblico su HTTP o HTTPS
- Policy di container di esempio: Accesso in lettura multiaccount con abilitazione HTTP
- Policy di container di esempio: Accesso in lettura multiaccount su HTTPS
- Policy di container di esempio: Accesso in lettura multiaccount a un ruolo
- Policy di container di esempio: Accesso completo multiaccount a un ruolo
- Policy di container di esempio: Accesso limitato a indirizzi IP specifici

Policy di container di esempio: Default (predefinito)

Quando crei un contenitore, AWS ElementalMediaStoreapplica automaticamente le seguenti policy basate su risorse:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "MediaStoreFullAccess",
      "Action": [ "mediastore:*" ],
      "Principal":{
          "AWS" : "arn:aws:iam::<aws_account_number>:root"},
      "Effect": "Allow",
```

```
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
      "Condition": {
        "Bool": { "aws:SecureTransport": "true" }
      }
    }
  ]
}
```

La policy è integrata nel servizio, quindi non è necessario crearla. Tuttavia, è possibilemodifica della policynel contenitore se le autorizzazioni nel criterio predefinito non sono allineate con le autorizzazioni che si desidera utilizzare per il contenitore.

La policy predefinita assegnata a tutti i nuovi container consente l'accesso a tutte le operazioni di MediaStore sul container e specifica che tale accesso ha la condizione di richiedere il protocollo HTTPS per le operazioni.

Policy di container di esempio: Accesso in lettura pubblico su HTTPS

Questa policy di esempio consente agli utenti di recuperare un oggetto tramite una richiesta HTTPS. Consente accesso in lettura a chiunque su una connessione SSL/TLS protetta, utenti autenticati e anonimi (utenti che non sono connessi). L'istruzione ha il nome `PublicReadOverHttps`. Consente l'accesso alle operazioni `GetObject` e `DescribeObject` su qualsiasi oggetto (come specificato dal simbolo * alla fine del percorso della risorsa) e specifica che tale accesso ha la condizione di richiedere il protocollo HTTPS per le operazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadOverHttps",
      "Effect": "Allow",
      "Action": ["mediastore:GetObject", "mediastore:DescribeObject"],
      "Principal": "*",
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
      "Condition": {
        "Bool": {
            "aws:SecureTransport": "true"
        }
      }
    }
```

```
  ]
}
```

Policy di container di esempio: Accesso in lettura pubblico su HTTP o HTTPS

Questa policy di esempio consente l'accesso alle operazioni `GetObject` e `DescribeObject` su qualsiasi oggetto (come specificato dal simbolo * alla fine del percorso della risorsa). Consente accesso in lettura a chiunque, compresi tutti gli utenti autenticati e quelli anonimi (gli utenti che non sono connessi):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadOverHttpOrHttps",
      "Effect": "Allow",
      "Action": ["mediastore:GetObject", "mediastore:DescribeObject"],
      "Principal": "*",
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
      "Condition": {
        "Bool": { "aws:SecureTransport": ["true", "false"] }
      }
    }
  ]
}
```

Policy di container di esempio: Accesso in lettura multiaccount con abilitazione HTTP

Questa policy di esempio consente agli utenti di recuperare un oggetto attraverso una richiesta HTTP. Consente l'accesso agli utenti autenticati con accesso multiaccount. Non è necessario che l'oggetto sia ospitato in un server con un certificato SSL/TLS:

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Sid" : "CrossAccountReadOverHttpOrHttps",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::<other acct number>:root"
    },
    "Action" : [ "mediastore:GetObject", "mediastore:DescribeObject" ],
```

```
    "Resource" : "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : [ "true", "false" ]
      }
    }
  } ]
}
```

Policy di container di esempio: Accesso in lettura multiaccount su HTTPS

Questa policy di esempio consente l'accesso allaGetObjecteDescribeObjectoperazioni su qualsiasi oggetto (come specificato dal valore * alla fine del percorso della risorsa) di proprietà dell'utente root dell'account specificato<other acct number>. e specifica che tale accesso ha la condizione di richiedere il protocollo HTTPS per le operazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountReadOverHttps",
      "Effect": "Allow",
      "Action": ["mediastore:GetObject", "mediastore:DescribeObject"],
      "Principal":{
        "AWS": "arn:aws:iam::<other acct number>:root"},
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
      "Condition": {
        "Bool": {
            "aws:SecureTransport": "true"
        }
      }
    }
  ]
}
```

Policy di container di esempio: Accesso in lettura multiaccount a un ruolo

La policy di esempio consente di accedere alle operazioni `GetObject` e `DescribeObject` su qualsiasi oggetto (come specificato dal simbolo * alla fine del percorso della risorsa) di proprietà

dell'account <numero account proprietario>. Consente l'accesso a qualsiasi utente dell'account <numero altro account> se tale account ha assunto il ruolo specificato in <nome ruolo>:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountRoleRead",
      "Effect": "Allow",
      "Action": ["mediastore:GetObject", "mediastore:DescribeObject"],
      "Principal":{
        "AWS": "arn:aws:iam::<other acct number>:role/<role name>"},
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
    }
  ]
}
```

Policy di container di esempio: Accesso completo multiaccount a un ruolo

Questa policy di esempio consente accesso multiaccount per aggiornare qualsiasi oggetto nell'account, se l'utente è connesso tramite HTTP. Inoltre, consente accesso multiaccount per eliminare, scaricare e descrivere gli oggetti su HTTP o HTTPS in un account che ha assunto il ruolo specificato:

- La prima istruzione è `CrossAccountRolePostOverHttps`. Consente l'accesso all'operazione `PutObject` su qualsiasi oggetto e consente l'accesso a qualsiasi utente dell'account specificato se tale account ha assunto il ruolo specificato in <nome ruolo>. Specifica che l'accesso ha la condizione di richiedere il protocollo HTTPS per l'operazione (tale condizione deve sempre essere inclusa quando si assegna l'accesso a `PutObject`).

  In altre parole, qualsiasi principale che abbia un accesso multiaccount può accedere a `PutObject`, ma solo tramite HTTPS.
- La seconda istruzione è `CrossAccountFullAccessExceptPost`. Consente l'accesso a tutte le operazioni tranne `PutObject` su qualsiasi oggetto. Consente questo accesso a qualsiasi utente dell'account specificato se tale account ha assunto il ruolo specificato in <nome ruolo>. Questo accesso non ha la condizione di richiedere il protocollo HTTPS per le operazioni.

In altre parole, qualsiasi account con accesso multiaccount può accedere a `DeleteObject`, `GetObject` e così via (ma non a `PutObject`) e può eseguire questa operazione su HTTP o HTTPS.

La seconda istruzione non sarà valida se non viene escluso `PutObject`, perché per includere `PutObject` è necessario impostare esplicitamente HTTPS come condizione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountRolePostOverHttps",
      "Effect": "Allow",
      "Action": "mediastore:PutObject",
      "Principal":{
        "AWS": "arn:aws:iam::<other acct number>:role/<role name>"},
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*",
      "Condition": {
        "Bool": {
            "aws:SecureTransport": "true"
        }
      }
    },
    {
      "Sid": "CrossAccountFullAccessExceptPost",
      "Effect": "Allow",
      "NotAction": "mediastore:PutObject",
      "Principal":{
        "AWS": "arn:aws:iam::<other acct number>:role/<role name>"},
      "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/<container
 name>/*"
    }
  ]
}
```

Policy di container di esempio: Accesso limitato a indirizzi IP specifici

Questa policy di esempio consente l'accesso a tutte le AWS ElementalMediaStoreoperazioni su oggetti nel container specificato. La richiesta deve, tuttavia, avere origine dall'intervallo di indirizzi IP specificati nella condizione.

La condizione in questa istruzione identifica l'intervallo 198.51.100.* di indirizzi IP di Internet Protocol versione 4 (IPv4) consentiti, con un'unica eccezione: 198.51.100.188.

Il blocco `Condition` utilizza le condizioni `IpAddress` e `NotIpAddress` e la chiave di condizione `aws:SourceIp`, che è una chiave di condizione AWS. I valori IPv4 `aws:sourceIp` utilizzano la notazione CIDR standard. Per ulteriori informazioni, consultaOperatori di condizione con indirizzo IPNella Guida per l'utente di IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessBySpecificIPAddress",
            "Effect": "Allow",
            "Action": [
                "mediastore:GetObject",
                "mediastore:DescribeObject"
            ],
            "Principal": "*",
            "Resource": "arn:aws:mediastore:<region>:<owner acct number>:container/
<container name>/*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "198.51.100.0/24"
                    ]
                },
                "NotIpAddress": {
                    "aws:SourceIp": "198.51.100.188/32"
                }
            }
        }
    ]
}
```

Policy CORS (Cross-Origin Resource Sharing) in AWS ElementalMediaStore

La funzionalità CORS (Cross-Origin Resource Sharing, condivisione delle risorse multiorigine) definisce un metodo con cui le applicazioni Web dei clienti caricate in un dominio possono interagire con le risorse situate in un dominio differente. Con il supporto CORS in AWS ElementalMediaStore, è possibile creare applicazioni Web lato client complete conMediaStoree consenti in modo selettivo l'accesso cross-origin al tuoMediaStorerisorse AWS.

> **Note**
>
> Se utilizzi AmazonCloudFrontper distribuire contenuti da un contenitore che dispone di una politica CORS, assicurati diconfigurare la distribuzione per AWS ElementalMediaStore(incluso il passaggio per modificare il comportamento della cache per configurare CORS).

In questa sezione viene fornita una panoramica della funzionalità CORS. Negli argomenti secondari viene descritto come abilitare la funzionalità CORS utilizzando AWS ElementalMediaStoreconsole o utilizzando a livello di programmazioneMediaStoreAPI REST e gli SDK AWS.

Argomenti

Scenari di casi d'uso di CORS

Di seguito sono riportati alcuni scenari di esempio per l'uso della funzionalità CORS.

- Scenario 1: Supponi di distribuire video in streaming live in un AWS ElementalMediaStoredenominato containerLiveVideo. I tuoi utenti caricano l'endpoint manifest del

video `http://livevideo.mediastore.ap-southeast-2.amazonaws.com` da un'origine specifica come `www.example.com`. Intendi utilizzare unaJavaScriptper accedere a tutti i video provenienti da questo container tramite non autenticati`GET`e`PUT`. In genere, un browser bloccaJavaScriptdall'consentire queste richieste, ma puoi impostare una policy CORS nel container in modo da consentire esplicitamente queste richieste da`www.example.com`.

- Scenario 2: Supponi di voler ospitare la stessa diretta streaming dello Scenario 1 dalMediaStorecontainer, ma vogliono consentire richieste da qualsiasi origine. Puoi configurare una policy CORS per consentire origini contrassegnate con un carattere jolly (*), in modo che le richieste da qualsiasi origine possono accedere al video.

Aggiunta di una policy CORS a un container

In questa sezione viene descritto come aggiungere una configurazione CORS (Cross-Origin Resource Sharing) a un AWS ElementalMediaStore. La funzionalità CORS consente l'interazione tra le applicazioni client Web caricate in un dominio e le risorse situate in un altro dominio.

Per configurare il container per permettere richieste multiorigine, aggiungi una policy CORS al container. La policy CORS definisce le regole che identificano le origini che potranno accedere al container, le operazioni (metodi HTTP) supportate per ogni origine e altre informazioni specifiche dell'operazione.

Quando aggiungi una policy CORS al container, le policy del container (che disciplinano i diritti di accesso al container) continueranno a essere applicate.

Per aggiungere una policy CORS (console)

1. Apertura dellaMediaStorela consolehttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container per il quale vuoi creare una policy CORS.

   Viene visualizzata la pagina dei dettagli del container.
3. Nella sezione Container CORS policy (Policy CORS del container) scegli Create CORS policy (Crea policy CORS).
4. Inserisci la policy in formato JSON e quindi scegli Save (Salva).

Per aggiungere una policy CORS (AWS CLI)

1. Creare un file che definisca la policy CORS:

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "HEAD"
    ],
    "AllowedOrigins": [
      "*"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

2. In AWS CLI, usa il comando `put-cors-policy`.

```
aws mediastore put-cors-policy --container-name ExampleContainer --cors-policy
 file://corsPolicy.json --region us-west-2
```

   Il comando non ha un valore restituito.

Visualizzazione di una policy CORS

La funzionalità CORS (Cross-Origin Resource Sharing, condivisione delle risorse multiorigine) definisce un metodo con cui le applicazioni Web dei clienti caricate in un dominio possono interagire con le risorse situate in un dominio differente.

Per visualizzare una policy CORS (console)

1. Apertura dellaMediaStorela consolehttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container di cui vuoi visualizzare la policy CORS.

Viene visualizzata la pagina dei dettagli del container con la policy CORS nella sezione Container CORS policy (Policy CORS del container).

Per visualizzare una policy CORS (AWS CLI)

- In AWS CLI, usa il comando `get-cors-policy`.

```
aws mediastore get-cors-policy --container-name ExampleContainer --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "CorsPolicy": [
        {
            "AllowedMethods": [
                "GET",
                "HEAD"
            ],
            "MaxAgeSeconds": 3000,
            "AllowedOrigins": [
                "*"
            ],
            "AllowedHeaders": [
                "*"
            ]
        }
    ]
}
```

Modifica di una policy CORS

La funzionalità CORS (Cross-Origin Resource Sharing, condivisione delle risorse multiorigine) definisce un metodo con cui le applicazioni Web dei clienti caricate in un dominio possono interagire con le risorse situate in un dominio differente.

Per modificare una policy CORS (console)

1. Apertura dellaMediaStorela consolehttps://console.aws.amazon.com/mediastore/.

2. Nella pagina Containers (Container), scegli il nome del container di cui vuoi modificare la policy CORS.

   Viene visualizzata la pagina dei dettagli del container.

3. Nella sezione Container CORS policy (Policy CORS del container) scegli Edit CORS policy (Modifica policy CORS).
4. Effettua le modifiche alla policy, quindi scegli Save (Salva).

Per modificare una policy CORS (AWS CLI)

1. Creare un file che definisca la policy CORS aggiornata:

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://www.example.com"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

2. In AWS CLI, usa il comando `put-cors-policy`.

```
aws mediastore put-cors-policy --container-name ExampleContainer --cors-policy
 file://corsPolicy2.json --region us-west-2
```

   Il comando non ha un valore restituito.

Eliminazione di una policy CORS

La funzionalità CORS (Cross-Origin Resource Sharing, condivisione delle risorse multiorigine) definisce un metodo con cui le applicazioni Web dei clienti caricate in un dominio possono interagire

con le risorse situate in un dominio differente. L'eliminazione di una policy CORS da un container rimuove le autorizzazioni per le richieste multiorigine.

Per eliminare una policy CORS (console)

1. Apertura dellaMediaStorela consolehttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container di cui vuoi eliminare la policy CORS.

   Viene visualizzata la pagina dei dettagli del container.
3. Nella sezione Container CORS policy (Policy CORS del container) scegli Delete CORS policy (Elimina policy CORS).
4. Scegli Continue (Continua) per confermare, quindi scegli Save (Salva).

Per eliminare una policy CORS (AWS CLI)

- In AWS CLI, usa il comando `delete-cors-policy`.

  ```
  aws mediastore delete-cors-policy --container-name ExampleContainer --region us-west-2
  ```

  Il comando non ha un valore restituito.

Risoluzione dei problemi correlati alla configurazione CORS

Se si verifica un comportamento imprevisto quando accedi a un container che dispone di una policy CORS, segui questa procedura per risolvere il problema.

1. Verifica che la policy CORS sia collegata al container.

   Per istruzioni, consultare the section called “Visualizzazione di una policy CORS”.
2. Acquisisci la richiesta e la risposta complete utilizzando uno strumento di tua scelta (ad esempio la console di sviluppo del browser). Verifica che la policy CORS collegata al container includa almeno una regola CORS che soddisfi i dati nella richiesta, come segue:

   a. Verifica che la richiesta abbia un'intestazione `Origin`.

Se l'intestazione non è presente, AWS ElementalMediaStorenon considera la richiesta come una richiesta multiorigine e non riinvia le intestazioni della risposta CORS nella risposta.

b. Verifica che l'intestazione `Origin` nella richiesta corrisponda ad almeno uno degli elementi `AllowedOrigins` nella `CORSRule` specifica.

   Lo schema, l'host e i valori della porta nell'intestazione della richiesta `Origin` devono corrispondere a `AllowedOrigins` in `CORSRule`. Se ad esempio imposti `CORSRule` per consentire l'origine `http://www.example.com`, nessuna delle due origini `https://www.example.com` e `http://www.example.com:80` nella richiesta corrisponde all'origine consentita nella configurazione.

c. Verifica che il metodo nella richiesta (o il metodo specificato in `Access-Control-Request-Method` in caso di una richiesta preliminare) corrisponda a uno degli elementi `AllowedMethods` nella stessa `CORSRule`.

d. Per una richiesta preliminare, se la richiesta include un'intestazione `Access-Control-Request-Headers`, verificare che la `CORSRule` includa le voci `AllowedHeaders` per ogni valore nell'intestazione `Access-Control-Request-Headers`.

Policy CORS di esempio

I seguenti esempi mostrano le policy CORS (Cross-Origin Resource Sharing).

Argomenti

- Policy CORS di esempio: Accesso in lettura per qualsiasi dominio
- Policy CORS di esempio: Accesso in lettura per un dominio specifico

Policy CORS di esempio: Accesso in lettura per qualsiasi dominio

La policy seguente consente a una pagina Web da qualsiasi dominio di recuperare contenuti dal AWS ElementalMediaStore. La richiesta include tutte le intestazioni HTTP dal dominio di origine e il servizio risponde solo alle richieste HTTP GET e HTTP HEAD dal dominio di origine. I risultati vengono memorizzati nella cache per 3.000 secondi prima della consegna di un nuovo set di risultati.

```
[
  {
    "AllowedHeaders": [
      "*"
```

```
    ],
    "AllowedMethods": [
      "GET",
      "HEAD"
    ],
    "AllowedOrigins": [
      "*"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

Policy CORS di esempio: Accesso in lettura per un dominio specifico

La policy seguente consente a una pagina Web dahttps://www.example.comper recuperare contenuti dal tuo AWS ElementalMediaStore. La richiesta include tutte le intestazioni HTTP da https://www.example.come il servizio risponde solo alle richieste HTTP GET e HTTP HEAD da https://www.example.com. I risultati vengono memorizzati nella cache per 3.000 secondi prima della consegna di un nuovo set di risultati.

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://www.example.com"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

Policy del ciclo di vita degli oggetti in AWS ElementalMediaStore

Per ogni container, puoi creare una policy del ciclo di vita degli oggetti che gestisce la durata di archiviazione degli oggetti nel container. Quando gli oggetti raggiungono l'età massima specificata,

AWS ElementalMediaStoreelimina gli oggetti. Puoi eliminare gli oggetti quando non sono più necessari per risparmiare sui costi di storage.

Puoi inoltre specificare che MediaStore deve spostare gli oggetti nella classe di archiviazione con accesso non frequente (IA) dopo aver raggiunto una certa età. Gli oggetti archiviati nella classe di archiviazione IA hanno velocità diverse per l'archiviazione e il recupero rispetto agli oggetti archiviati nella classe di archiviazione standard. Per ulteriori informazioni, consultare Prezzi di MediaStore.

Una policy del ciclo di vita degli oggetti contiene le regole che definiscono la durata di oggetti per sottocartella. Non puoi assegnare una policy del ciclo di vita degli oggetti a singoli oggetti. Puoi collegare una sola policy del ciclo di vita degli oggetti a un container, ma puoi aggiungere fino a 10 regole a ogni policy del ciclo di vita degli oggetti. Per ulteriori informazioni, consultare . Componenti di una policy del ciclo di vita degli oggetti .

Argomenti

Componenti di una policy del ciclo di vita degli oggetti

Le policy del ciclo di vita degli oggetti regolano la durata di permanenza degli oggetti in un AWS ElementalMediaStorecontainer. Ogni policy del ciclo di vita degli oggetti è costituita da una o più regole, che determinano la durata degli oggetti. Una regola può essere associata a una cartella, più cartelle o l'intero container.

Puoi collegare una policy del ciclo di vita degli oggetti a un container e ogni policy del ciclo di vita degli oggetti può contenere fino a 10 regole. Non puoi assegnare una policy del ciclo di vita degli oggetti a un singolo oggetto.

Regole in una policy del ciclo di vita degli oggetti

È possibile creare tre tipi di regole:

- Dati transitori
- Eliminazione dell'oggetto
- Transizione del ciclo di vita

Dati transitori

Una regola di dati transitoria imposta la scadenza degli oggetti entro pochi secondi. Questo tipo di regola si applica solo agli oggetti aggiunti al container dopo che la policy diventa efficace. Sono necessari fino a 20 minuti affinché MediaStore applichi la nuova policy al container.

Un esempio di regola per i dati transitori è simile alla seguente:

```
        {
            "definition": {
                "path": [ {"wildcard": "Football/index*.m3u8"} ],
                "seconds_since_create": [
                    {"numeric": [">", 120]}
                ]
            },
            "action": "EXPIRE"
        },
```

Le regole dei dati transitori hanno tre parti:

- `path`: sempre impostato su `wildcard`. Utilizza questa parte per definire gli oggetti da eliminare. Puoi utilizzare uno o più caratteri jolly, rappresentati da un asterisco (*). Ogni carattere jolly rappresenta qualsiasi combinazione di zero o più caratteri. Ad esempio, `"path": [ {"wildcard": "Football/index*.m3u8"} ],` si applica a tutti i file nella cartella `Football` che corrispondono al modello di `index*.m3u8` (ad esempio index.m3u8, index1.m3us8 e index123456.m3u8). Puoi includere fino a 10 percorsi in un'unica regola.
- `seconds_since_create`: sempre impostato su `numeric`. Puoi specificare un valore compreso tra 1 e 300 secondi Puoi anche impostare l'operatore su maggiore di (**>**) oppure maggiore o uguale a (**>=**).
- `action`: sempre impostato su `EXPIRE`.

Per le regole di dati transitori (gli oggetti scadono in pochi secondi), non vi è alcun ritardo tra la scadenza di un oggetto e l'eliminazione dell'oggetto.

> **Note**
>
> Gli oggetti soggetti a una regola di dati transitori non sono inclusi nella risposta di `list-items`. Inoltre, gli oggetti che scadono a causa di una regola di dati transitori non emettono unCloudWatchevento quando scadono.

Eliminazione dell'oggetto

Una regola di eliminazione dell'oggetto imposta la scadenza degli oggetti entro pochi giorni. Questo tipo di regola si applica a tutti gli oggetti nel container, anche se sono stati aggiunti al container prima della creazione della policy. L'applicazione della nuova policy da parte di MediaStore richiede fino a 20 minuti, ma possono essere necessarie fino a 24 ore prima che gli oggetti vengano cancellati dal container.

Un esempio di due regole per l'eliminazione di oggetti è simile al seguente:

```
        {
            "definition": {
                "path": [ { "prefix": "FolderName/" }  ],
                "days_since_create": [
                    {"numeric": [">" , 5]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [ { "wildcard": "Football/*.ts" }  ],
                "days_since_create": [
                    {"numeric": [">" , 5]}
                ]
            },
            "action": "EXPIRE"
        }
```

Le regole dell'oggetto di eliminazione hanno tre parti:

- `path`: impostare su `prefix` o su `wildcard`. Non puoi mescolare `prefix` e `wildcard` nella stessa regola. Se desideri utilizzare entrambi, è necessario creare una regola per `prefix` e una regola separata per `wildcard`, come mostrato nell'esempio precedente.

  - `prefix` – Puoi impostare il percorso su `prefix` se desideri eliminare tutti gli oggetti all'interno di una determinata cartella. Se il parametro è vuoto (`"path": [ { "prefix": "" } ],`), la destinazione è tutti gli oggetti archiviati ovunque all'interno del container corrente. Puoi includere fino a 10 percorsi `prefix` in un'unica regola.
  - `wildcard` – Per eliminare oggetti specifici in base al nome del file e/o al tipo di file imposti il percorso su `wildcard`. Puoi utilizzare uno o più caratteri jolly, rappresentati da un asterisco (*). Ogni carattere jolly rappresenta qualsiasi combinazione di zero o più caratteri. Ad esempio, `"path": [ {"wildcard": "Football/*.ts"} ],` si applica a tutti i file della cartella `Football` che corrispondono al modello di `*.ts` (ad esempio filename.ts, filename1.ts e filename123456.ts). Puoi includere fino a 10 percorsi `wildcard` in un'unica regola.
- `days_since_create`: sempre impostato su `numeric`. Puoi specificare un valore compreso tra 1 e 36.500 giorni. Puoi anche impostare l'operatore su maggiore di (**>**) oppure maggiore o uguale a (**>=**).
- `action`: sempre impostato su `EXPIRE`.

Per le regole di eliminazione degli oggetti (gli oggetti scadono entro pochi giorni), potrebbe esserci un leggero ritardo tra la scadenza di un oggetto e l'eliminazione dell'oggetto. Tuttavia, le modifiche nella fatturazione avvengono non appena l'oggetto scade. Ad esempio, se una regola del ciclo di vita specifica 10 `days_since_create`, l'account non viene fatturato per l'oggetto dopo 10 giorni, anche se l'oggetto non è ancora stato eliminato.

Transizione del ciclo di vita

Una regola di transizione del ciclo di vita imposta gli oggetti da spostare nella classe di archiviazione con accesso non frequente (IA) dopo aver raggiunto una certa età, misurata in giorni. Gli oggetti archiviati nella classe di archiviazione IA hanno velocità diverse per l'archiviazione e il recupero rispetto agli oggetti archiviati nella classe di archiviazione standard. Per ulteriori informazioni, consultare Prezzi di MediaStore.

Una volta che un oggetto si è spostato nella classe di storage IA, non è possibile spostarlo nella classe di storage standard.

La regola di transizione del ciclo di vita si applica a tutti gli oggetti nel container, anche se sono stati aggiunti al container prima della creazione della policy. L'applicazione della nuova policy da parte di MediaStore richiede fino a 20 minuti, ma possono essere necessarie fino a 24 ore prima che gli oggetti vengano cancellati dal container.

Un esempio di una regola di transizione del ciclo di vita è simile a questo:

```
        {
            "definition": {
                "path": [
                    {"prefix": "AwardsShow/"}
                ],
                "days_since_create": [
                    {"numeric": [">=" , 30]}
                ]
            },
            "action": "ARCHIVE"
        }
```

Le regole di transizione del ciclo di vita hanno tre parti:

- `path`: impostare su `prefix` o su `wildcard`. Non puoi mescolare `prefix` e `wildcard` nella stessa regola. Se desideri utilizzare entrambi, devi creare una regola per `prefix` e una regola separata per `wildcard`.
  - `prefix` - Imposti il percorso su `prefix` se desideri passare tutti gli oggetti all'interno di una particolare cartella alla classe di archiviazione IA. Se il parametro è vuoto (`"path": [ { "prefix": "" } ],`), la destinazione è tutti gli oggetti archiviati ovunque all'interno del container corrente. Puoi includere fino a 10 percorsi `prefix` in un'unica regola.
  - `wildcard` - Imposti il percorso su `wildcard` se desideri passare oggetti specifici alla classe di archiviazione IA in base al nome del file e/o al tipo di file. Puoi utilizzare uno o più caratteri jolly, rappresentati da un asterisco (*). Ogni carattere jolly rappresenta qualsiasi combinazione di zero o più caratteri. Ad esempio, `"path": [ {"wildcard": "Football/*.ts"} ],` si applica a tutti i file della cartella `Football` che corrispondono al modello di `*.ts` (ad esempio filename.ts, filename1.ts e filename123456.ts). Puoi includere fino a 10 percorsi `wildcard` in un'unica regola.
- `days_since_create`: sempre impostato su `"numeric": [">=" , 30]`.
- `action`: sempre impostato su `ARCHIVE`.

Esempio

Ad esempio, un container denominato `LiveEvents` dispone di quattro sottocartelle: `Football`, `Baseball`, `Basketball` e `AwardsShow`. L'aspetto della policy del ciclo di vita degli oggetti assegnata alla cartella `LiveEvents` è simile al seguente:

```
{
    "rules": [
         {
            "definition": {
                "path": [
                    {"prefix": "Football/"},
                    {"prefix": "Baseball/"}
                ],
                "days_since_create": [
                    {"numeric": [">" , 28]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [ { "prefix": "AwardsShow/" }  ],
                "days_since_create": [
                    {"numeric": [">=" , 15]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [ { "prefix": "" }  ],
                "days_since_create": [
                    {"numeric": [">" , 40]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [ { "wildcard": "Football/*.ts" }  ],
                "days_since_create": [
                    {"numeric": [">" , 20]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
```

```
                "path": [
                    {"wildcard": "Football/index*.m3u8"}
                ],
                "seconds_since_create": [
                    {"numeric": [">" , 15]}
                ]
            },
            "action": "EXPIRE"
        },
        {
                "definition": {
                    "path": [
                        {"prefix": "Program/"}
                    ],
                    "days_since_create": [
                        {"numeric": [">=" , 30]}
                    ]
                },
                "action": "ARCHIVE"
            }
    ]
}
```

La policy precedente specifica quanto segue:

- La prima regola indica AWS ElementalMediaStoreper eliminare gli oggetti memorizzati nella`LiveEvents/Football`folder e la cartella`LiveEvents/Baseball`cartella dopo che hanno più di 28 giorni.
- La seconda regola impone al servizio di eliminare gli oggetti archiviati nella cartella `LiveEvents/AwardsShow` quando sono più vecchi di 15 giorni.
- La terza regola impone al servizio di eliminare gli oggetti archiviati in qualsiasi parte del container `LiveEvents` quando sono più vecchi di 40 giorni. Questa regola si applica a oggetti archiviati direttamente nel container `LiveEvents`, nonché a oggetti archiviati in una qualsiasi delle quattro sottocartelle del container.
- La quarta regola indica al servizio di eliminare gli oggetti nella cartella `Football` che corrispondono al modello `*.ts` quando sono più vecchi di 20 giorni.
- La quinta regola indica al servizio di eliminare gli oggetti nel`Football`cartella corrispondente al modello`index*.m3u8`dopo che hanno più di 15 secondi. MediaStoreelimina questi file 16 secondi dopo che sono stati inseriti nel contenitore.

- La sesta regola indica al servizio di spostare gli oggetti nella cartella `Program` nella classe di archiviazione IA dopo 30 giorni.

Per altri esempi di policy relative al ciclo di vita degli oggetti, consulta Esempio di policy del ciclo di vita degli oggetti.

Aggiunta di una policy del ciclo di vita degli oggetti a un container

Una policy del ciclo di vita degli oggetti consente di specificare la durata di archiviazione degli oggetti in un container. Hai impostato una data di scadenza e dopo la data di scadenza di AWS ElementalMediaStoreelimina gli oggetti. Sono necessari fino a 20 minuti affinché il servizio applichi la nuova policy al container.

Per informazioni su come creare una policy del ciclo di vita, consulta Componenti di una policy del ciclo di vita degli oggetti.

> **Note**
>
> Per le regole di eliminazione degli oggetti (gli oggetti scadono entro pochi giorni), potrebbe esserci un leggero ritardo tra la scadenza di un oggetto e l'eliminazione dell'oggetto. Tuttavia, le modifiche nella fatturazione avvengono non appena l'oggetto scade. Ad esempio, se una regola del ciclo di vita specifica 10 `days_since_create`, l'account non viene fatturato per l'oggetto dopo 10 giorni, anche se l'oggetto non è ancora stato eliminato.

Per aggiungere una policy del ciclo di vita degli oggetti (console)

1. Apertura dellaMediaStoreConsole alhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container per il quale vuoi creare una policy del ciclo di vita degli oggetti.

   Viene visualizzata la pagina dei dettagli del container.
3. Nella sezione Object lifecycle policy (Policy del ciclo di vita degli oggetti), scegliere Create object lifecycle policy (Crea policy del ciclo di vita degli oggetti).
4. Inserisci la policy in formato JSON e quindi scegli Save (Salva).

Per aggiungere una policy del ciclo di vita degli oggetti (AWS CLI)

1. Crea un file che definisce la policy del ciclo di vita degli oggetti:

```
{
    "rules": [
         {
            "definition": {
                "path": [
                    {"prefix": "Football/"},
                    {"prefix": "Baseball/"}
                ],
                "days_since_create": [
                    {"numeric": [">" , 28]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [
                    {"wildcard": "AwardsShow/index*.m3u8"}
                ],
                "seconds_since_create": [
                    {"numeric": [">" , 8]}
                ]
            },
            "action": "EXPIRE"
        }
    ]
}
```

2. In AWS CLI, usa il comando `put-lifecycle-policy`.

```
aws mediastore put-lifecycle-policy --container-name LiveEvents --lifecycle-
policy file://LiveEventsLifecyclePolicy.json --region us-west-2
```

Il comando non ha un valore restituito. Il servizio collega la policy specificata al container.

Visualizzazione di una policy del ciclo di vita degli oggetti

Una policy del ciclo di vita degli oggetti specifica per quanto tempo gli oggetti devono essere conservati in un container.

Per visualizzare una policy del ciclo di vita di un oggetto (console)

1. Apertura dellaMediaStoreConsole alhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container di cui vuoi visualizzare la policy del ciclo di vita degli oggetti.

   Viene visualizzata la pagina dei dettagli del container, con la policy del ciclo di vita degli oggetti nella sezione Object lifecycle policy (Policy del ciclo di vita degli oggetti).

Per visualizzare una policy del ciclo di vita degli oggetti (AWS CLI)

- In AWS CLI, usa il comando `get-lifecycle-policy`.

  ```
  aws mediastore get-lifecycle-policy --container-name LiveEvents --region us-west-2
  ```

  L'esempio seguente mostra il valore restituito:

  ```
  {
      "LifecyclePolicy": "{
          "rules": [
              {
                  "definition": {
                      "path": [
                          {"prefix": "Football/"},
                          {"prefix": "Baseball/"}
                      ],
                      "days_since_create": [
                          {"numeric": [">" , 28]}
                      ]
                  },
               "action": "EXPIRE"
              }
          ]
      }"
  }
  ```

Modifica di una policy del ciclo di vita degli oggetti

Non puoi modificare una policy del ciclo di vita degli oggetti esistente. Tuttavia, puoi modificare una policy esistente caricando una policy di sostituzione. Sono necessari fino a 20 minuti affinché il servizio applichi la policy aggiornata al container.

Per modificare una policy del ciclo di vita degli oggetti (console)

1. Apertura dellaMediaStoreConsole alhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container di cui vuoi modificare la policy del ciclo di vita degli oggetti.

   Viene visualizzata la pagina dei dettagli del container.
3. Nella sezione Object lifecycle policy (Policy del ciclo di vita degli oggetti), scegliere Edit object lifecycle policy (Modifica policy del ciclo di vita degli oggetti).
4. Effettua le modifiche alla policy, quindi scegli Save (Salva).

Per modificare una policy del ciclo di vita degli oggetti (AWS CLI)

1. Crea un file che definisce la policy del ciclo di vita degli oggetti aggiornata:

```
{
    "rules": [
         {
            "definition": {
                "path": [
                    {"prefix": "Football/"},
                    {"prefix": "Baseball/"}
                    {"prefix": "Basketball/"}
                ],
                "days_since_create": [
                    {"numeric": [">" , 28]}
                ]
            },
            "action": "EXPIRE"
        }
    ]
}
```

2. In AWS CLI, usa il comando `put-lifecycle-policy`.

```
aws mediastore put-lifecycle-policy --container-name LiveEvents --lifecycle-
policy file://LiveEvents2LifecyclePolicy --region us-west-2
```

Il comando non ha un valore restituito. Il servizio collega la policy specificata al container, sostituendo la policy precedente.

Eliminazione di una policy del ciclo di vita degli oggetti

Quando elimini una policy del ciclo di vita dell'oggetto, sono necessari fino a 20 minuti affinché il servizio applichi la modifica al container.

Per eliminare una policy del ciclo di vita degli oggetti (console)

1. Apertura dellaMediaStoreConsole alhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container di cui vuoi eliminare la policy del ciclo di vita degli oggetti.

   Viene visualizzata la pagina dei dettagli del container.
3. Nella sezione Object lifecycle policy (Policy del ciclo di vita degli oggetti), scegliere Delete lifecycle policy (Elimina policy del ciclo di vita degli oggetti).
4. Scegli Continue (Continua) per confermare, quindi scegli Save (Salva).

Per eliminare una policy del ciclo di vita degli oggetti (AWS CLI)

- In AWS CLI, usa il comando `delete-lifecycle-policy`.

```
aws mediastore delete-lifecycle-policy --container-name LiveEvents --region us-
west-2
```

Il comando non ha un valore restituito.

Esempio di policy del ciclo di vita degli oggetti

Negli esempi seguenti vengono illustrate le policy relative al ciclo di vita degli oggetti.

Argomenti

- Policy di esempio relative al ciclo di vita degli oggetti: Scadenza in pochi secondi
- Policy di esempio relative al ciclo di vita degli oggetti: Scadenza entro alcuni giorni
- Policy di esempio relative al ciclo di vita degli oggetti: Passaggio alla classe di archiviazione con accesso non frequente
- Policy di esempio relative al ciclo di vita degli oggetti: Regole multiple
- Policy di esempio relative al ciclo di vita degli oggetti: Container vuoto

Policy di esempio relative al ciclo di vita degli oggetti: Scadenza in pochi secondi

La policy seguente consente a MediaStore di eliminare gli oggetti che corrispondono a tutti i seguenti criteri:

- L'oggetto è stato aggiunto al container dopo che la policy era divenuta efficace.
- L'oggetto è memorizzato nella cartella `Football`.
- L'oggetto ha un'estensione del file di `m3u8`.
- L'oggetto è stato nel container per più di 20 secondi.

```
{
    "rules": [
        {
            "definition": {
                "path": [
                    {"wildcard": "Football/*.m3u8"}
                ],
                "seconds_since_create": [
                    {"numeric": [ ">", 20 ]}
                ]
            },
            "action": "EXPIRE"
        }
    ]
}
```

Policy di esempio relative al ciclo di vita degli oggetti: Scadenza entro alcuni giorni

La policy seguente consente a MediaStore di eliminare gli oggetti che corrispondono a tutti i seguenti criteri:

- L'oggetto è memorizzato nella `Program` cartella
- L'oggetto ha un'estensione del file di `ts`
- L'oggetto è rimasto nel container per più di 5 giorni

```
{
    "rules": [
        {
            "definition": {
                "path": [
                    {"wildcard": "Program/*.ts"}
                ],
                "days_since_create": [
                    {"numeric": [ ">", 5 ]}
                ]
            },
            "action": "EXPIRE"
        }
    ]
}
```

Policy di esempio relative al ciclo di vita degli oggetti: Passaggio alla classe di archiviazione con accesso non frequente

La policy seguente specifica cheMediaStoreSposta gli oggetti nella classe di archiviazione con accesso non frequente (IA) quando hanno 30 giorni di età precedente. Gli oggetti archiviati nella classe di archiviazione IA hanno velocità diverse per l'archiviazione e il recupero rispetto agli oggetti archiviati nella classe di archiviazione standard.

Il campo `days_since_create` deve essere impostato su `"numeric": [">=" ,30]`.

```
{
    "rules": [
        {
            "definition": {
                "path": [
                    {"prefix": "Football/"},
                    {"prefix": "Baseball/"}
                ],
                "days_since_create": [
                    {"numeric": [">=" , 30]}
```

```
                ]
            },
            "action": "ARCHIVE"
        }
    ]
}
```

Policy di esempio relative al ciclo di vita degli oggetti: Regole multiple

La seguente policy specifica che MediaStore deve effettuare le seguenti operazioni:

- Spostare gli oggetti memorizzati nella cartella `AwardsShow` nella classe di archiviazione con accesso non frequente (IA) dopo 30 giorni
- Eliminare gli oggetti che hanno un'estensione del file di `m3u8` e che sono memorizzati nella cartella `Football` dopo 20 secondi
- Eliminare gli oggetti memorizzati nella cartella `April` dopo 10 giorni
- Eliminare gli oggetti che hanno un'estensione di file `ts` e che sono memorizzati nella cartella `Program` dopo 5 giorni

```
{
    "rules": [
        {
            "definition": {
                "path": [
                    {"prefix": "AwardsShow/"}
                ],
                "days_since_create": [
                    {"numeric": [ ">=" , 30 ]}
                ]
            },
            "action": "ARCHIVE"
        },
        {
            "definition": {
                "path": [
                    {"wildcard": "Football/*.m3u8"}
                ],
                "seconds_since_create": [
                    {"numeric": [ ">", 20 ]}
                ]
```

```
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [
                    {"prefix": "April"}
                ],
                "days_since_create": [
                    {"numeric": [ ">", 10 ]}
                ]
            },
            "action": "EXPIRE"
        },
        {
            "definition": {
                "path": [
                    {"wildcard": "Program/*.ts"}
                ],
                "days_since_create": [
                    {"numeric": [ ">", 5 ]}
                ]
            },
            "action": "EXPIRE"
        }
    ]
}
```

Policy di esempio relative al ciclo di vita degli oggetti: Container vuoto

La seguente policy del ciclo di vita degli oggetti specifica che MediaStore deve eliminare tutti gli oggetti nel container, incluse cartelle e sottocartelle, 1 giorno dopo l'aggiunta al container. Se il container contiene oggetti prima dell'applicazione di questa policy,MediaStoreelimina gli oggetti 1 giorno dopo l'entrata in vigore della policy. Sono necessari fino a 20 minuti affinché il servizio applichi la nuova policy al container.

```
{
    "rules": [
        {
            "definition": {
                "path": [
                    {"wildcard": "*"}
                ],
```

```
                "days_since_create": [
                    {"numeric": [ ">=", 1 ]}
                ]
            },
            "action": "EXPIRE"
        }
    ]
}
```

Politiche metriche in AWS Elemental MediaStore

Per ogni contenitore, puoi aggiungere una policy metrica per consentire ad AWS MediaStore Elemental di inviare metriche ad Amazon CloudWatch. Affinché la nuova policy diventi effettiva, sono necessari fino a 20 minuti. Per una descrizione di ogni MediaStore metrica, consultaMediaStore metriche.

Un policy di parametro contiene quanto segue:

- Impostazione per abilitare o disabilitare i parametri a livello di container.
- Da zero a cinque regole che abilitano i parametri a livello di oggetto. Se la policy contiene regole, ogni regola deve includere entrambi i seguenti elementi:
  - Gruppo di oggetti che definisce gli oggetti da includere nel gruppo. La definizione può essere un percorso o un nome di file, ma non può contenere più di 900 caratteri. I caratteri validi sono: a-z, A-Z, 0-9, _ (carattere di sottolineatura), = (uguale), : (due punti), . (punto), - (trattino), ~ (tilde), / (barra) e * (asterisco). I caratteri jolly (*) sono accettabili.
  - Nome di un gruppo di oggetti che consente di fare riferimento al gruppo di oggetti. Il nome non può contenere più di 30 caratteri. I caratteri validi sono: a-z, A-Z, 0-9 e _ (carattere di sottolineatura).

Se un oggetto corrisponde a più regole, CloudWatch visualizza un punto dati per ogni regola corrispondente. Ad esempio, se un oggetto corrisponde a due regole denominate`rule1` e`rule2`, CloudWatch visualizza due punti dati per queste regole. Il primo ha la dimensione `ObjectGroupName=rule1`, mentre per il secondo la dimensione è `ObjectGroupName=rule2`.

Argomenti

- Aggiunta di una policy di parametro
- Visualizzazione di una policy di parametro

Aggiunta di una policy di parametro

Una politica metrica contiene regole che stabiliscono quali metriche AWS Elemental MediaStore invia ad Amazon CloudWatch. Per esempi di policy di parametro, consulta Policy di parametro di esempio.

Per aggiungere una policy di parametro (console)

1. Apri la MediaStore console all'indirizzo https://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container a cui aggiungere la policy di parametro.

   Viene visualizzata la pagina dei dettagli del container.
3. Nella sezione Metric policy (Policy di parametro), scegli Create metric policy (Crea policy di parametro).
4. Inserisci la policy in formato JSON e quindi scegli Save (Salva).

Visualizzazione di una policy di parametro

Puoi utilizzare la console o AWS CLI per visualizzare la policy di parametro di un container.

Per visualizzare una policy di parametro (console)

1. Apri la MediaStore console all'indirizzo https://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere il nome del container.

   Viene visualizzata la pagina dei dettagli del container. La policy viene visualizzata nella sezione Metric policy (Policy di parametro).

Modifica di una policy di parametro

Una politica metrica contiene regole che stabiliscono quali metriche AWS Elemental MediaStore invia ad Amazon CloudWatch. Quando si modifica una policy di parametro esistente, occorrono fino a 20 minuti prima che la nuova policy abbia effetto. Per esempi di policy di parametro, consulta Policy di parametro di esempio.

Per modificare una policy di parametro (console)

1. Apri la MediaStore console all'indirizzo https://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere il nome del container.
3. Nella sezione Metric policy (Policy di parametro), scegli Edit metric policy (Modifica policy di parametro).
4. Apportare le opportune modifiche e selezionare Save (Salva).

Policy di parametro di esempio

Gli esempi seguenti mostrano policy di parametro destinate a diversi casi d'uso.

Argomenti

- Policy di parametro di esempio: parametri a livello di container
- Policy di parametro di esempio: parametri a livello di percorso
- Policy di parametro di esempio: parametri a livello di container e percorso
- Policy di parametro di esempio: parametri a livello di percorso utilizzando caratteri jolly
- Policy di parametro di esempio: parametri a livello di percorso con regole sovrapposte

Policy di parametro di esempio: parametri a livello di container

Questa politica di esempio indica che AWS Elemental MediaStore deve inviare metriche ad Amazon CloudWatch a livello di container. Ad esempio, include il parametro `RequestCount` che conta il numero di richieste `Put` effettuate al container. In alternativa, puoi impostare su `DISABLED`.

Poiché non ci sono regole in questa politica, MediaStore non invia metriche a livello di percorso. Ad esempio, non puoi visualizzare quante richieste `Put` sono state effettuate a una determinata cartella all'interno di questo container.

```
{
   "ContainerLevelMetrics": "ENABLED"
}
```

Policy di parametro di esempio: parametri a livello di percorso

Questa politica di esempio indica che AWS Elemental non MediaStore deve inviare metriche ad Amazon CloudWatch a livello di container. Inoltre, MediaStore non deve inviare parametri per gli

oggetti in due cartelle specifiche: `baseball/saturday` e `football/saturday`. I parametri per le richieste di MediaStore sono i seguenti:

- Le richieste alla`baseball/saturday` cartella hanno una CloudWatch dimensione di`ObjectGroupName=baseballGroup`.
- Le richieste alla cartella `football/saturday` hanno una dimensione `ObjectGroupName=footballGroup`.

```
{
   "ContainerLevelMetrics": "DISABLED",
   "MetricPolicyRules": [
     {
       "ObjectGroup": "baseball/saturday",
       "ObjectGroupName": "baseballGroup"
     },
     {
       "ObjectGroup": "football/saturday",
       "ObjectGroupName": "footballGroup"
     }
   ]
}
```

Policy di parametro di esempio: parametri a livello di container e percorso

Questa politica di esempio indica che AWS Elemental MediaStore deve inviare metriche ad Amazon CloudWatch a livello di container. Inoltre, MediaStore dovrebbe inviare le metriche per gli oggetti in due cartelle specifiche:`baseball/saturday` e`football/saturday`. I parametri per le richieste di MediaStore sono i seguenti:

- Le richieste alla`baseball/saturday` cartella hanno una CloudWatch dimensione di`ObjectGroupName=baseballGroup`.
- Le richieste alla`football/saturday` cartella hanno una CloudWatch dimensione`ObjectGroupName=footballGroup`.

```
{
   "ContainerLevelMetrics": "ENABLED",
   "MetricPolicyRules": [
     {
```

```
        "ObjectGroup": "baseball/saturday",
        "ObjectGroupName": "baseballGroup"
      },
      {
        "ObjectGroup": "football/saturday",
        "ObjectGroupName": "footballGroup"
      }
    ]
}
```

Policy di parametro di esempio: parametri a livello di percorso utilizzando caratteri jolly

Questa politica di esempio indica che AWS Elemental MediaStore deve inviare metriche ad Amazon CloudWatch a livello di container. Inoltre, MediaStore dovrebbe inviare anche metriche per gli oggetti in base al nome del file. Un carattere jolly indica che gli oggetti possono essere archiviati in qualsiasi punto del container e avere qualsiasi nome del file purché terminino con un'estensione `.m3u8`.

```
{
   "ContainerLevelMetrics": "ENABLED",
   "MetricPolicyRules": [
     {
       "ObjectGroup": "*.m3u8",
       "ObjectGroupName": "index"
     }
   ]
 }
```

Policy di parametro di esempio: parametri a livello di percorso con regole sovrapposte

Questa politica di esempio indica che AWS Elemental MediaStore deve inviare metriche ad Amazon CloudWatch a livello di container. Inoltre, MediaStore dovrebbe inviare metriche per due cartelle:`sports/football/saturday` `esports/football`.

Le metriche relative MediaStore alle richieste alla`sports/football/saturday` cartella hanno una CloudWatch dimensione di`ObjectGroupName=footballGroup1`. Poiché gli oggetti archiviati nella cartella `sports/football` corrispondono a entrambe le regole, CloudWatch visualizza due punti dati per questi oggetti: uno con una dimensione `ObjectGroupName=footballGroup1` e il secondo con una dimensione `ObjectGroupName=footballGroup2`.

```
{
   "ContainerLevelMetrics": "ENABLED",
```

```
  "MetricPolicyRules": [
    {
      "ObjectGroup": "sports/football/saturday",
      "ObjectGroupName": "footballGroup1"
    },
    {
      "ObjectGroup": "sports/football",
      "ObjectGroupName": "footballGroup2"
    }
  ]
}
```

Cartelle in AWS ElementalMediaStore

Le cartelle sono divisioni all'interno di un container, utilizzate per suddividere il container proprio come si fa con le sottocartelle per dividere una cartella in un file system. È possibile creare fino a 10 livelli di cartelle (escluso il container stesso).

Le cartelle sono facoltative; è possibile scegliere di caricare gli oggetti direttamente in un container, invece che in una cartella. Tuttavia, le cartelle sono un modo semplice per organizzare gli oggetti.

Per caricare un oggetto in una cartella, devi specificare il percorso della cartella. Se la cartella esiste già, AWS ElementalMediaStorearchivia l'oggetto nella cartella. Se la cartella non esiste, il servizio la crea e quindi archivia l'oggetto nella cartella.

Supponiamo ad esempio che tu abbia un container denominato`moviese` carichi un file denominato`mlaw.ts`con il percorso`premium/canada`. AWS ElementalMediaStorearchivia l'oggetto nella sottocartella "canada" della cartella "premium". Se nessuna delle due cartelle esiste, il servizio crea sia la cartella `premium` che la sottocartella `canada`, quindi archivia l'oggetto nella sottocartella `canada`. Se specifichi solo il container `movies` (senza percorso), il servizio archivia l'oggetto direttamente nel container.

AWS ElementalMediaStoreUna volta eliminato l'ultimo oggetto in una cartella, elimina automaticamente la cartella e anche le eventuali cartelle superiori vuote. Ad esempio, supponi di avere una cartella denominata "premium" che non contiene file ma una sottocartella denominata `canada`. La sottocartella `canada` contiene un file denominato `mlaw.ts`. Se elimini il file `mlaw.ts`, il servizio elimina entrambe le cartelle `premium` e `canada`. L'eliminazione automatica si applica solo per le cartelle. Il servizio non elimina i container vuoti.

Argomenti

Regole per i nomi di cartella

Quando scegli un nome per la cartella, ricordati quanto segue:

- Il nome può contenere solo i seguenti caratteri: lettere maiuscole (A-Z), minuscole (a-z), numeri (0-9), punti (.), trattini (-), tilde (~), caratteri di sottolineatura (_), segni di uguale (=) e due punti (:).
- Il nome deve essere composto da almeno un carattere. Nomi di cartelle vuote (come ad esempio`folder1//folder3/`) non sono ammessi.
- I nomi rispettano la distinzione tra lettere maiuscole e minuscole. Ad esempio, puoi avere una cartella denominata `myFolder` e una denominata `myfolder` nello stesso container o cartella perché tali nomi sono univoci.
- Il nome deve essere univoco solo all'interno della cartella o del container padre. Ad esempio puoi creare una cartella denominata `myfolder` in due diversi container: `movies/myfolder` e `sports/myfolder`.
- Il nome può avere lo stesso nome del container padre.
- La cartella non può essere rinominata dopo che è stata creata.

Creazione di una cartella

Puoi creare le cartelle al momento di caricare gli oggetti. Per caricare un oggetto in una cartella, devi specificare il percorso della cartella. Se la cartella esiste già, AWS ElementalMediaStorearchivia l'oggetto nella cartella. Se la cartella non esiste, il servizio la crea e quindi archivia l'oggetto nella cartella.

Per ulteriori informazioni, consultare . the section called “Caricamento di un oggetto” .

Eliminazione di una cartella

Puoi eliminare le cartelle solo se sono vuote; non è possibile eliminare cartelle che contengono oggetti.

AWS ElementalMediaStoreUna volta eliminato l'ultimo oggetto in una cartella, elimina automaticamente la cartella e anche le eventuali cartelle superiori vuote. Ad esempio, supponi di avere una cartella denominata `premium` che non contiene file ma una sottocartella denominata `canada`. La sottocartella `canada` contiene un file denominato `mlaw.ts`. Se elimini il file `mlaw.ts`, il servizio elimina entrambe le cartelle `premium` e `canada`. L'eliminazione automatica si applica solo per le cartelle. Il servizio non elimina i container vuoti.

Per ulteriori informazioni, consultare Eliminazione di un oggetto.

Oggetti in AWS ElementalMediaStore

AWS ElementalMediaStorele risorse di sono chiamateoggetti. Puoi caricare un oggetto in un container o in una cartella all'interno del container.

In MediaStore, puoi caricare, scaricare ed eliminare oggetti:

- Upload (Carica): aggiungere un oggetto a un container o una cartella. Non corrisponde alla creazione di un oggetto. Devi creare gli oggetti in locale prima di poterli caricare in MediaStore.
- Download (Scarica): copiare un oggetto da MediaStore in un'altra posizione. Questa operazione non elimina l'oggetto da MediaStore.
- Delete (Elimina): rimuovere completamente un oggetto da MediaStore. È possibile eliminare gli oggetti individualmente oppure aggiungere una policy del ciclo di vita degli oggetti per eliminare automaticamente gli oggetti all'interno di un container dopo un intervallo di tempo specificato.

MediaStore accetta tutti i tipi di file.

Argomenti

Caricamento di un oggetto

Puoi caricare gli oggetti in un container o in una cartella all'interno di un container. Per caricare un oggetto in una cartella, devi specificare il percorso della cartella. Se la cartella esiste già, AWS ElementalMediaStorearchivia l'oggetto nella cartella. Se la cartella non esiste, il servizio la crea e quindi archivia l'oggetto nella cartella. Per ulteriori informazioni sulle cartelle, consulta Cartelle in AWS ElementalMediaStore.

Puoi utilizzare la console di MediaStore o AWS CLI per caricare gli oggetti.

MediaStore supporta il trasferimento a blocchi di oggetti, che consente di ridurre la latenza rendendo un oggetto disponibile per il download mentre è ancora in fase di caricamento. Per usare questa

funzionalità, imposta la disponibilità di caricamento dell'oggetto su `streaming`. Puoi impostare il valore di questa intestazione quando carichi l'oggetto utilizzando l'API. Se non specifichi questa intestazione nella richiesta, MediaStore assegna il valore predefinito di `standard` per la disponibilità di caricamento dell'oggetto.

Le dimensioni dell'oggetto non possono superare 25 MB per disponibilità di caricamento standard e a 10 MB per disponibilità di caricamento in streaming.

> **Note**
>
> I nomi di file di oggetti possono contenere solo lettere, numeri, punti (.), trattini bassi (_), tilde (~), trattini (-), segni di uguale (=) e virgole (:).

Per caricare un oggetto (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container) scegliere il nome del container. Viene visualizzato il pannello dei dettagli del container.
3. Scegli Upload object (Carica oggetto).
4. In Target path (Percorso di destinazione) digita un percorso per le cartelle. Ad esempio, `premium/canada`. Se una delle cartelle del percorso specificato non esiste ancora, il servizio la crea automaticamente.
5. Nella sezione Object (Oggetto) scegli Browse (Sfoglia).
6. Passa alla cartella appropriata e scegli un oggetto da caricare.
7. Seleziona Open (Apri), quindi Upload (Carica).

> **Note**
>
> Se un file con lo stesso nome esiste già nella cartella selezionata, il servizio sostituisce il file originale con il file caricato.

Per caricare un oggetto (AWS CLI)

- In AWS CLI, usa il comando `put-object`. È anche possibile includere i seguenti parametri: `content-type`, `cache-control` (per consentire al chiamante di controllare il comportamento della cache dell'oggetto) e `path` (per inserire l'oggetto in una cartella all'interno del container).

  > **Note**
  >
  > Dopo aver caricato l'oggetto, non è possibile modificare `content-type`, `cache-control` o `path`.

```
aws mediastore-data put-object --endpoint https://
aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --body README.md --path /
folder_name/README.md --cache-control "max-age=6, public" --content-type binary/
octet-stream --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "ContentSHA256":
 "74b5fdb517f423ed750ef214c44adfe2be36e37d861eafe9c842cbe1bf387a9d",
    "StorageClass": "TEMPORAL",
    "ETag": "af3e4731af032167a106015d1f2fe934e68b32ed1aa297a9e325f5c64979277b"
}
```

Visualizzazione di un elenco di oggetti

È possibile utilizzare AWS ElementalMediaStoreConsole per visualizzare gli elementi (oggetti e cartelle) memorizzati nel livello principale di un container o in una cartella. Gli elementi archiviati in una sottocartella del container o della cartella corrente non verranno visualizzati. Puoi utilizzare AWS CLI per visualizzare un elenco di oggetti e cartelle all'interno di un container, indipendentemente dal numero di cartelle o sottocartelle presenti all'interno del container.

Per visualizzare un elenco di oggetti in un determinato container (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.

2. Nella pagina Containers (Container), scegli il nome del container che contiene la cartella che desideri visualizzare.
3. Scegli il nome della cartella dall'elenco.

   Viene visualizzata una pagina di dettagli che mostra tutte le cartelle e gli oggetti memorizzati nella cartella.

Per visualizzare un elenco di oggetti in una determinata cartella (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container che contiene la cartella che desideri visualizzare.

   Viene visualizzata una pagina di dettagli che mostra tutte le cartelle e gli oggetti memorizzati nel container.

Per visualizzare un elenco di oggetti e cartelle in un determinato container (AWS CLI)

- In AWS CLI, usa il comando `list-items`.

```
aws mediastore-data list-items --endpoint https://
aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "Items": [
        {
            "ContentType": "image/jpeg",
            "LastModified": 1563571859.379,
            "Name": "filename.jpg",
            "Type": "OBJECT",
            "ETag":
 "543ab21abcd1a234ab123456a1a2b12345ab12abc12a1234abc1a2bc12345a12",
            "ContentLength": 3784
        },
        {
            "Type": "FOLDER",
            "Name": "ExampleLiveDemo"
```

```
        }
    ]
}
```

> **Note**
>
> Gli oggetti soggetti a una regola `seconds_since_create` non sono inclusi nella risposta di `list-items`.

Per visualizzare un elenco di oggetti e cartelle in una determinata cartella (AWS CLI)

- In AWS CLI, utilizza il comando `list-items` con il nome della cartella specificato alla fine della richiesta.

```
aws mediastore-data list-items --endpoint https://
aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --path /folder_name --
region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "Items": [
        {
            "Type": "FOLDER",
            "Name": "folder_1"
        },
        {
            "LastModified": 1563571940.861,
            "ContentLength": 2307346,
            "Name": "file1234.jpg",
            "ETag":
 "111a1a22222a1a1a222abc333a444444b55ab1111ab2222222222ab333333a2b",
            "ContentType": "image/jpeg",
            "Type": "OBJECT"
        }
    ]
}
```

> **Note**
>
> Gli oggetti soggetti a una regola `seconds_since_create` non sono inclusi nella risposta di `list-items`.

Visualizzazione dei dettagli di un oggetto

Dopo aver caricato un oggetto, AWS ElementalMediaStorearchivia i dettagli quali la data di modifica, la lunghezza del contenuto, l'ETag (tag di entità) e il tipo di contenuto. Per informazioni sull'utilizzo dei metadati di un oggetto, consulta Interazione di MediaStore con le cache HTTP.

Per visualizzare i dettagli di un oggetto (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container che contiene l'oggetto che desideri visualizzare.
3. Se l'oggetto che desideri visualizzare si trova in una cartella, continua a selezionare i nomi di cartella fino a visualizzare l'oggetto.
4. Scegli il nome dell'oggetto.

   Viene visualizzata una pagina di dettagli che mostra le informazioni sull'oggetto.

Per visualizzare i dettagli di un oggetto (AWS CLI)

- In AWS CLI, usa il comando `describe-object`.

```
aws mediastore-data describe-object --endpoint https://
aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --path /folder_name/
file1234.jpg --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "ContentType": "image/jpeg",
    "LastModified": "Fri, 19 Jul 2019 21:32:20 GMT",
    "ContentLength": "2307346",
```

```
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3"
}
```

Download di un oggetto

È possibile utilizzare la console per scaricare un oggetto. Puoi utilizzare AWS CLI per scaricare un oggetto intero o solo una parte.

Per scaricare un oggetto (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container che contiene l'oggetto da scaricare.
3. Se l'oggetto che desideri scaricare si trova in una cartella, continua a selezionare i nomi di cartella fino a visualizzare l'oggetto.
4. Scegli il nome dell'oggetto.
5. Nella pagina dei dettagli Object (Oggetto), scegli Download (Scarica).

Per scaricare un oggetto (AWS CLI)

- In AWS CLI, usa il comando `get-object`.

```
aws mediastore-data get-object --endpoint https://
aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --path=/folder_name/
README.md README.md --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "ContentLength": "2307346",
    "ContentType": "image/jpeg",
    "LastModified": "Fri, 19 Jul 2019 21:32:20 GMT",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
    "StatusCode": 200
}
```

Per scaricare parte di un oggetto (AWS CLI)

- In AWS CLI, utilizza il comando `get-object` e specifica un intervallo.

```
aws mediastore-data get-object --endpoint https://
aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --path /folder_name/
README.md --range="bytes=0-100" README2.md --region us-west-2
```

L'esempio seguente mostra il valore restituito:

```
{
    "StatusCode": 206,
    "ContentRange": "bytes 0-100/2307346",
    "ContentLength": "101",
    "LastModified": "Fri, 19 Jul 2019 21:32:20 GMT",
    "ContentType": "image/jpeg",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3"
}
```

Eliminazione di oggetti

AWS ElementalMediaStoreoffre diverse opzioni per eliminare oggetti dai container:

- Elimina un singolo oggetto. Non soggetto a costi.
- Svuota un container per eliminare tutti gli oggetti all'interno del container contemporaneamente. Poiché questo processo utilizza chiamate API, si applicano le normali tariffe API.
- Aggiungi una policy del ciclo di vita degli oggetti per eliminare gli oggetti dopo un determinato periodo. Non soggetto a costi.

Eliminazione di un oggetto

Puoi eliminare gli oggetti utilizzando la console o AWS CLI. In alternativa, puoi aggiungere una policy del ciclo di vita degli oggetti per eliminare automaticamente gli oggetti dopo un determinato periodo in un container oppure svuotare un container per eliminare tutti gli oggetti all'interno del container.

> **Note**
>
> Quando elimini l'unico oggetto in una cartella, AWS ElementalMediaStoreelimina automaticamente la cartella e tutte cartelle vuote ai livelli superiori della cartella. Ad esempio, supponi di avere una cartella denominata `premium` che non contiene file ma una sottocartella denominata `canada`. La sottocartella `canada` contiene un file denominato `mlaw.ts`. Se elimini il file `mlaw.ts`, il servizio elimina entrambe le cartelle `premium` e `canada`.

Per eliminare un oggetto (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli il nome del container che contiene l'oggetto da eliminare.
3. Se l'oggetto che desideri eliminare si trova in una cartella, continua a selezionare i nomi di cartella fino a visualizzare l'oggetto.
4. Scegli l'opzione a sinistra del nome dell'oggetto.
5. Scegliere Delete (Elimina).

Per eliminare un oggetto (AWS CLI)

- In AWS CLI, usa il comando `delete-object`.

  Esempio:

  ```
  aws mediastore-data --region us-west-2 delete-object --endpoint=https://
  aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com --path=/folder_name/
  README.md
  ```

  Il comando non ha un valore restituito.

Svuotamento di un container

Puoi svuotare un container per eliminare tutti gli oggetti archiviati all'interno del container. In alternativa, puoi aggiungere una policy del ciclo di vita degli oggetti per eliminare automaticamente gli oggetti dopo un determinato periodo in un container oppure eliminare gli oggetti singolarmente.

Per svuotare un container (console)

1. Apertura dellaMediaStoreConsole inhttps://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegli l'opzione per il container da svuotare.
3. Scegli Empty container (Svuota container). Viene visualizzato un messaggio di conferma.
4. Confermare che si desidera svuotare il container immettendo il nome del container nel campo di testo, quindi scegliereEmpty (Vuoto).

Sicurezza in AWS Elemental MediaStore

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

La sicurezza è una responsabilità condivisa tra AWSe l'utente. Il modello di responsabilità condivisa fa riferimento ad una sicurezza del cloud e nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS in Cloud AWS. AWS fornisce inoltre i servizi che è possibile utilizzare in modo sicuro. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad AWS Elemental MediaStore, consulta AWSServices in Scope by Compliance Program AWS Services in Scope Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo MediaStore. I seguenti argomenti mostrano come eseguire la configurazione MediaStore per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere MediaStore le tue risorse.

Argomenti

Protezione dei dati in AWS Elemental MediaStore

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in AWS Elemental MediaStore. Come descritto in questo modello, AWSè responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori MediaStore o Servizi AWS utilizzi la console, l'API o gli AWS SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati

MediaStore crittografa i contenitori e gli oggetti inattivi utilizzando l'algoritmo AES-256 standard del settore. Ti consigliamo di utilizzare MediaStore per proteggere i tuoi dati nei seguenti modi:

- Crea una politica del contenitore per controllare i diritti di accesso a tutte le cartelle e gli oggetti in quel contenitore. Per ulteriori informazioni, consulta the section called “Policy di container”.
- Crea una politica di condivisione delle risorse tra origini (CORS) per consentire l'accesso selettivo tra origini diverse alle tue risorse. MediaStore Con CORS, puoi consentire alle applicazioni Web client caricate in un dominio di interagire con le risorse situate in un dominio differente. Per ulteriori informazioni, consulta the section called “Policy CORS”.

Identity and Access Management per AWS Elemental MediaStore

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

Argomenti

Destinatari

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

Utente del servizio: se utilizzi il MediaStore servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più MediaStore funzionalità 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 MediaStore, consulta Risoluzione dei problemi di MediaStore identità e accesso ad AWS Elemental.

Amministratore del servizio: se sei responsabile delle MediaStore risorse della tua azienda, probabilmente hai pieno accesso a MediaStore. È tuo compito determinare a quali MediaStore funzionalità e risorse 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 MediaStore, consultaCome funziona AWS Elemental con MediaStore IAM.

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

Autenticazione con identità

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

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

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

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede a Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono a Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli 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 una identità all'interno del tuo Account AWSche dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con

utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Consolemediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLIo API AWSoppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le

credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le

policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

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

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAFe Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi

di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come funziona AWS Elemental con MediaStore IAM

Prima di utilizzare IAM per gestire l'accesso a MediaStore, scopri con MediaStore quali funzionalità IAM è disponibile l'uso.

Funzionalità IAM che puoi usare con AWS Elemental MediaStore

Funzionalità IAM	MediaStore supporto
Policy basate su identità	Sì
Policy basate su risorse	Sì

Funzionalità IAM	MediaStore supporto
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per avere una panoramica di alto livello su come MediaStore e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWSi servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per MediaStore

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 Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy

JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per MediaStore

Per visualizzare esempi di politiche basate sull' MediaStore identità, vedere. Esempi di policy basate sull'identità per AWS Elemental MediaStore

Politiche basate sulle risorse all'interno MediaStore

Supporta le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

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 l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

> **Note**
>
> MediaStore supporta anche le politiche dei contenitori che definiscono quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire azioni sul contenitore. Per ulteriori informazioni, consulta Policy di container.

Azioni politiche per MediaStore

Supporta le operazioni di policy	Sì

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

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di MediaStore azioni, consulta Azioni definite da AWS Elemental MediaStore nel Service Authorization Reference.

Le azioni politiche in MediaStore uso utilizzano il seguente prefisso prima dell'azione:

```
mediastore
```

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

```
"Action": [
      "mediastore:action1",
      "mediastore:action2"
         ]
```

Per visualizzare esempi di politiche MediaStore basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Elemental MediaStore

Risorse politiche per MediaStore

Supporta le risorse di policy	Sì

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

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

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

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

Per visualizzare un elenco dei tipi di MediaStore risorse e dei relativi ARN, consulta Risorse definite da AWS MediaStore Elemental nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Azioni definite da AWS Elemental. MediaStore

La risorsa MediaStore contenitore ha il seguente ARN:

```
arn:${Partition}:mediastore:${Region}:${Account}:container/${containerName}
```

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

Ad esempio, per specificare il container `AwardsShow` nell'istruzione, utilizza il seguente ARN:

```
"Resource": "arn:aws:mediastore:us-east-1:111122223333:container/AwardsShow"
```

Chiavi relative alle condizioni delle politiche per MediaStore

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

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

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

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

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

Per visualizzare un elenco di chiavi di MediaStore condizione, consulta Condition keys for AWS Elemental MediaStore nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da AWS Elemental MediaStore.

Per visualizzare esempi di politiche MediaStore basate sull'identità, consulta. Esempi di policy basate sull'identità per AWS Elemental MediaStore

ACL in MediaStore

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con MediaStore

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con MediaStore

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWSnon funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Consoleutilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le

credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per MediaStore

Supporta sessioni di accesso diretto (FAS)	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per MediaStore

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. MediaStore Modifica i ruoli di servizio solo quando viene MediaStore fornita una guida in tal senso.

Ruoli collegati ai servizi per MediaStore

Supporta i ruoli collegati ai servizi	No

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

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 AWS Elemental MediaStore

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse MediaStore. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

Per dettagli sulle azioni e sui tipi di risorse definiti da MediaStore, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per AWS MediaStore Elemental nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di MediaStore
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare MediaStore risorse nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

Utilizzo della console di MediaStore

Per accedere alla MediaStore console AWS Elemental, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle MediaStore risorse del 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 le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la MediaStore console, allega anche la policy MediaStore *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente 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 allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API AWS.

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

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi di MediaStore identità e accesso ad AWS Elemental

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con MediaStore un IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in MediaStore
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie MediaStore risorse

Non sono autorizzato a eseguire alcuna azione in MediaStore

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 `mediastore:`*`GetWidget`* fittizie.

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

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

Non sono autorizzato a eseguire iam: PassRole

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

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

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in MediaStore. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

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

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

Voglio consentire a persone esterne a me di accedere Account AWS alle mie MediaStore risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se MediaStore supporta queste funzionalità, consultaCome funziona AWS Elemental con MediaStore IAM.

- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Registrazione e monitoraggio in AWS Elemental MediaStore

Questa sezione fornisce una panoramica delle opzioni per il logging e il monitoraggio in AWS Elemental MediaStore per scopi di sicurezza. Per ulteriori informazioni sul logging e il monitoraggio in MediaStore consulta Monitoraggio e etichettatura in AWS Elemental MediaStore.

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di AWS Elemental MediaStore e delle soluzioni AWS. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno. AWSfornisce diversi strumenti per monitorare le MediaStore risorse e rispondere a potenziali incidenti.

CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi, osservi una singola metrica per un periodo di tempo specificato. Se la metrica supera una determinata soglia, viene inviata una notifica a un argomento di Amazon SNS o a una policy di AWS Auto Scaling. CloudWatch gli allarmi non richiamano azioni perché si trovano in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato. Per ulteriori informazioni, consulta Monitoraggio con CloudWatch.

Log di AWS CloudTrail

CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in. AWS Elemental MediaStore Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata inviata MediaStore, 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, consulta Registrazione delle chiamate API con CloudTrail.

AWS Trusted Advisor

Trusted Advisor sfrutta le best practice acquisite durante il servizio di centinaia di migliaia di clienti AWS. Trusted Advisor controlla l'ambiente AWS, quindi fornisce suggerimenti nel caso in cui vi siano opportunità di risparmio, di miglioramento delle prestazioni e della disponibilità dei sistemi o di risoluzione dei problemi di sicurezza. Tutti i clienti AWS possono accedere a cinque controlli Trusted Advisor. I clienti che hanno sottoscritto un piano di supporto Business o Enterprise possono visualizzare tutti i controlli di Trusted Advisor.

Per ulteriori informazioni, consulta AWS Trusted Advisor.

Convalida della conformità per AWS Elemental MediaStore

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

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

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWSincentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWSper creare applicazioni conformi alla normativa HIPAA.

> **Note**
>
> Non tutti i Servizi AWSsono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- AWSGuide 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 le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Configvaluta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWSe 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.
- AWS Audit Manager: questo Servizio AWSaiuta a verificare continuamente l'utilizzo di AWSper semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza in AWS Elemental MediaStore

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità di trasmissione effettiva elevata. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

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

Oltre all'infrastruttura AWS globale, MediaStore offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

Sicurezza dell'infrastruttura in AWS Elemental MediaStore

In quanto servizio gestito, AWS Elemental MediaStore è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di sicurezza AWSe su come AWSprotegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWSutilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWSWell-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere MediaStore 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.

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. In AWS, la rappresentazione cross-service può comportare il problema confused deputy. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Consigliamo di utilizzare le chiavi di contesto `aws:SourceArn`e `aws:SourceAccount`global condition nelle policy delle risorse per limitare le autorizzazioni che AWS MediaStore Elemental fornisce a un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.

Il valore di `aws:SourceArn` deve essere la configurazione per la quale vengono MediaStore pubblicati CloudWatch i log nella tua regione e nel tuo account.

L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition MediaStore per evitare il confuso problema del vice.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "servicename:ActionName",
    "Resource": [
      "arn:aws:servicename:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:servicename:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Monitoraggio e etichettatura in AWS Elemental MediaStore

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di AWS Elemental MediaStore e delle tue altreAWS soluzioni. AWSfornisce i seguenti strumenti di monitoraggio per controllare MediaStore, segnalare un problema e intervenire automaticamente quando necessario:

- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.
- Amazon CloudWatch monitora leAWS risorse e le applicazioni che esegui suAWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi impostare perché CloudWatch tenga traccia dell'uso della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.
- Amazon CloudWatch Events fornisce un flusso di eventi di sistema che descrivono le modifiche nelleAWS risorse. In genere,AWS i servizi forniscono notifiche di CloudWatch eventi a Events in pochi secondi, ma a volte può essere necessario un minuto o più. CloudWatch Events consente il calcolo automatizzato basato sugli eventi, così che tu possa scrivere le regole che osservano determinati eventi e attivano le operazioni automatizzate in altriAWS servizi quando si verificano gli eventi. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch Events.
- Amazon CloudWatch Logs consente di monitorare, archiviare e accedere ai file di log dalle istanze Amazon EC2 e da altre origini. CloudTrail CloudWatch I log possono monitorare le informazioni nei file di log e notificare quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Guida per l'utente CloudWatch di Amazon Logs.

Puoi anche assegnare metadati ai MediaStore contenitori sotto forma di tag. Ogni tag è un'etichetta che comprende una chiave e il valore definiti. I tag possono semplificare la gestione, la ricerca e il filtro delle risorse. Puoi usare i tag per organizzare le risorse AWS nella console di gestione AWS,

creare report di utilizzo e di fatturazione per tutte le risorse AWS e filtrare le risorse durante le attività di automazione dell'infrastruttura.

Argomenti

Registrazione delle chiamate MediaStore API AWS Elemental conAWS CloudTrail

AWS Elemental MediaStore è integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unAWS servizio in MediaStore. CloudTrail acquisisce un sottoinsieme di chiamate API per MediaStore come eventi, incluse le chiamate dalla MediaStore console e dalle chiamate in codice all' MediaStore API. Se si crea un percorso, è possibile abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per MediaStore. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console di in Cronologia eventi. Le informazioni raccolte da consentono CloudTrail di determinare la richiesta effettuata a MediaStore, l'indirizzo IP da cui è stata eseguita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altro.

Per ulteriori informazioni CloudTrail, incluso come configurarlo e abilitarlo, consulta la Guida per l'AWS CloudTrailutente.

Argomenti

MediaStoreInformazioni AWS Elemental in CloudTrail

CloudTrail è abilitato sull'AWSaccount al momento della sua creazione. Quando si verifica un'attività in AWS Elemental MediaStore, questa viene registrata in un CloudTrail evento insieme ad altri eventi delAWS servizio in Event history (Cronologia eventi). È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi di.

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per MediaStore, creare un trail. Un percorso consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altriAWS servizi per analizzare con maggiore dettaglio e usare i dati raccolti nei CloudTrail log. Per ulteriori informazioni, consulta i seguenti argomenti:

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

AWS Elemental MediaStore supporta la registrazione delle operazioni seguenti come eventi nei file di CloudTrail log:

- `CreateContainer`
- `DeleteContainer`
- `DeleteContainerPolicy`
- `DeleteCorsPolicy`
- `DescribeContainer`
- `GetContainerPolicy`
- `GetCorsPolicy`
- `ListContainers`
- `PutContainerPolicy`
- `PutCorsPolicy`

Ogni evento o voce del 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 con le credenziali di sicurezza temporanee per un ruolo o un utente federato.

- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Esempio: voci del file di MediaStore registro di AWS Elemental

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sul operazione richiesta, data e ora dell'operazione, parametri richiesti e così via. CloudTrail i file di log non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail log di che illustra l'`CreateContainer`operazione:

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGHIJKL123456789",
        "arn": "arn:aws:iam::111122223333:user/testUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "testUser",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-07-09T12:55:42Z"
            }
        },
        "invokedBy": "signin.amazonaws.com"
    },
    "eventTime": "2018-07-09T12:56:54Z",
    "eventSource": "mediastore.amazonaws.com",
    "eventName": "CreateContainer",
    "awsRegion": "ap-northeast-1",
    "sourceIPAddress": "54.239.119.16",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "containerName": "TestContainer"
```

```
    },
    "responseElements": {
        "container": {
            "status": "CREATING",
            "creationTime": "Jul 9, 2018 12:56:54 PM",
            "name": " TestContainer ",
            "aRN": "arn:aws:mediastore:ap-northeast-1:111122223333:container/
TestContainer"
        }
    },
    "requestID":
 "MNCTGH4HRQJ27GRMBVDPIVHEP4LO2BN6MUVHBCPSHOAWNSOKSXCO24B2UEOBBND5DONRXTMFK3TOJ4G7AHWMESI",
    "eventID": "7085b140-fb2c-409b-a329-f567912d704c",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Monitoraggio di AWS MediaStore Elemental con Amazon CloudWatch

Puoi monitorare AWS Elemental MediaStore utilizzando CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili. CloudWatch conserva le statistiche per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e ottenere una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.

AWSfornisce i seguenti strumenti di monitoraggio per controllare MediaStore, segnalare un problema e intervenire automaticamente quando necessario:

- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai file di log daAWS servizi come AWS Elemental MediaStore. È possibile utilizzare CloudWatch i log per monitorare applicazioni e sistemi utilizzando i dati di log. Ad esempio, CloudWatch Logs è in grado di monitorare il numero di errori che si verificano nei registri delle applicazioni e di inviare una notifica ogni volta che il tasso di errori supera una soglia specificata. CloudWatch Logs utilizza i dati di log per il monitoraggio, quindi non sono necessarie modifiche al codice. Ad esempio, è possibile monitorare i registri delle applicazioni per termini letterali specifici (come "ValidationException«) o contare il numero di`PutObject` richieste effettuate durante un determinato periodo di tempo. Quando il termine che cerchi viene trovato, CloudWatch Logs segnala i dati a una CloudWatch

metrica da te specificata. I dati di log vengono crittografati durante il transito e mentre sono a riposo.

- Amazon CloudWatch Events fornisce eventi di sistema che descrivono i cambiamenti nelleAWS risorse, come MediaStore gli oggetti. In genere,AWS i servizi forniscono notifiche di CloudWatch eventi a Events in pochi secondi, ma a volte può essere necessario un minuto o più. È possibile impostare regole per abbinare eventi (come una`DeleteObject` richiesta) e instradarli a una o più funzioni o flussi di destinazione. CloudWatch Gli eventi si accorgono delle modifiche operative appena si verificano. Inoltre, CloudWatch Events risponde a queste modifiche operative e prende le misure correttive necessarie inviando messaggi per rispondere all'ambiente attivando funzioni, effettuando modifiche e catturando informazioni sullo stato.

CloudWatch Registri

La registrazione degli accessi fornisce record dettagliati per le richieste che vengono effettuate a oggetti in un container. I log di accesso sono utili per molte applicazioni, ad esempio controlli di accesso e di sicurezza. Possono inoltre fornire informazioni sulla base clienti e sulla MediaStore fattura. CloudWatch I registri sono classificati come segue:

- Un flusso di log è una sequenza di log eventi che condividono la stessa origine.
- Un gruppo di log è un gruppo di flussi di log che condividono le stesse impostazioni di conservazione, monitoraggio e controllo degli accessi. Quando abiliti la registrazione degli accessi su un contenitore, MediaStore crea un gruppo di log con un nome come`/aws/mediastore/MyContainerName`. Puoi definire i gruppi di log e specificare quali flussi inserire in ciascun gruppo. Non vi è alcuna quota per il numero di flussi di log che possono appartenere a un gruppo di log.

Per impostazione predefinita, i log vengono conservati a tempo indeterminato e non scadono mai. Puoi modificare la policy di conservazione per ogni gruppo di log mantenendo la conservazione a tempo indeterminato o scegliendo un periodo di conservazione da un giorno a 10 anni.

Impostazione delle autorizzazioni per Amazon CloudWatch

UsaAWS Identity and Access Management (IAM) per creare un ruolo che dia ad AWS Elemental MediaStore l'accesso ad Amazon CloudWatch. Devi eseguire questi passaggi per pubblicare CloudWatch i log per il tuo account. CloudWatch pubblica automaticamente le metriche per il tuo account.

Per consentire MediaStore l'accesso a CloudWatch

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione della console IAM, scegli Policies (Policy), quindi scegli Create policy (Crea policy).
3. Scegliere la scheda JSON e incollare la policy seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/mediastore/*"
        }
    ]
}
```

   Questa politica consente di MediaStore creare gruppi di log e flussi di log per qualsiasi contenitore in qualsiasi regione all'internoAWS del tuo account.
4. Scegli Review policy (Esamina policy).
5. Nella pagina Review policy (Esamina policy), in Name (Nome) immettere **`MediaStoreAccessLogsPolicy`** e quindi scegliere Create policy (Crea policy).
6. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
7. Selezionare il tipo di ruolo Another AWS account (Un altro account AWS).
8. In Account ID (ID account) immettere l'ID dell'account AWS.
9. Scegliere Successivo: Autorizzazioni.

10. Nella casella di ricerca immetti **`MediaStoreAccessLogsPolicy`**.
11. Selezionare la casella di controllo accanto alla nuova policy, quindi scegliere Next: Tags (Successivo: Tag).
12. Scegliere Next: Review (Successivo: Esamina) per visualizzare in anteprima i nuovi utenti.
13. In Role name (Nome ruolo) immettere **`MediaStoreAccessLogs`** e quindi selezionare Create role (Crea ruolo).
14. Nel messaggio di conferma, scegliere il nome del ruolo creato (**`MediaStoreAccessLogs`**).
15. Nella pagina Summary (Riepilogo) del ruolo, selezionare la scheda Trust relationships (Relazioni di trust).
16. Seleziona Edit trust relationship (Modifica relazione di trust).
17. Nel documento di policy, impostare l'entità principale sul servizio MediaStore. L'URL dovrebbe essere simile a questo:

    ```
    "Principal": {
       "Service": "mediastore.amazonaws.com"
    },
    ```

    La policy intera dovrebbe risultare come segue:

    ```
    {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "mediastore.amazonaws.com"
          },
          "Action": "sts:AssumeRole",
          "Condition": {}
        }
      ]
    }
    ```

18. Scegli Update Trust Policy (Aggiorna policy di trust).

Abilitazione della registrazione degli accessi per un container

Per default, AWS Elemental MediaStore non raccoglie i log di accesso. Quando si abilita la registrazione degli accessi in un container, MediaStore fornisce ad Amazon i log di accesso per gli oggetti memorizzati in quel container CloudWatch. I log di accesso forniscono record dettagliati per le richieste che vengono effettuate a qualsiasi oggetto archiviato nel container. I report possono includere informazioni quali il tipo di richiesta, le risorse in essa specificate, l'ora e la data di elaborazione.

> **Important**
>
> L'attivazione di questa funzione non comporta costi aggiuntivi su un container MediaStore. Tuttavia, i file di log distribuiti dal servizio accumulano i consueti addebiti per lo storage. (Puoi eliminare il file di log in qualsiasi momento.) AWS non valuta i costi di trasferimento dati per la distribuzione di file di log, ma addebita le normali tariffe di trasferimento dati per l'accesso ai file di log.

Per abilitare la registrazione degli accessi (AWS CLI)

- In AWS CLI, usa il comando `start-access-logging`.

```
aws mediastore start-access-logging --container-name LiveEvents --region us-west-2
```

  Il comando non ha un valore restituito.

Disabilitazione della registrazione degli accessi per un container

Quando disabiliti la registrazione degli accessi su un contenitore, AWS Elemental MediaStore interrompe l'invio dei log di accesso ad Amazon CloudWatch. Questi log di accesso non vengono salvati e non sono recuperabili.

Per disabilitare la registrazione degli accessi (AWS CLI)

- In AWS CLI, usa il comando `stop-access-logging`.

```
aws mediastore stop-access-logging --container-name LiveEvents --region us-west-2
```

Il comando non ha un valore restituito.

Risoluzione dei problemi di registrazione degli accessi in AWS Elemental MediaStore

Quando i log di MediaStore accesso di AWS Elemental non vengono visualizzati in Amazon CloudWatch, consulta la tabella seguente per cause e risoluzioni potenziali.

> **Note**
>
> Assicurati di abilitare AWS CloudTrail Logs per supportare il processo di risoluzione dei problemi.

Sintomo	Il problema potrebbe essere...	Prova questa soluzione...
Non viene visualizzato alcun CloudTrail evento, anche se CloudTrail i registri sono abilitati.	Il ruolo IAM non esiste o il nome, le autorizzazioni o la policy di attendibilità non sono corretti.	Crea un ruolo con il nome, le autorizzazioni e la policy di attendibilità corrette. Consultare the section called “Impostazione delle autorizzazioni per CloudWatch”.
Hai inviato una richiesta API `DescribeContainer` , ma la risposta mostra che il parametro `AccessLoggingEnabled` ha un valore di `False`. Inoltre, non visualizzi eventi CloudTrail per il ruolo `MediaStoreAccessLogs` quando effettui una chiamata `DescribeLogGroup` , `CreateLogGroup` , `DescribeLogStream` o `CreateLogStream` .	Il ruolo IAM non esiste o il nome, le autorizzazioni o la policy di attendibilità non sono corretti.	Crea un ruolo con il nome, le autorizzazioni e la policy di attendibilità corrette. Consultare the section called “Impostazione delle autorizzazioni per CloudWatch”.
	La registrazione degli accessi non è abilitata sul container.	Abilita i log di accesso per il container. Consultare the section called “Abilitazione della registrazione degli accessi”.

Sintomo	Il problema potrebbe essere...	Prova questa soluzione...

Sulla CloudTrail console, viene visualizzato un evento con un errore di accesso negato relativo al`MediaStoreAccessLogs` ruolo. L' CloudTrail evento potrebbe includere righe come le seguenti:
 	
`"eventSource": "logs.amazonaws.com",`
 	
`"errorCode": "AccessDenied",`
 	
`"errorMessage": "User: arn:aws:sts::111122223333:assumed-role/MediaStoreAccessLogs/MediaStoreAccessLogsSession is not authorized to perform: logs:DescribeLogGroups on resource: arn:aws:logs:us-west-2:111122223333:log-group::log-stream:",`
	Il ruolo IAM non dispone delle autorizzazioni corrette per AWS Elemental MediaStore.	Aggiorna il ruolo IAM per avere le autorizzazioni e la policy di attendibilità corretti. Consultare the section called “Impostazione delle autorizzazioni per CloudWatch”.

Sintomo	Il problema potrebbe essere...	Prova questa soluzione...
Non vedi alcun log per un intero container o più container.	Il tuo account potrebbe aver superato la CloudWatch quota di gruppi di registro per account per regione. Consulta le quote per i gruppi di log nella Amazon CloudWatch Logs User Guide.	Sulla CloudWatch console, stabilisci se il tuo account ha raggiunto la CloudWatch quota per i gruppi di log. Se necessario, richiedere un aumento delle quote.
Vengono visualizzati alcuni log in CloudWatch, ma non tutti i log che ci si aspetta di vedere.	Il tuo account potrebbe aver superato la CloudWatch quota di transazioni al secondo per account per regione. Consulta le quote di cui `PutLogEvents` alla guida per l'utente di Amazon CloudWatch Logs.	Richiedi un aumento della quota di CloudWatch transazioni al secondo per account per regione.

Formato del log di accesso

I file di log di accesso sono costituiti da una sequenza di record di log in formato JSON, dove ogni record di log rappresenta una richiesta. L'ordine dei campi all'interno del log può variare. Di seguito è riportato un esempio di log costituito da due record di log:

```
{
  "Path": "/FootballMatch/West",
  "Requester": "arn:aws:iam::111122223333:user/maria-garcia",
  "AWSAccountId": "111122223333",
```

```
  "RequestID":
 "aaaAAA111bbbBBB222cccCCC333dddDDD444eeeEEE555fffFFF666gggGGG777hhhHHH888iiiIII999jjjJJJ",
  "ContainerName": "LiveEvents",
  "TotalTime": 147,
  "BytesReceived": 1572864,
  "BytesSent": 184,
  "ReceivedTime": "2018-12-13T12:22:06.245Z",
  "Operation": "PutObject",
  "ErrorCode": null,
  "Source": "192.0.2.3",
  "HTTPStatus": 200,
  "TurnAroundTime': 7,
  "ExpiresAt": "2018-12-13T12:22:36Z"
}
 {
  "Path": "/FootballMatch/West",
  "Requester": "arn:aws:iam::111122223333:user/maria-garcia",
  "AWSAccountId": "111122223333",
  "RequestID":
 "dddDDD444eeeEEE555fffFFF666gggGGG777hhhHHH888iiiIII999jjjJJJ000cccCCC333bbbBBB222aaaAAA",
  "ContainerName": "LiveEvents",
  "TotalTime": 3,
  "BytesReceived": 641354,
  "BytesSent": 163,
  "ReceivedTime": "2018-12-13T12:22:51.779Z",
  "Operation": "PutObject",
  "ErrorCode": "ValidationException",
  "Source": "198.51.100.15",
  "HTTPStatus": 400,
  "TurnAroundTime": 1,
  "ExpiresAt": null
}
```


L'elenco di seguito descrive i campi dei record di log.

AWSAccountId

L'ID account AWS dell'account che è stato utilizzato per effettuare la richiesta.

BytesReceived

Il numero di byte nel corpo della richiesta che il server MediaStore riceve.

BytesSent

Il numero di byte nel corpo della risposta inviato dal server MediaStore. Tale valore spesso è identico a quello dell'intestazione `Content-Length` inclusa con le risposte del server.

ContainerName

Il nome del container che ha ricevuto la richiesta.

ErrorCode

Il codice MediaStore di errore (ad esempio`InternalServerError`). Se non si è verificato alcun errore, viene visualizzato il carattere `-`. Un codice di errore può essere visualizzato anche se il codice di stato è 200 (che indica una connessione chiusa o un errore dopo che il server ha avviato lo streaming della risposta).

ExpiresAt

Data e ora di scadenza dell'oggetto. Questo valore si basa sull'età di scadenza impostata da una[transient data rule](#) politica del ciclo di vita applicata al contenitore. Il valore è la data e ora `ISO-8601` ed è basata sull'orologio di sistema dell'host che ha servito la richiesta. Se la politica del ciclo di vita non ha una regola dei dati transitori che si applica all'oggetto o se non è stata applicata alcuna politica del ciclo di vita al contenitore, il valore di questo campo è`null`. Questo campo si applica solo alle seguenti operazioni:`PutObject`,`GetObject`,`DescribeObject`,`eDeleteObject`.

HTTPStatus

Il codice di stato HTTP numerico della risposta.

Operazioni

L'operazione che è stata eseguita, ad esempio `PutObject` o `ListItems`.

Percorso

Il percorso all'interno del container in cui è archiviato l'oggetto. Se l'operazione non accetta un parametro path, viene visualizzato il carattere `-`.

ReceivedTime

L'ora del giorno in cui la richiesta è stata ricevuta. Il valore è la data e ora `ISO-8601` ed è basata sull'orologio di sistema dell'host che ha servito la richiesta.

Richiedente

L'Amazon Resource Name (ARN) dell'utente dell'account che è stato utilizzato per effettuare la richiesta. Per le richieste non autenticate, questo valore è `anonymous`. Se la richiesta non riesce prima del completamento dell'autenticazione, questo campo potrebbe mancare dal registro. Per tali richieste, `ErrorCode` potrebbe identificare il problema di autorizzazione.

RequestID

Una stringa generata da AWS MediaStore Elemental per identificare in maniera univoca ogni richiesta.

Origine

L'indirizzo Internet apparente del richiedente o l'entità principale del servizio AWS che effettua la chiamata. Se proxy e firewall intermedi oscurano l'indirizzo del computer che effettua la richiesta, il valore è impostato su null.

TotalTime

Il numero di millisecondi (ms) durante i quali la richiesta è stata in transito dalla prospettiva del server. Tale valore viene misurato dal momento in cui la richiesta viene ricevuta dal servizio, fino al momento in cui l'ultimo byte della risposta è stato inviato. Questo valore viene misurato dalla prospettiva del server perché misurazioni effettuate dalla prospettiva del client non sono influenzate dalla latenza di rete.

TurnAroundTime

Il numero di millisecondi che sono MediaStore stati necessari per elaborare la richiesta. Questo valore viene misurato dal momento in cui si riceve l'ultimo byte della richiesta al momento in cui viene inviato il primo byte di risposta.

L'ordine dei campi nel log può variare.

Tempo richiesto per l'applicazione delle modifiche dello stato di registrazione

L'applicazione effettiva delle modifiche dello stato di registrazione di un container sulla distribuzione dei file di log richiede tempo. Ad esempio, se si abilita la registrazione per un container, è possibile che nell'ora successiva alcune richieste vengano registrate nel log e altre no. Se si disabilita la registrazione per container B, alcuni log per l'ora successiva potrebbero continuare a essere recapitati, mentre altri no. In tutti i casi, le nuove impostazioni diventano effettive automaticamente.

Distribuzione dei log del server sulla base del miglior tentativo

I report dei log di accesso vengono distribuiti sulla base del miglior tentativo. La maggior parte delle richieste di un container correttamente configurato per la registrazione determinano la distribuzione di un record del log. La maggior parte dei report vengono consegnati entro qualche ora dal momento della creazione, ma possono essere consegnati con maggior frequenza.

La completezza e la tempestività della registrazione degli accessi non è tuttavia garantita. È possibile che il report del log per una richiesta specifica venga consegnato molto tempo dopo l'elaborazione effettiva della richiesta o non venga consegnato affatto. Lo scopo dei log di accesso è fornire un'idea della natura del traffico nel container. I report del log vengono persi raramente, ma la registrazione degli accessi non intende essere un resoconto completo di tutte le richieste.

Il fatto che la funzione di registrazione degli accessi si basi sul miglior tentativo fa sì che i report di utilizzo disponibili nel portale AWS (report Gestione di costi e fatturazione nella AWS Management Console) possano includere una o più richieste di accesso non visibili nel log di accesso distribuito.

Considerazioni in materia di programmazione per il formato dei log di accesso

Di tanto in tanto, è possibile estendere il formato dei log di accesso aggiungendo nuovi campi. Il codice che analizza i log di accesso deve essere scritto per gestire ulteriori campi che non capisce.

CloudWatch Eventi

Amazon CloudWatch Events ti consente di automatizzare iAWS servizi e rispondere automaticamente a eventi di sistema, come i problemi relativi alla disponibilità delle applicazioni o le modifiche delle risorse. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali azioni automatizzate intraprendere quando un evento corrisponde a una regola.

> **Important**
>
> In genere,AWS i servizi forniscono notifiche di CloudWatch eventi a Events in pochi secondi, ma a volte può essere necessario un minuto o più.

Quando un file viene caricato in un contenitore o rimosso da un contenitore, nel CloudWatch servizio vengono generati due eventi in successione:

1. the section called “Evento di modifica dello stato di un oggetto”

2. the section called “Evento di modifica dello stato di un container”

Per informazioni sulla sottoscrizione a questi eventi, consulta Amazon CloudWatch.

Le azioni che possono essere attivate automaticamente includono le seguenti:

- Richiamo di una funzione AWS Lambda
- Richiamo del comando di esecuzione di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di unaAWS SMS coda

Alcuni esempi di utilizzo di CloudWatch Events con AWS Elemental MediaStore includono i seguenti:

- Attivazione di una funzione Lambda ogni volta che viene creato un container
- Notifica di un argomento Amazon SNS quando un oggetto viene eliminato

Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch Events.

Argomenti

- Evento di modifica dello stato MediaStore dell'oggetto AWS Elemental
- Evento di modifica dello stato MediaStore del contenitore AWS Elemental

Evento di modifica dello stato MediaStore dell'oggetto AWS Elemental

Questo evento viene pubblicato quando lo stato di un oggetto cambia (quando l'oggetto è stato caricato o eliminato).

> **Note**
>
> Gli oggetti che scadono a causa di una regola di dati transitoria non emettono un CloudWatch evento quando scadono.

Per informazioni sulla sottoscrizione a questo evento, consulta Amazon CloudWatch.

Oggetto aggiornato

```
{
  "version": "1",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "MediaStore Object State Change",
  "source": "aws.mediastore",
  "account": "111122223333",
  "time": "2017-02-22T18:43:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediastore:us-east-1:111122223333:MondayMornings/Episode1/
Introduction.avi"
  ],
  "detail": {
    "ContainerName": "Movies",
    "Operation": "UPDATE",
    "Path":"TVShow/Episode1/Pilot.avi",
    "ObjectSize":123456,
    "URL": "https://a832p1qeaznlp9.files.mediastore-us-west-2.com/Movies/
MondayMornings/Episode1/Introduction.avi"
  }
}
```

Oggetto rimosso

```
{
  "version": "1",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "MediaStore Object State Change",
  "source": "aws.mediastore",
  "account": "111122223333",
  "time": "2017-02-22T18:43:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediastore:us-east-1:111122223333:Movies/MondayMornings/Episode1/
Introduction.avi"
  ],
  "detail": {
    "ContainerName": "Movies",
    "Operation": "REMOVE",
    "Path":"Movies/MondayMornings/Episode1/Introduction.avi",
    "URL": "https://a832p1qeaznlp9.files.mediastore-us-west-2.com/Movies/
MondayMornings/Episode1/Introduction.avi"
  }
```

```
}
```

Evento di modifica dello stato MediaStore del contenitore AWS Elemental

Questo evento viene pubblicato quando lo stato di un container cambia (quando il container è stato aggiunto o eliminato). Per informazioni sulla sottoscrizione a questo evento, consulta Amazon CloudWatch.

Container creato

```
{
  "version": "1",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "MediaStore Container State Change",
  "source": "aws.mediastore",
  "account": "111122223333",
  "time": "2017-02-22T18:43:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediastore:us-east-1:111122223333:container/Movies"
  ],
  "detail": {
    "ContainerName": "Movies",
    "Operation": "CREATE"
    "Endpoint": "https://a832p1qeaznlp9.mediastore-us-west-2.amazonaws.com"
  }
}
```

Container rimosso

```
{
  "version": "1",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "MediaStore Container State Change",
  "source": "aws.mediastore",
  "account": "111122223333",
  "time": "2017-02-22T18:43:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediastore:us-east-1:111122223333:container/Movies"
  ],
  "detail": {
```

```
    "ContainerName": "Movies",
    "Operation": "REMOVE"
  }
}
```

Monitoraggio di AWS MediaStore Elemental con le CloudWatch metriche di Amazon

Puoi monitorare AWS Elemental MediaStore utilizzando CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili. CloudWatchle statistiche di vengono conservate per un periodo di 15 mesi, per consentire l'accesso alle informazioni storiche e ottenere una prospettiva migliore sull'esecuzione del servizio o dell'applicazione Web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.

Per AWS Elemental MediaStore, potresti voler controllare`BytesDownloaded` e inviare un'email a te stesso quando quella metrica raggiunge una determinata soglia.

Come visualizzare i parametri utilizzando la CloudWatch console

I parametri vengono raggruppati prima in base allo spazio dei nomi del servizio e successivamente in base alle diverse combinazioni di dimensioni all'interno di ogni spazio dei nomi.

1. Accedere aAWS Management Console e aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, selezionare Parametri.
3. In Tutte le metriche, scegli loMediaStore spazio dei nomi AWS/.
4. Scegli la dimensione del parametro per visualizzare i parametri. Ad esempio, seleziona `Request metrics by container` per visualizzare i parametri per i diversi tipi di richieste inviate al container.

Visualizzazione dei parametri usando AWS CLI

- Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/MediaStore"
```

MediaStore Metriche AWS Elemental

La tabella seguente elenca le metriche a cui AWS Elemental MediaStore invia CloudWatch.

> **Note**
>
> Per visualizzare le metriche, devi aggiungere una politica metrica al contenitore per consentire MediaStore l'invio di metriche ad Amazon CloudWatch.

Parametro	Descrizione
`RequestCount`	Il numero totale di richieste HTTP effettuate a un container MediaStore, separate dal tipo di operazione (`Put`, `Get`, `Delete`, `Describe`, `List`). Unità: numero Dimensioni valide: • Nome del container • Nome del gruppo di oggetti • Tipo richiesta Statistiche valide: somma
`4xxErrorCount`	Il numero di richieste HTTP effettuate MediaStore ha provocato un errore 4xx. Unità: numero Dimensioni valide: • Nome del container • Nome del gruppo di oggetti • Tipo richiesta Statistiche valide: somma

Parametro	Descrizione
`5xxErrorCount`	Il numero di richieste HTTP effettuate MediaStore ha provocato un errore 5xx. Unità: numero Dimensioni valide: • Nome del container • Nome del gruppo di oggetti • Tipo richiesta Statistiche valide: somma
`BytesUploaded`	Il numero di byte caricati per le richieste effettuate a un container MediaStore in cui la richiesta include un corpo. Unità: byte Dimensioni valide: • Nome del container • Nome del gruppo di oggetti Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo (come P0,0), massimo (come p100), qualsiasi percentile tra p0,0 e p99,9

Parametro	Descrizione
`BytesDownloaded`	Il numero di byte scaricati per le richieste effettuate a un container MediaStore in cui la risposta include un corpo. Unità: byte Dimensioni valide: • Nome del container • Nome del gruppo di oggetti Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo (come P0,0), massimo (come p100), qualsiasi percentile tra p0,0 e p99,9
`TotalTime`	Il numero di millisecondi durante i quali la richiesta è stata in transito dalla prospettiva del server. Questo valore viene misurato dal momento in cui si MediaStore riceve la richiesta al momento in cui viene inviato l'ultimo byte della risposta. Questo valore viene misurato dalla prospettiva del server perché misurazioni effettuate dalla prospettiva del client non sono influenzate dalla latenza di rete. Unità: millisecondi Dimensioni valide: • Nome del container • Nome del gruppo di oggetti • Tipo richiesta Statistiche valide: media, minimo (come P0,0), massimo (come p100), qualsiasi percentile tra p0,0 e p100

Parametro	Descrizione
`TurnaroundTime`	Il numero di millisecondi che sono MediaStore stati necessari per elaborare la richiesta. Questo valore viene misurato dal momento in cui si MediaStore riceve l'ultimo byte della richiesta al momento in cui viene inviato il primo byte della risposta. Unità: millisecondi Dimensioni valide: • Nome del container • Nome del gruppo di oggetti • Tipo richiesta Statistiche valide: media, minimo (come P0,0), massimo (come p100), qualsiasi percentile tra p0,0 e p100
`ThrottleCount`	Il numero di richieste HTTP effettuate a MediaStore tale scopo è stato limitato. Unità: numero Dimensioni valide: • Nome del container • Nome del gruppo di oggetti • Tipo richiesta Statistiche valide: somma

Etichettatura delle risorse AWS MediaStore Elemental

Un tag è un'etichetta di attributi personalizzata assegnata dall'utente o da AWS a una risorsa AWS. Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.

- Un campo facoltativo noto come valore del tag (ad esempio, `111122223333` o `Production`). Non specificare il valore del tag equivale a utilizzare una stringa vuota. Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra lettere maiuscole e minuscole.

I tag consentono di eseguire le seguenti operazioni:

- Identificare e organizzare le risorse AWS. Molti servizi AWS supportano il tagging, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che le risorse sono correlate. Ad esempio, puoi assegnare lo stesso tag a un contenitore AWS MediaStore *`Elemental`* che assegni a un input. AWS Elemental MediaLive
- Tenere traccia dei costi AWS. Questi tag vengono attivati nel pannello di controllo di AWS Billing and Cost Management. AWS utilizza i tag per organizzare in categorie i costi e invia all'utente un report mensile di allocazione dei costi. Per ulteriori informazioni, consulta la pagina sull'utilizzo dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing.

Le seguenti sezioni forniscono ulteriori informazioni sui tag per AWS Elemental MediaStore.

Risorse supportate in AWS Elemental MediaStore

Le seguenti risorse nella codifica del MediaStore supporto AWS Elemental:

- *`container`*

Per informazioni sull'aggiunta e la gestione dei tag, consulta Gestione dei tag.

AWS Elemental MediaStore non supporta la funzionalità di controllo degli accessi basata su tag di AWS Identity and Access Management (IAM).

Convenzioni di denominazione e utilizzo dei tag

Le seguenti convenzioni di base di denominazione e utilizzo si applicano all'uso dei tag con le risorse AWS MediaStore Elemental:

- Ogni risorsa può avere un massimo di 50 tag.
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- La lunghezza massima delle chiavi di tag è 128 caratteri Unicode in UTF-8.

- Il valore massimo dei tag è 256 caratteri Unicode in UTF-8.
- I caratteri consentiti sono lettere, numeri, spazi rappresentabili in formato UTF-8, oltre ai seguenti caratteri: . : + = @ _ / - (trattino). Le risorse Amazon EC2 consentono qualsiasi carattere.
- i valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole; Come best practice, è consigliabile definire una strategia per l'uso delle lettere maiuscole e minuscole nei tag e implementarla costantemente in tutti i tipi di risorse. Ad esempio, puoi decidere se utilizzare `Costcenter`, `costcenter` o `CostCenter` e utilizzare la stessa convenzione per tutti i tag. Non utilizzare tag simili con lettere maiuscole o minuscole incoerenti.
- Il prefisso `aws:` non può essere utilizzato con i tag; è riservato per l'uso in AWS. Non è possibile modificare né eliminare le chiavi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per la quota di tag per risorsa.

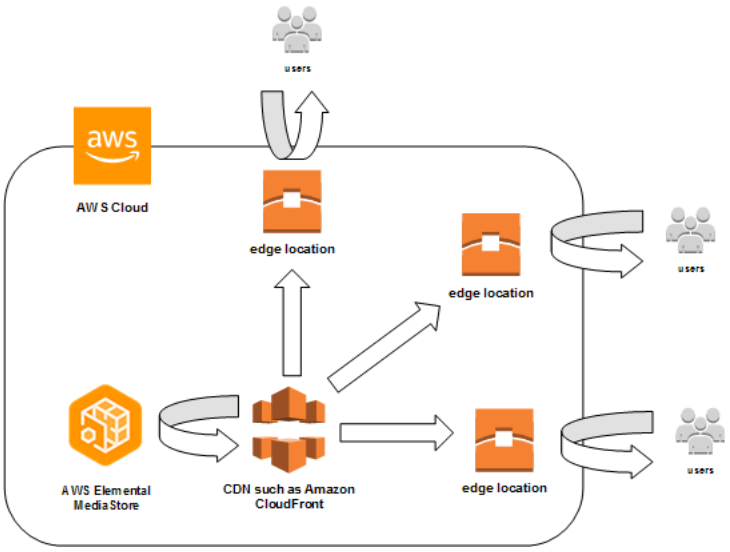
Gestione dei tag

I tag sono formati dalle proprietà `Key` e `Value` in una risorsa. Puoi utilizzare l'API AWS CLI o l' MediaStore API per aggiungere, modificare o eliminare i valori di queste proprietà. Per informazioni sull'utilizzo dei tag, consulta le seguenti sezioni nell'AWS Elemental MediaStore API Reference:

- CreateContainer
- ListTagsForResource
- Risorse
- TagResource
- UntagResource

Utilizzo delle reti di distribuzione di contenuti (CDN)

Puoi utilizzare una rete di distribuzione di contenuti (CDN) come Amazon CloudFront per distribuire i contenuti archiviati in AWS Elemental MediaStore. Una CDN è un insieme di server distribuiti a livello globale che effettua il caching di contenuti quali i video. Quando un utente richiede i tuoi contenuti, la CDN instrada la richiesta alla edge location che offre la latenza minore. Se il caching è già stato effettuato in tale edge location, la CDN distribuisce immediatamente i contenuti. Se il contenuto non si trova attualmente in quella posizione periferica, il CDN lo recupera dall'origine (ad esempio il MediaStore contenitore) e lo distribuisce all'utente.



Argomenti

- Consentire CloudFront ad Amazon di accedere al tuo MediaStore contenitore AWS Elemental
- Interazione MediaStore di AWS Elemental con le cache HTTP

Consentire CloudFront ad Amazon di accedere al tuo MediaStore contenitore AWS Elemental

Puoi usare Amazon CloudFront per distribuire i contenuti archiviati in un contenitore in AWS Elemental MediaStore. Questa operazione può essere eseguita in uno dei seguenti modi:

- Utilizzo di Origin Access Control (OAC)- (Consigliato) Utilizzate questa opzione seRegione AWS supportate la funzionalità OAC di CloudFront.

- Utilizzo di segreti condivisi- Utilizzate questa opzione seRegione AWS non supportate la funzionalità OAC di CloudFront.

Utilizzo di Origin Access Control (OAC)

Puoi utilizzare la funzionalità Origin Access Control (OAC) di Amazon CloudFront per proteggere MediaStore le origini di AWS Elemental con una maggiore sicurezza. È possibile abilitare AWSSignature Version 4 (SIGv4) sulle CloudFront richieste di MediaStore origine e impostare quando e CloudFront se firmare le richieste. Puoi accedere alla funzionalità OAC CloudFront tramite console, API, SDK o CLI e non sono previsti costi aggiuntivi per il suo utilizzo.

Per ulteriori informazioni sull'utilizzo della funzionalità OAC con MediaStore, consulta Restricting access to a MediaStore origin nella Amazon CloudFront Developer Guide.

Utilizzo di segreti condivisi

Se nonRegione AWS supporta la funzionalità OAC di Amazon CloudFront, puoi allegare una policy al tuo MediaStore contenitore AWS Elemental che garantisca l'accesso in lettura o superiore a CloudFront.

> **Note**
>
> Ti consigliamo di utilizzare la funzione OAC se laRegione AWS supporta. Le seguenti procedure richiedono la configurazione MediaStore e l' CloudFront uso di segreti condivisi per limitare l'accesso ai MediaStore contenitori. Per seguire le migliori pratiche di sicurezza, questa configurazione manuale richiede una rotazione periodica dei segreti. Con OAC on MediaStore origin, puoi chiedere di firmare le richieste utilizzando SigV4 e inoltrarle a esse MediaStore per la corrispondenza delle firme, eliminando la necessità di utilizzare e ruotare i segreti. CloudFront Ciò garantisce che le richieste vengano verificate automaticamente prima che i contenuti multimediali vengano forniti, rendendo la distribuzione dei contenuti multimediali CloudFront più semplice MediaStore e sicura.

Per consentire l'accesso CloudFront al contenitore (console)

1. Apri la MediaStore console all'indirizzo https://console.aws.amazon.com/mediastore/.
2. Nella pagina Containers (Container), scegliere il nome del container.

Viene visualizzata la pagina dei dettagli del container.

3. Nella sezione Politica relativa ai container, allega una politica che garantisca ad Amazon l'accesso in lettura o un livello superiore CloudFront.

   Example

   La seguente politica di esempio, simile alla politica di esempio per l'accesso alla lettura pubblica tramite HTTPS, soddisfa questi requisiti perché consente`GetObject` l'invio di`DescribeObject` comandi da parte di chiunque invii richieste al tuo dominio tramite HTTPS. Inoltre, la seguente politica di esempio protegge meglio il flusso di lavoro perché consente CloudFront l'accesso agli MediaStore oggetti solo quando la richiesta avviene tramite una connessione HTTPS e contiene l'intestazione Referer corretta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudFrontRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "mediastore:GetObject",
        "mediastore:DescribeObject"
      ],
      "Resource": "arn:aws:mediastore:<region>:<owner acct
 number>:container/<container name>/*",
      "Condition": {
        "StringEquals": {
          "aws:Referer": "<secretValue>"
        },
        "Bool": {
          "aws:SecureTransport": "true"
        }
      }
    }
 ]}
```

4. Nella sezione Container CORS policy (Policy CORS container), assegnare una policy che garantisca il livello di accesso desiderato.

> **Note**
>
> Una policy CORS è necessaria solo per fornire l'accesso a un lettore basato su browser.

5. Annotare i dettagli riportati di seguito:
   - L'endpoint dati assegnato al tuo container . Questa informazione è reperibile nella sezione Info della pagina Containers (Container). In CloudFront, l'endpoint dei dati viene definito nome di dominio di origine.
   - La struttura della cartella nel container in cui gli oggetti vengono archiviati. Nel CloudFront, questo viene chiamato percorso di origine. Questa impostazione è facoltativa. Per ulteriori informazioni sui percorsi di origine, consulta la Amazon CloudFront Developer Guide.
6. In CloudFront, crea una distribuzione configurata per fornire contenuti da AWS Elemental MediaStore. Saranno necessarie le informazioni raccolte nella fase precedente.

Dopo aver allegato la policy ai MediaStore contenitori, è necessario CloudFront configurare l'utilizzo solo delle connessioni HTTPS per le richieste di origine e aggiungere anche un'intestazione personalizzata con il valore segreto corretto.

Per configurare l'accesso CloudFront al contenitore tramite una connessione HTTPS con un valore segreto per l'intestazione Referer (console)

1. Aprire la CloudFront console.
2. Nella pagina Origini, scegli la tua MediaStore origine.
3. Scegliere Edit (Modifica).
4. Scegli HTTPS solo per il protocollo.
5. Nella sezione Aggiungi intestazione personalizzata, scegli Aggiungi intestazione.
6. Per il nome, scegli Referer. Per il valore, usa la stessa <secretValue>stringa che hai usato nella politica del contenitore.
7. Scegli Salva e lascia che le modifiche vengano implementate.

Interazione MediaStore di AWS Elemental con le cache HTTP

AWS Elemental MediaStore archivia gli oggetti in modo che possano essere memorizzati nella cache in modo corretto ed efficiente da reti di distribuzione di contenuti (CDN) come Amazon CloudFront.

Quando un utente finale o una rete CDN recupera un oggetto da MediaStore, il servizio restituisce le intestazioni HTTP che influiscono sul comportamento di memorizzazione nella cache dell'oggetto. Gli standard per il comportamento di memorizzazione nella cache HTTP 1.1 si trovano nella sezione 13 RFC2616. Queste intestazioni sono:

- **`ETag`** (non personalizzabile): l'intestazione del tag entità è un identificatore univoco per la risposta inviata da MediaStore . I CDN e i browser Web conformi agli standard utilizzano questo tag come chiave con cui memorizzare nella cache l'oggetto. MediaStore genera automaticamente un`ETag` per ogni oggetto quando viene caricato. Puoi visualizzare i dettagli di un oggetto per determinarne il valore ETag.
- **`Last-Modified`**(non personalizzabile) - Il valore di questa intestazione indica la data e l'ora in cui l'oggetto è stato modificato. MediaStore genera automaticamente questo valore quando l'oggetto viene caricato.
- **`Cache-Control`** (personalizzabile): il valore di questa intestazione controlla per quanto tempo un oggetto deve essere memorizzato nella cache prima che la CDN controlli se è stato modificato. Puoi impostare questa intestazione su qualsiasi valore quando carichi un oggetto in un MediaStore contenitore utilizzando la CLI o l'API. Il set completo dei valori validi è descritto nella documentazione HTTP/1.1. Se non imposti questo valore quando carichi un oggetto, MediaStore non restituirà questa intestazione quando l'oggetto viene recuperato.

  Un caso di utilizzo comune per l'intestazione Cache-Control consiste nel specificare una durata per la memorizzazione dell'oggetto nella cache. Supponi, ad esempio, di avere un file manifest video che viene spesso sovrascritto da un codificatore. Puoi impostare `max-age` su 10 per indicare che l'oggetto deve essere memorizzato nella cache per soli 10 secondi. In alternativa supponi di avere un segmento video memorizzato che non verrà mai sovrascritto. Puoi impostare `max-age` per questo oggetto su 31536000 per memorizzare l'oggetto nella cache per circa 1 anno.

Richieste condizionali

Richieste condizionali a MediaStore

MediaStore risponde in modo identico alle richieste condizionali (utilizzando intestazioni di richiesta come`If-Modified-Since` e`If-None-Match`, come descritto in RFC7232) e alle richieste incondizionate. Ciò significa che quando MediaStore riceve una`GetObject` richiesta valida, il servizio restituisce sempre l'oggetto anche se il client lo possiede già.

Richieste condizionali alle CDN

Le CDN che forniscono contenuti per conto di MediaStore possono elaborare le richieste condizionali restituendole`304 Not Modified`, come descritto nella sezione 4.1 di RFC7232. Ciò significa che non è necessario trasferire il contenuto completo dell'oggetto, poiché il richiedente dispone già di un oggetto che corrisponde alla richiesta condizionale.

Le CDN (e altre cache conformi a HTTP/1.1) basano queste decisioni sulle intestazioni `ETag` e `Cache-Control` inoltrate dai server di origine. Per controllare la frequenza con cui i CDN interrogano i server di MediaStore origine per gli aggiornamenti degli oggetti recuperati ripetutamente, imposta le`Cache-Control` intestazioni di tali oggetti quando li carichi MediaStore.

Quote in AWS Elemental MediaStore

La console Service Quotas fornisce le informazioni sulle MediaStore quote di AWS Elemental. Oltre a visualizzare le quote predefinite, è possibile utilizzare la console Service Quotas per richiedere aumenti di quota per le quote modificabili.

La tabella seguente descrive le quote, precedentemente denominate limiti, in AWS Elemental MediaStore. Le quote rappresentano il numero massimo di risorse di servizio o operazioni per l'account AWS.

> **Note**
>
> Per assegnare quote a singoli contenitori all'interno del tuo account, contatta AWS Support o il tuo account manager. Questa opzione può aiutarti a suddividere i limiti a livello di account tra i tuoi contenitori, per evitare che un contenitore esaurisca l'intera quota.

Operazione o risorsa	Quota predefinita	Commenti
Container	100	Numero massimo di container che puoi creare in questo account.
Livelli di cartella	10	Numero massimo di livelli di cartella che puoi creare in un container. Puoi creare il numero di cartelle che desideri, per non più di 10 livelli all'interno di un container.
Cartelle	Illimitato	Puoi creare il numero di cartelle che desideri, per non più di 10 livelli all'interno di un container.
Dimensione oggetto	25 MB	Dimensione massima del file di un singolo oggetto.
Oggetti	Illimitato	Puoi caricare tutti gli oggetti che desideri in una cartella o in un contenitore nel tuo account.

Operazione o risorsa	Quota predefinita	Commenti
Frequenza delle richieste API DeleteObject	100	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota.
Frequenza delle richieste API DescribeObject	1.000	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota.
Frequenza delle richieste GetObject API per la disponibilità di caricamento standard	1.000	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota.
Frequenza delle richieste GetObject API per la disponibilità di caricamento in streaming	25	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota.
Frequenza delle richieste API ListItems	5	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota.

Operazione o risorsa	Quota predefinita	Commenti
Frequenza delle richieste PutObject API per la codifica di trasferimento chunked (nota anche come disponibilità di caricamento in streaming)	10	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota. Nella richiesta, specificare il TPS richiesto e la dimensione media dell'oggetto.
Frequenza delle richieste PutObject API per la disponibilità di caricamento standard	100	Il numero massimo di richieste di operazioni che puoi effettuare al secondo. Ulteriori richieste verranno sottoposte a throttling. È possibile richiedere un aumento della quota. Nella richiesta, specificare il TPS richiesto e la dimensione media dell'oggetto.
Regole di una policy di parametro	10	Numero massimo di regole che è possibile includere in una policy di parametro.
Regole in una policy del ciclo di vita degli oggetti	10	Il numero massimo di regole che puoi includere in una policy del ciclo di vita degli oggetti.

Informazioni MediaStore relative ad AWS Elemental

La tabella seguente elenca le risorse correlate che si riveleranno utili durante l'utilizzo di AWS Elemental MediaStore.

- Corsi e seminari: collegamenti a corsi basati su ruoli e di specializzazione nonché a corsi gestiti dall'utente per affinareAWS le proprie competenze e acquisire esperienza pratica.
- AWSCentro per sviluppatori: esplora i tutorial, scarica gli strumenti e scopri di più sugli eventi per gliAWS sviluppatori.
- AWSStrumenti per sviluppatori: collegamenti a strumenti per sviluppatori, SDK, kit di strumenti IDE e strumenti a riga di comando per lo sviluppo e la gestione delleAWS applicazioni.
- Centro risorse per iniziare: scopri come configurare il tuoAccount AWS, entrare a far parte dellaAWS community e lanciare la tua prima applicazione.
- Esercitazioni pratiche: scopri le step-by-step esercitazioni per avviare la tua prima applicazione suAWS.
- AWSWhitepaper: collegamenti a un elenco completo diAWS whitepaper tecnici, relativi ad argomenti come l'architettura, la sicurezza e l'economia, creati daAWS Solution Architect o da altri esperti tecnici.
- AWS SupportCentro : il centro in cui creare e gestire i tuoi casi AWS Support. Include inoltre link ad altre risorse utili, quali forum, domande frequenti di tipo tecnico, stato d'integrità del servizio e AWS Trusted Advisor.
- AWS Support- La pagina Web principale che include le informazioni suAWS Support one-on-one, un canale di assistenza rapida che aiuta a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS.
- AWS Termini di utilizzo del sito: informazioni dettagliate sul copyright e i marchi, l'account, la licenza, l'accesso al sito e altri argomenti.

Cronologia dei documenti per la Guida per l'utente

La tabella seguente descrive la documentazione per questa versione di AWS Elemental MediaStore. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile abbonarti a un feed RSS.

Modifica	Descrizione	Data
Miglioramento dell'Origin Access Control (OAC)	Aggiunta di informazioni su come utilizzare OAC con AWS Elemental MediaStore.	17 aprile 2023
Aggiornamenti delle quote	Valore e descrizione della quota corretti per`Rules in a Metric Policy`.	25 ottobre 2022
ExpiresAt campo	I log di accesso ora includono un`ExpiresAt` campo che indica la data e l'ora di scadenza dell'oggetto in base alle regole relative ai dati transitori nella politica del ciclo di vita del contenitore.	16 luglio 2020
Regole di transizione del ciclo di vita	Puoi ora aggiungere una regola di transizione del ciclo di vita alla policy del ciclo di vita dell'oggetto che imposta gli oggetti da spostare nella classe di archiviazione con accesso non frequente (IA) dopo aver raggiunto una certa età.	20 aprile 2020
Contenitore vuoto	Puoi eliminare tutti gli oggetti all'interno di un container contemporaneamente.	7 aprile 2020

Support per le CloudWatch metriche di Amazon	Puoi impostare una politica di metrica per stabilire a quali metriche MediaStore inviare le metriche CloudWatch.	30 marzo 2020
Jolly nelle regole di eliminazione degli oggetti	In una policy del ciclo di vita degli oggetti, è ora possibile utilizzare un carattere jolly in una regola dell'oggetto di eliminazione. Ciò consente di specificare i file in base al nome del file o all'estensione che si desidera eliminare dal servizio dopo un certo numero di giorni.	20 dicembre 2019
Criteri relativi al ciclo di vita degli oggetti	Ora puoi aggiungere una regola alla policy del ciclo di vita degli oggetti che indica la scadenza per età in secondi.	13 settembre 2019
Supporto AWS CloudFormation	Puoi ora utilizzare un modello AWS CloudFormation per creare un container automaticamente. Il modello AWS CloudFormation gestisce i dati per cinque operazioni API: creazione di un container, impostazione della registrazione degli accessi, aggiornamento della policy del container di default, aggiunta di una policy CORS e aggiunta della policy del ciclo di vita degli oggetti.	17 maggio 2019

Quote per la disponibilità di caricamento in streaming	Per gli oggetti con disponibilità di upload in streaming (trasferimento a pezzi di oggetti), l'operazione `PutObject` non può superare i 10 TPS e l'operazione `GetObject` non può superare i 25 TPS.	8 Aprile 2019
Trasferimento di oggetti in blocchi	Aggiunto il supporto per il trasferimento a blocchi di oggetti. Questa funzionalità consente di specificare che un oggetto è disponibile per il download prima che sia completamente caricato.	5 aprile 2019
Registrazione degli accessi	AWS Elemental MediaStore ora supporta la registrazione degli accessi, che fornisce record dettagliati per le richieste che sono effettuate agli oggetti situate in un contenitore.	25 febbraio 2019
Criteri relativi al ciclo di vita degli oggetti	Aggiunto il supporto per le policy del ciclo di vita degli oggetti, che gestiscono la data di scadenza di oggetti all'interno del container corrente.	12 dicembre 2018
Quota di dimensioni degli oggetti aumentata	La quota della dimensione di un oggetto è ora di 25 MB.	10 ottobre 2018
Quota di dimensioni degli oggetti aumentata	La quota per la dimensione di un oggetto è ora di 20 MB.	6 settembre 2018

Integrazione di AWS CloudTrail	Il contenuto dell' CloudTrail integrazione è stato aggiornato per allinearlo alle recenti modifiche al CloudTrail servizio.	12 luglio 2018
Collaborazione CDN	Sono state aggiunte informazioni su come utilizzare AWS Elemental MediaStore con una rete di distribuzione di contenuti (CDN) come Amazon CloudFront.	14 aprile 2018
Configurazioni CORS	AWS Elemental MediaStore ora supporta la funzionalità CORS (Cross-Origin Resource Sharing, condivisione delle risorse multiorigine), che consente alle applicazioni Web dei clienti caricate in un dominio possono interagire con le risorse situate in un dominio differente.	7 febbraio 2018
Nuovo servizio e guida	Questa è la versione iniziale del servizio di origine e archiviazione video, AWS Elemental MediaStore, e della AWS Elemental MediaStore User Guide.	27 Novembre 2017

Note

- I ServiziAWS multimediali non sono progettati o destinati all'uso con applicazioni o in situazioni che richiedono prestazioni a prova di guasto, come operazioni di sicurezza personale, sistemi di navigazione o comunicazione, controllo del traffico aereo o macchine

di supporto vitale in cui l'indisponibilità, l'interruzione o il guasto dei servizi potrebbero causare morte, lesioni personali, danni alla proprietà o danni ambientali.

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

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