



Guida per l'utente

# Amazon Managed Service per Prometheus



# Amazon Managed Service per Prometheus: Guida per l'utente

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

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

---

# Table of Contents

Cos'è il servizio gestito da Amazon per Prometheus? .....	1
Regioni supportate .....	1
Prezzi .....	3
Supporto premium .....	4
Nozioni di base .....	5
Configurazione .....	5
Registrati per un Account AWS .....	5
Crea un utente con accesso amministrativo .....	6
Creare un'area di lavoro .....	7
Inserisci i parametri di Prometheus nell'area di lavoro .....	8
Fase 1: aggiunta di nuovi repository del grafico Helm .....	9
Fase 2: creazione di un namespace Prometheus. ....	9
Fase 3: configurazione dei ruoli IAM per gli account del servizio. ....	10
Fase 4: configurazione del nuovo server e avvio dell'importazione dei parametri .....	10
Esegui una ricerca sui parametri Prometheus .....	12
Gestione delle aree di lavoro .....	14
Creare un'area di lavoro .....	14
Modificare un'area di lavoro .....	17
Trova il tuo spazio di lavoro ARN .....	18
Eliminazione di un'area di lavoro. ....	18
Parametri di acquisizione .....	20
AWS collezionisti gestiti .....	21
Utilizzo di un raccoglitore gestito .....	22
Parametri compatibili con Prometheus .....	36
Raccoglitori gestiti dal cliente .....	37
Proteggi l'importazione dei tuoi parametri .....	38
ADOT Collectors .....	39
Raccoglitori Prometheus .....	55
Dati di disponibilità elevata .....	64
Interroga i tuoi parametri .....	72
Protezione delle interrogazioni dei parametri .....	72
Utilizzo AWS PrivateLink con Amazon Managed Service for Prometheus .....	38
Autenticazione e autorizzazione .....	38
Configurazione di Grafana gestito da Amazon .....	73

Connessione ad Grafana gestito da Amazon in un VPC privato .....	74
Configurazione di Grafana open source .....	74
Configurazione di AWS SigV4 .....	75
Aggiungi l'origine dati Prometheus a Grafana .....	76
Risoluzione dei problemi se l'opzione Salva ed esegui test non funziona .....	78
Configurare Grafana in esecuzione in Amazon EKS .....	79
AWS Configura SigV4 .....	79
Imposta ruoli IAM per gli account del servizio .....	80
Aggiorna il server Grafana utilizzando Helm .....	81
Aggiungi l'origine dati Prometheus a Grafana .....	81
Interrogazione tramite API compatibili con Prometheus .....	82
Utilizzo di awscurl per interrogare le API compatibili con Prometheus .....	83
Informazioni sulle statistiche nella risposta di interrogazione dell'API .....	85
Regole di registrazione e regole di avviso .....	89
Autorizzazioni IAM necessarie .....	90
Creazione di un file di regole .....	91
Caricamento di un file di configurazione delle regole nel servizio gestito da Amazon per Prometheus .....	92
Modifica di un file di configurazione delle regole .....	94
Risoluzione dei problemi per ruler .....	95
Alert Manager .....	97
Autorizzazioni IAM necessarie .....	98
Creazione di un file di configurazione di alert manager .....	99
Configurazione del ricevitore di avvisi .....	101
(Facoltativo) Creazione di un nuovo argomento Amazon SNS .....	102
Autorizzazione al servizio gestito da Amazon per Prometheus per inviare messaggi al tuo argomento Amazon SNS .....	102
Specificare l'argomento di Amazon SNS nel file di configurazione di alert manager .....	105
(Facoltativo) Configurazione di alert manager per inviare JSON ad Amazon SNS .....	106
(Facoltativo) Invio da Amazon SNS verso altre destinazioni .....	108
Regole di convalida e troncamento dei messaggi del ricevitore SNS .....	109
Caricamento del file di configurazione di alert manager .....	110
Integrazione degli avvisi con Grafana .....	113
Prerequisiti .....	113
Configurazione di Amazon Managed Grafana .....	114
Risoluzione dei problemi di alert manager .....	115

Avviso di contenuto vuoto .....	115
Avviso non ASCII .....	116
Avviso non valido key/value .....	116
Avviso di limite dei messaggi .....	117
Nessun errore di policy basata su risorse .....	117
Registrazione di log e monitoraggio .....	119
CloudWatch metriche .....	119
Impostazione di una CloudWatch sveglia .....	125
CloudWatch Registri .....	126
Configurazione dei registri CloudWatch .....	126
Comprendi e ottimizza i costi .....	129
Cosa contribuisce ai miei costi? .....	129
Qual è il modo migliore per ridurre i miei costi? Come posso ridurre i costi di acquisizione? .....	129
Qual è il modo migliore per ridurre i costi delle mie richieste? .....	129
Se riduco il periodo di conservazione dei miei parametri, ciò contribuirà a ridurre la mia fattura totale? .....	130
Come posso mantenere bassi i costi delle mie richieste di avviso? .....	130
Quali parametri posso utilizzare per monitorare i miei costi? .....	131
Posso controllare la mia fattura in qualsiasi momento? .....	131
Perché la mia fattura è più alta all'inizio del mese rispetto alla fine del mese? .....	131
Ho eliminato tutte le mie aree di lavoro Amazon Managed Service for Prometheus, ma sembra che continuino a ricevere degli addebiti. Cosa potrebbe succedere? .....	132
Integrazioni .....	133
Monitoraggio dei costi di Amazon EKS .....	133
AWS Observability Accelerator .....	134
Prerequisiti .....	134
Utilizzo dell'esempio di monitoraggio dell'infrastruttura .....	135
AWS Controller per Kubernetes .....	136
Prerequisiti .....	137
Implementazione di un'area di lavoro .....	138
Configurare il cluster per la scrittura remota .....	142
CloudWatch Metriche di Amazon con Firehose .....	144
Infrastruttura .....	144
Creazione di uno CloudWatch stream Amazon .....	147
Rimozione .....	148
Sicurezza .....	149

Protezione dei dati .....	150
Dati raccolti da Amazon Managed Service per Prometheus .....	151
Crittografia a riposo .....	152
Identity and Access Management .....	165
Destinatari .....	166
Autenticazione con identità .....	166
Gestione dell'accesso con policy .....	170
In che modo il servizio gestito da Amazon per Prometheus funziona con IAM .....	173
Esempi di policy basate su identità .....	180
AWS politiche gestite .....	183
Risoluzione dei problemi .....	195
Autorizzazioni e policy IAM .....	197
Permessi di Amazon Managed Service per Prometheus .....	197
Esempio di policy IAM .....	200
Convalida della conformità .....	201
Resilienza .....	202
Sicurezza dell'infrastruttura .....	203
Uso di ruoli collegati ai servizi .....	203
Il ruolo dello scraping dei parametri .....	204
CloudTrail tronchi .....	206
Informazioni su Amazon Managed Service per Prometheus in CloudTrail .....	206
Informazioni sulle voci dei file di log di Amazon Managed Service for Prometheus .....	208
Imposta ruoli IAM per gli account di servizio. ....	212
Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS. ....	213
Imposta ruoli IAM per gli account di servizio per le domande delle metriche .....	216
Endpoint VPC di interfaccia .....	219
Creazione di un endpoint VPC di interfaccia per Amazon Managed Service per Prometheus .....	220
Risoluzione dei problemi .....	223
429 o limita gli errori superati .....	223
Vedo esempi duplicati .....	224
Vedo errori sui timestamp dei campioni .....	224
Viene visualizzato un messaggio di errore relativo a un limite .....	225
L'output del server Prometheus locale supera il limite. ....	225
Alcuni dei miei dati non vengono visualizzati .....	226
Assegnazione di tag .....	228

Taggare le aree di lavoro .....	229
Aggiunta di tag a un'area di lavoro .....	229
Visualizzazione dei tag per un'area di lavoro .....	231
Come modificare i tag per un'area di lavoro .....	232
Rimuovi un tag da un'area di lavoro .....	233
Tag dei namespace dei gruppi di regole .....	235
Aggiungi un tag a un namespace dei gruppi di regole .....	235
Visualizzazione dei tag per un namespace dei gruppi di regole .....	237
Modifica i tag per un namespace dei gruppi di regole .....	238
Rimuovere un tag da un namespace dei gruppi di regole .....	239
Quote del servizio .....	242
Quote del servizio .....	242
Serie attive (impostazione predefinita) .....	247
Limitazione dell'ingestione .....	248
Limiti aggiuntivi per i dati importati .....	249
Documentazione di riferimento delle API .....	250
Amazon Managed Service for Prometheus .....	250
Utilizzo di Amazon Managed Service per Prometheus con un SDK AWS .....	250
API compatibili con Prometheus .....	251
CreateAlertManagerAlerts .....	251
DeleteAlertManagerSilence .....	253
GetAlertManagerStatus .....	254
GetAlertManagerSilence .....	255
GetLabels .....	256
GetMetricMetadata .....	258
GetSeries .....	260
ListAlerts .....	262
ListAlertManagerAlerts .....	263
ListAlertManagerAlertGroups .....	264
ListAlertManagerReceivers .....	266
ListAlertManagerSilences .....	267
ListRules .....	269
PutAlertManagerSilences .....	270
QueryMetrics .....	272
RemoteWrite .....	274
Cronologia dei documenti .....	276

---

Glossario per AWS .....	281
.....	cclxxxii

# Cos'è il servizio gestito da Amazon per Prometheus?

Il servizio gestito da Amazon per Prometheus è un servizio di monitoraggio serverless compatibile con Prometheus per i parametri dei container che semplifica il monitoraggio sicuro di ambienti container su larga scala. Con il servizio gestito da Amazon per Prometheus, puoi utilizzare lo stesso modello di dati open source Prometheus e lo stesso linguaggio di interrogazione che usi oggi per monitorare le prestazioni dei tuoi carichi di lavoro containerizzati e anche godere di una maggiore scalabilità, disponibilità e sicurezza senza dover gestire l'infrastruttura sottostante.

Il servizio gestito da Amazon per Prometheus ridimensiona automaticamente l'acquisizione, il salvataggio e l'interrogazione dei parametri operativi man mano che i carichi di lavoro aumentano e diminuiscono. Si integra con i servizi AWS di sicurezza per consentire un accesso rapido e sicuro ai dati.

Il servizio gestito da Amazon per Prometheus è progettato per garantire un'elevata disponibilità utilizzando implementazioni multiple con zone di disponibilità (Multi-AZ). I dati inseriti in uno spazio di lavoro vengono replicati in tre zone di disponibilità nella stessa regione.

Il servizio gestito da Amazon per Prometheus funziona con cluster di container eseguiti su Amazon Elastic Kubernetes Service e ambienti Kubernetes autogestiti.

Con il servizio gestito da Amazon per Prometheus, usi lo stesso modello di dati open source Prometheus e lo stesso linguaggio di interrogazione Prometheus che usi con Prometheus. I team di progettazione possono utilizzare ProMQL per filtrare, aggregare e generare allarmi in base ai parametri e ottenere rapidamente visibilità delle prestazioni senza modifiche al codice. Il servizio gestito da Amazon per Prometheus offre funzionalità di interrogazione flessibili senza costi operativi e complessità.

Le metriche inserite in un'area di lavoro vengono archiviate per 150 giorni per impostazione predefinita e vengono quindi eliminate automaticamente. [Questa lunghezza è una quota regolabile.](#)

## Regioni supportate

Il servizio gestito da Amazon per Prometheus supporta attualmente le seguenti regioni:

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	aps.us-east-2.amazonaws.com	HTTPS
		aps-workspaces.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	aps.us-east-1.amazonaws.com	HTTPS
		aps-workspaces.us-east-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	aps.us-west-2.amazonaws.com	HTTPS
		aps-workspaces.us-west-2.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	aps.ap-south-1.amazonaws.com	HTTPS
		aps-workspaces.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	aps.ap-northeast-2.amazonaws.com	HTTPS
		aps-workspaces.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	aps.ap-southeast-1.amazonaws.com	HTTPS
		aps-workspaces.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	aps.ap-southeast-2.amazonaws.com	HTTPS
		aps-workspaces.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	aps.ap-northeast-1.amazonaws.com	HTTPS
		aps-workspaces.ap-northeast-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Frankfurt)	eu-central-1	aps.eu-central-1.amazonaws.com	HTTPS
		aps-workspaces.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	aps.eu-west-1.amazonaws.com	HTTPS
		aps-workspaces.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	aps.eu-west-2.amazonaws.com	HTTPS
		aps-workspaces.eu-west-2.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	aps.eu-west-3.amazonaws.com	HTTPS
		aps-workspaces.eu-west-3.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	aps.eu-north-1.amazonaws.com	HTTPS
		aps-workspaces.eu-north-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	aps.sa-east-1.amazonaws.com	HTTPS
		aps-workspaces.sa-east-1.amazonaws.com	HTTPS

## Prezzi

Sono previsti costi per l'inserimento e l'archiviazione dei parametri. I costi di archiviazione si basano sulla dimensione compressa dei campioni metrici e dei metadati. Per ulteriori informazioni, consultare [Prezzi del servizio gestito da Amazon per Prometheus](#).

Puoi utilizzare Cost Explorer e AWS Cost and Usage Reports per monitorare i tuoi addebiti. Per ulteriori informazioni, consulta [Esplorazione dei dati utilizzando Cost Explorer](#) e [Cosa sono i report su AWS costi e utilizzo](#).

## Supporto premium

Se ti abboni a qualsiasi livello dei piani di supporto AWS premium, l'assistenza premium si applica ad Amazon Managed Service for Prometheus.

## Nozioni di base

Questa sezione spiega come creare rapidamente aree di lavoro Amazon Managed Service per Prometheus, configurare l'inserimento dei parametri di Prometheus in tali aree di lavoro e interrogare tali parametri.

Include anche informazioni sulla configurazione di un Account AWS, nel caso in cui tu non lo sappia AWS.

### Argomenti

- [Configurazione](#)
- [Creare un'area di lavoro](#)
- [Inserisci i parametri di Prometheus nell'area di lavoro](#)
- [Esegui una ricerca sui parametri Prometheus](#)

## Configurazione

Completa le attività in questa sezione per iniziare la configurazione AWS per la prima volta. Se hai già un AWS account, vai avanti a [Creare un'area di lavoro](#).

Quando ti registri AWS, il tuo AWS account ha automaticamente accesso a tutti i servizi in AWS, incluso Amazon Managed Service for Prometheus. Tuttavia, vengono addebitati solo i servizi che utilizzi.

### Argomenti

- [Registrati per un Account AWS](#)
- [Crea un utente con accesso amministrativo](#)

## Registrati per un Account AWS

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

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.

## 2. Segui le istruzioni online.

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

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso da parte dell'utente root](#).

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo <https://aws.amazon.com/> e selezionando Il mio account.

## Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Signing in as the root user](#) della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta [Abilitare un dispositivo MFA virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

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

### Accedi come utente con accesso amministrativo

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

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

### Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, consulta [Creare un set di autorizzazioni](#) nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente.AWS IAM Identity Center

## Creare un'area di lavoro

Un'area di lavoro è uno spazio logico dedicato all'archiviazione e all'interrogazione dei parametri di Prometheus. Un'area di lavoro supporta un controllo granulare degli accessi per autorizzarne la gestione, ad esempio l'aggiornamento, l'elenco, la descrizione e l'eliminazione, nonché l'inserimento e l'interrogazione dei parametri. Si possono avere una o più aree di lavoro in ogni Regione del tuo account.

Per configurare un'area di lavoro, procedi nel seguente modo.

#### Note

Per informazioni più dettagliate su come creare un'area di lavoro, consulta [Creare un'area di lavoro](#).

Come creare un'area di lavoro Amazon Managed Service per Prometheus.

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Per l'alias Area di lavoro, inserisci un alias per la nuova area di lavoro.

Gli alias dell'area di lavoro sono nomi descrittivi che consentono di identificare le aree di lavoro. I nomi non devono essere univoci. Due aree di lavoro potrebbero avere lo stesso alias, ma tutte le aree di lavoro avranno ID di area di lavoro univoci, generati da Amazon Managed Service per Prometheus.

3. (Facoltativo) Per aggiungere tag al namespace, scegli Aggiungi nuovo tag.

Poi, per Chiave, inserire un nome per il tag. È possibile aggiungere un valore facoltativo al tag in Value (Valore).

Per aggiungere un altro tag, scegli nuovamente Add tag (Aggiungi tag).

4. Scegli Crea area di lavoro.

Viene visualizzata la pagina dei dettagli dell'area di lavoro. Visualizza informazioni tra cui lo stato, l'ARN, l'ID dell'area di lavoro e gli URL degli endpoint per questo spazio di lavoro sia per la scrittura remota che per le domande.

Inizialmente, lo stato è probabilmente IN CREAZIONE. Attendi che lo stato sia ATTIVO prima di passare alla configurazione dell'importazione dei parametri.

Prendi nota degli URL visualizzati per Endpoint - remote write URL e Endpoint - query URL. Ne avrai bisogno quando configurerai il tuo server Prometheus per la scrittura remota di parametri in questa area di lavoro o e quando interroghi tali parametri.

## Inserisci i parametri di Prometheus nell'area di lavoro

Un modo per inserire i parametri consiste nell'utilizzare un agente Prometheus autonomo (un'istanza Prometheus in esecuzione in modalità agente) per importare i parametri dal cluster e inoltrarli al servizio gestito da Amazon per Prometheus per l'archiviazione e il monitoraggio. Questa sezione spiega come configurare l'importazione dei parametri nell'area di lavoro del servizio gestito da Amazon per Prometheus da Amazon EKS configurando una nuova istanza dell'agente Prometheus utilizzando Helm.

Per informazioni su altri modi per inserire dati nel servizio gestito da Amazon per Prometheus, incluso come proteggere i parametri e creare parametri ad alta disponibilità, consulta [Inserisci le metriche nel tuo spazio di lavoro](#).

#### Note

Le metriche inserite in un'area di lavoro vengono archiviate per 150 giorni per impostazione predefinita e vengono quindi eliminate automaticamente. [Questa lunghezza è una quota regolabile](#).

Le istruzioni in questa sezione ti consentono di iniziare rapidamente a utilizzare il servizio gestito da Amazon per Prometheus. Hai configurato un nuovo server Prometheus in un cluster Amazon EKS e il nuovo server utilizza una configurazione predefinita per fungere da agente per inviare i parametri al servizio gestito da Amazon per Prometheus. Questo metodo ha i seguenti prerequisiti:

- È necessario disporre di un cluster Amazon EKS da cui il nuovo server Prometheus raccoglierà i parametri.
- È necessario utilizzare Helm CLI 3.0 o una versione successiva
- È necessario utilizzare un computer Linux o macOS per eseguire i passaggi descritti nelle seguenti sezioni.

## Fase 1: aggiunta di nuovi repository del grafico Helm

Immetti i seguenti comandi per aggiungere il nuovo repository del grafico Helm. Per ulteriori informazioni su questi comandi, consulta [Repository Helm](#).

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
helm repo add kube-state-metrics https://kubernetes.github.io/kube-state-metrics
helm repo update
```

## Fase 2: creazione di un namespace Prometheus.

Immetti il seguente comando per creare un namespace Prometheus per il server Prometheus e altri componenti di monitoraggio. Sostituisci *prometheus-agent-namespace* con il nome che desideri per questo namespace.

```
kubectl create namespace prometheus-agent-namespace
```

### Fase 3: configurazione dei ruoli IAM per gli account del servizio.

Per questo metodo di inserimento, è necessario utilizzare i ruoli IAM per gli account del servizio nel cluster Amazon EKS in cui l'agente Prometheus è in esecuzione.

Grazie ai ruoli IAM per gli account del servizio, è possibile associare un ruolo IAM a un account del servizio Kubernetes. Questo account del servizio può quindi fornire le autorizzazioni AWS ai container in qualsiasi pod che utilizza tale account. Per ulteriori informazioni, consulta [Ruoli IAM per gli account del servizio](#).

Se non hai già impostato questi ruoli, segui le istruzioni riportate in [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS](#), per configurare i ruoli. Le istruzioni contenute in quella sezione richiedono l'uso di `eksctl`. Per ulteriori informazioni, consulta [Nozioni di base su Amazon Elastic Kubernetes Service – eksctl](#).

#### Note

Quando non utilizzi EKS o utilizzi solo la chiave di accesso AWS e la chiave segreta per accedere ad Amazon Managed Service for Prometheus, non puoi usare il SigV4 basato. EKS-IAM-ROLE

### Fase 4: configurazione del nuovo server e avvio dell'importazione dei parametri

Per installare il nuovo agente Prometheus e inviare i parametri alla tua area di lavoro del servizio gestito da Amazon per Prometheus, segui questi passaggi.

Per installare un nuovo agente Prometheus e inviare parametri alla tua area di lavoro del servizio gestito da Amazon per Prometheus

1. Utilizza un editor di testo per creare un file denominato `my_prometheus_values.yaml` con il seguente contenuto.
  - Sostituisci `IAM_PROXY_PROMETHEUS_ROLE_ARN` con l'ARN di `amp-iamproxy-ingest-role` che hai creato in [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS](#).

- Sostituisci *WORKSPACE\_ID* con l'ID della tua area di lavoro del servizio gestito da Amazon per Prometheus.
- Sostituisci *REGION* con la regione della tua area di lavoro del servizio gestito da Amazon per Prometheus.

```
## The following is a set of default values for prometheus server helm chart which
  enable remoteWrite to AMP
## For the rest of prometheus helm chart values see: https://github.com/prometheus-
community/helm-charts/blob/main/charts/prometheus/values.yaml
##
serviceAccounts:
  server:
    name: amp-iamproxy-ingest-service-account
    annotations:
      eks.amazonaws.com/role-arn: ${IAM_PROXY_PROMETHEUS_ROLE_ARN}
server:
  remoteWrite:
    - url: https://aps-workspaces.${REGION}.amazonaws.com/workspaces/
      ${WORKSPACE_ID}/api/v1/remote_write
      sigv4:
        region: ${REGION}
      queue_config:
        max_samples_per_send: 1000
        max_shards: 200
        capacity: 2500
```

## 2. Inserisci il seguente comando per creare il server di Prometheus.

- Sostituisci *prometheus-chart-name* con il nome della versione di Prometheus.
- Sostituisci *prometheus-agent-namespace* con il nome del tuo namespace Prometheus.

```
helm install prometheus-chart-name prometheus-community/prometheus -n prometheus-
agent-namespace \
-f my_prometheus_values.yaml
```

## Esegui una ricerca sui parametri Prometheus

Ora che i parametri vengono inseriti nell'area di lavoro, puoi interrogarli. Un modo comune per interrogare i parametri consiste nell'utilizzare un servizio come Grafana per interrogare i parametri. In questa sezione, imparerai a usare Grafana gestito da Amazon per interrogare i parametri del servizio gestito da Amazon per Prometheus.

### Note

Per ulteriori informazioni su altri modi per interrogare i parametri del servizio gestito da Amazon per Prometheus o utilizzare le API servizio gestito da Amazon per Prometheus, consulta [Esegui una ricerca sui parametri Prometheus](#).

Le interrogazioni vengono eseguite utilizzando Prometheus, il linguaggio di interrogazione standard di Prometheus, PromQL. Per ulteriori informazioni su PromQL e sulla sua sintassi, consulta [Interrogazione a Prometheus](#) nella documentazione di Prometheus.

Amazon Managed Grafana è un servizio completamente gestito per Grafana open source che semplifica la connessione a ISV open source di terze parti AWS e servizi per la visualizzazione e l'analisi delle fonti di dati su larga scala.

Il servizio gestito da Amazon per Prometheus supporta l'utilizzo di Grafana gestito da Amazon per interrogare i parametri in un'area di lavoro. Nella console Grafana gestito da Amazon, puoi aggiungere un'area di lavoro del servizio gestito da Amazon per Prometheus come origine dati scoprendo i tuoi account del servizio gestito da Amazon per Prometheus esistenti. Grafana gestito da Amazon gestisce la configurazione delle credenziali di autenticazione necessarie per accedere al servizio gestito da Amazon per Prometheus. Per istruzioni dettagliate sulla creazione di una connessione al servizio gestito da Amazon per Prometheus da Grafana gestito da Amazon, consulta le istruzioni nella [Guida per l'utente di Grafana gestito da Amazon](#).

Puoi inoltre visualizzare gli avvisi del servizio gestito da Amazon per Prometheus in Grafana gestito da Amazon. Per istruzioni su come configurare l'integrazione con gli avvisi, consulta [Integrazione degli avvisi con Amazon Managed Grafana o Grafana open source](#).

### Note

Se hai configurato la tua area di lavoro Grafana gestito da Amazon per utilizzare un VPC privato, devi connettere l'area di lavoro del servizio gestito da Amazon per Prometheus allo

stesso VPC. Per ulteriori informazioni, consulta [Connessione ad Grafana gestito da Amazon in un VPC privato](#).

# Gestione delle aree di lavoro

Un'area di lavoro è uno spazio logico dedicato all'archiviazione e all'interrogazione dei parametri di Prometheus. Un'area di lavoro supporta un controllo granulare degli accessi per autorizzarne la gestione, ad esempio l'aggiornamento, l'elenco, la descrizione e l'eliminazione, nonché l'inserimento e l'interrogazione dei parametri. Si possono avere una o più aree di lavoro in ogni Regione del tuo account.

Utilizza le procedure descritte in questa sezione per creare e gestire le aree di lavoro del servizio gestito da Amazon per Prometheus.

## Argomenti

- [Creare un'area di lavoro](#)
- [Modificare un'area di lavoro](#)
- [Trova il tuo spazio di lavoro ARN](#)
- [Eliminazione di un'area di lavoro.](#)

## Creare un'area di lavoro

Segui questi passaggi per creare un'area di lavoro del servizio gestito da Amazon per Prometheus. Puoi scegliere di utilizzare la console AWS CLI Amazon Managed Service for Prometheus.

### Note

Se utilizzi un cluster Amazon EKS, puoi anche creare un nuovo spazio di lavoro utilizzando [AWS Controllers for Kubernetes](#).

Per creare uno spazio di lavoro utilizzando il AWS CLI

1. Inserisci il seguente comando per creare l'area di lavoro. Questo esempio crea un'area di lavoro denominata `my-first-workspace`, ma puoi scegliere di utilizzare un alias diverso. Gli alias dell'area di lavoro sono nomi descrittivi che consentono di identificare le aree di lavoro. I nomi non devono essere univoci. Due aree di lavoro possono avere lo stesso alias, ma tutte le aree di lavoro hanno ID di area di lavoro univoci, generati da Amazon Managed Service per Prometheus.

(Facoltativo) Per utilizzare la propria chiave KMS per crittografare i dati archiviati nell'area di lavoro, è possibile includere il `kmsKeyArn` parametro nella chiave da utilizzare. AWS KMS. Sebbene Amazon Managed Service for Prometheus non addebiti alcun costo per l'utilizzo di chiavi gestite dai clienti, potrebbero esserci dei costi associati alle chiavi di AWS Key Management Service. Per ulteriori informazioni sulla crittografia dei dati nell'area di lavoro di Amazon Managed Service for Prometheus o su come creare, gestire e utilizzare la propria chiave gestita dal cliente, consulta [Crittografia a riposo](#).

I parametri tra parentesi ([ ]) sono facoltativi, non includono le parentesi nel comando.

```
aws amp create-workspace [--alias my-first-workspace] [--kmsKeyArn arn:aws:aps:us-west-2:111122223333:workspace/ws-sample-1234-abcd-56ef-7890abcd12ef] [--tags Status=Secret,Team=My-Team]
```

Questo comando restituisce i seguenti dati:

- `workspaceId` è l'ID univoco di quest'area di lavoro. Prendi nota di questo ID.
- `arn` è l'ARN per questa area di lavoro.
- `status` è lo stato corrente dell'area di lavoro. Immediatamente dopo aver creato l'area di lavoro, probabilmente sarà `CREATING`.
- `kmsKeyArn` è la chiave gestita dal cliente utilizzata per crittografare i dati dell'area di lavoro, se fornita.

#### Note

Le aree di lavoro create con chiavi gestite dal cliente non possono utilizzare [raccoglitori gestiti AWS](#) per l'importazione.

Scegli se utilizzare con attenzione le chiavi gestite dal cliente o le chiavi AWS di proprietà. Le aree di lavoro create con chiavi gestite dal cliente non possono essere convertite per utilizzare chiavi AWS di proprietà in un secondo momento (e viceversa).

- `tags` elenca gli eventuali tag dell'area di lavoro.
2. Se il `create-workspace` comando restituisce uno stato di `CREATING`, è possibile immettere il comando seguente per determinare quando l'area di lavoro è pronta. Sostituisci `my-workspace-id` con il valore restituito dal `create-workspace` comando. `workspaceId`

```
aws amp describe-workspace --workspace-id my-workspace-id
```

Quando il `describe-workspace` comando ritorna `ACTIVE` per `status`, l'area di lavoro è pronta per l'uso.

Creare un'area di lavoro utilizzando la console del servizio gestito da Amazon per Prometheus

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Scegli Crea.
3. Per l'alias Area di lavoro, inserisci un alias per la nuova area di lavoro.

Gli alias dell'area di lavoro sono nomi descrittivi che consentono di identificare le aree di lavoro. I nomi non devono essere univoci. Due aree di lavoro possono avere lo stesso alias, ma tutte le aree di lavoro hanno ID di area di lavoro univoci, generati da Amazon Managed Service per Prometheus.

4. (Facoltativo) Per utilizzare la propria chiave KMS per crittografare i dati archiviati nell'area di lavoro, è possibile selezionare Personalizza le impostazioni di crittografia e scegliere la AWS KMS chiave da utilizzare (o crearne una nuova). Puoi scegliere una chiave nel tuo account dall'elenco a discesa o inserire l'ARN per qualsiasi chiave a cui hai accesso. Sebbene Amazon Managed Service for Prometheus non addebiti alcun costo per l'utilizzo di chiavi gestite dai clienti, potrebbero esserci dei costi associati alle chiavi di AWS Key Management Service

Per ulteriori informazioni sulla crittografia dei dati nell'area di lavoro di Amazon Managed Service for Prometheus o su come creare, gestire e utilizzare la propria chiave gestita dal cliente, consulta [Crittografia a riposo](#).

#### Note

Le aree di lavoro create con chiavi gestite dal cliente non possono utilizzare [raccoglitori gestiti AWS](#) per l'importazione.

Scegli se utilizzare con attenzione le chiavi gestite dal cliente o le chiavi AWS di proprietà. Le aree di lavoro create con chiavi gestite dal cliente non possono essere convertite per utilizzare chiavi AWS di proprietà in un secondo momento (e viceversa).

5. (Facoltativo) Per aggiungere uno o più tag all'area di lavoro, scegli Aggiungi nuovo tag. Poi, per Chiave, inserisci un nome per il tag. È possibile aggiungere un valore facoltativo al tag in Value (Valore).

Per aggiungere un altro tag, scegli nuovamente Add tag (Aggiungi tag).

6. Scegli Crea area di lavoro.

Viene visualizzata la pagina dei dettagli dell'area di lavoro. Visualizza informazioni tra cui lo stato, l'ARN, l'ID dell'area di lavoro e gli URL degli endpoint per questo spazio di lavoro sia per la scrittura remota che per le domande.

Lo stato restituisce CREATING finché l'area di lavoro non è pronta. Attendi che lo stato sia ATTIVO prima di passare alla configurazione dell'importazione dei parametri.

Prendi nota degli URL visualizzati per Endpoint - remote write URL e Endpoint - query URL. Ne avrai bisogno quando configurerai il tuo server Prometheus per la scrittura remota di parametri in questa area di lavoro o e quando interroghi tali parametri.

Per informazioni su come inserire i parametri nell'area di lavoro, consulta [Inserisci i parametri di Prometheus nell'area di lavoro](#).

## Modificare un'area di lavoro

Puoi modificare un'area di lavoro per cambiarne l'alias. Per modificare l'alias dell'area di lavoro utilizzando il AWS CLI, inserisci il comando seguente:

```
aws amp update-workspace-alias --workspace-id my-workspace-id --alias "new-alias"
```

Per modificare un'area di lavoro utilizzando la console del servizio gestito da Amazon per Prometheus

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nell'angolo in alto a sinistra della pagina, scegli l'icona del menu, quindi scegli Tutte le aree di lavoro.
3. Scegli l'ID dell'area di lavoro che desideri modificare, quindi seleziona Modifica.
4. Inserisci un nuovo alias per l'area di lavoro, quindi scegli Salva.

## Trova il tuo spazio di lavoro ARN

Puoi trovare l'ARN del tuo workspace del servizio gestito da Amazon per Prometheus utilizzando la console o AWS CLI.

Per trovare l'ARN del tuo workspace utilizzando la console del servizio gestito da Amazon per Prometheus

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nell'angolo in alto a sinistra della pagina, scegli l'icona del menu, quindi scegli Tutte le aree di lavoro.
3. Scegli l'ID dell'area di lavoro.

L'ARN dell'area di lavoro viene visualizzato in ARN.

Per utilizzare l'ARN AWS CLI per trovare il tuo spazio di lavoro, inserisci il seguente comando.

```
aws amp describe-workspace --workspace-id my-workspace-id
```

Trova il valore `arn` nella risposta.

## Eliminazione di un'area di lavoro.

L'eliminazione di un'area di lavoro comporta l'eliminazione dei dati che vi sono stati inseriti.

### Note

L'eliminazione di un'area di lavoro di Amazon Managed Service for Prometheus non elimina automaticamente i raccoglitori gestiti che raccolgono le metriche e AWS le inviano all'area di lavoro. Per ulteriori informazioni, consulta [Trova ed elimina gli scraper](#).

Per eliminare un'area di lavoro utilizzando il AWS CLI

Utilizza il seguente comando:

```
aws amp delete-workspace --workspace-id my-workspace-id
```

Per eliminare un'area di lavoro utilizzando la console del servizio gestito da Amazon per Prometheus

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nell'angolo in alto a sinistra della pagina, scegli l'icona del menu, quindi scegli Tutte le aree di lavoro.
3. Scegli l'ID dell'area di lavoro che desideri eliminare, quindi seleziona Elimina.
4. Inserisci **delete** nel campo di conferma, quindi seleziona Elimina.

# Inserisci le metriche nel tuo spazio di lavoro

Le metriche devono essere inserite nell'area di lavoro di Amazon Managed Service for Prometheus prima di poter eseguire query o inviare avvisi su tali metriche. In questa sezione viene illustrato come configurare l'acquisizione di parametri nella tua area di lavoro.

## Note

Le metriche inserite in un'area di lavoro vengono archiviate per 150 giorni per impostazione predefinita e vengono quindi eliminate automaticamente. [Questa lunghezza è controllata da una quota regolabile.](#)

Esistono due metodi per inserire i parametri nell'area di lavoro del servizio gestito da Amazon per Prometheus.

- Utilizzando un collettore AWS gestito: Amazon Managed Service for Prometheus fornisce uno scraper completamente gestito e senza agenti per acquisire automaticamente i parametri dai cluster Amazon Elastic Kubernetes Service (Amazon EKS). Lo scraper estrae automaticamente i parametri dagli endpoint compatibili con Prometheus.
- Utilizzo di un raccoglitore gestito dal cliente: hai molte opzioni per gestire il tuo raccoglitore. Due dei raccoglitori più comuni da utilizzare sono l'installazione della propria istanza di Prometheus, l'esecuzione in modalità agente o l'utilizzo di Distro for AWS OpenTelemetry. Questi sono descritti in dettaglio nella sezione seguente.

I raccoglitori inviano i parametri al servizio gestito da Amazon per Prometheus utilizzando la funzionalità di scrittura remota Prometheus. Puoi inviare parametri direttamente al servizio gestito da Amazon per Prometheus utilizzando la scrittura remota di Prometheus nella tua applicazione. Per maggiori dettagli sull'utilizzo diretto delle configurazioni di scrittura remota e scrittura remota, vedere [remote\\_write](#) nella documentazione di Prometheus.

## Argomenti

- [AWS collezionisti gestiti](#)
- [Raccoglitori gestiti dal cliente](#)

## AWS collezionisti gestiti

Un caso d'uso comune del servizio gestito da Amazon per Prometheus è il monitoraggio dei cluster Kubernetes gestiti da Amazon Elastic Kubernetes Service (Amazon EKS). I cluster Kubernetes e molte applicazioni eseguite all'interno di Amazon EKS esportano automaticamente i propri parametri per consentire l'accesso agli scraper compatibili con Prometheus.

### Note

Molte tecnologie e applicazioni eseguite in ambienti Kubernetes forniscono parametri compatibili con Prometheus. Per un elenco completo degli esportatori disponibili, consulta [Esportatori e integrazioni](#) nella documentazione Prometheus.

Il servizio gestito da Amazon per Prometheus fornisce uno scraper o raccogliitore completamente gestito e senza agenti, che rileva e recupera automaticamente i parametri compatibili con Prometheus. Non è necessario gestire, installare, applicare patch o eseguire la manutenzione di agenti o scraper. Un raccogliitore del servizio gestito da Amazon per Prometheus fornisce una raccolta di parametri affidabile, stabile, ad alta disponibilità e scalata automaticamente per il tuo cluster Amazon EKS. I raccoglitori gestiti di Amazon Managed Service for Prometheus funzionano con i cluster Amazon EKS, inclusi EC2 e Fargate.

Un collettore Amazon Managed Service for Prometheus crea un'interfaccia di rete elastica (ENI) per sottorete specificata durante la creazione dello scraper. Il raccogliitore analizza i parametri attraverso questi ENI e utilizza `remote_write` per inviare i dati al tuo spazio di lavoro Amazon Managed Service for Prometheus utilizzando un endpoint VPC. Questi dati non viaggiano mai nell'internet pubblico.

I seguenti argomenti forniscono ulteriori informazioni su come utilizzare un raccogliitore del servizio gestito da Amazon per Prometheus nel cluster Amazon EKS e sui parametri raccolti.

### Argomenti

- [AWS Utilizzo di un raccogliitore gestito](#)
- [Quali sono i parametri compatibili con Prometheus?](#)

## AWS Utilizzo di un raccogliatore gestito

Per utilizzare un raccogliatore del servizio gestito da Amazon per Prometheus, devi creare uno scraper che rilevi e recuperi i parametri nel tuo cluster Amazon EKS.

- Puoi creare uno scraper come parte della creazione del cluster Amazon EKS. Per ulteriori informazioni sulla creazione di un cluster Amazon EKS, inclusa la creazione di uno scraper, consulta [Creazione di un cluster Amazon EKS](#) nella Guida per l'utente di Amazon EKS.
- Puoi creare il tuo scraper, a livello di codice con l' AWS API o utilizzando il. AWS CLI

### Note

Le aree di lavoro Amazon Managed Service for Prometheus create [con chiavi gestite dal cliente non possono utilizzare raccoglitori gestiti](#) per l'ingestione. AWS

Un raccogliatore del servizio gestito da Amazon per Prometheus analizza parametri compatibili con Prometheus. Per ulteriori informazioni sui parametri compatibili con Prometheus, consulta [Quali sono i parametri compatibili con Prometheus?](#)

I seguenti argomenti descrivono come creare, gestire e configurare scraper.

### Argomenti

- [Creare uno scraper](#)
- [Configurazione del cluster Amazon EKS](#)
- [Trova ed elimina gli scraper](#)
- [Configurazione dello scraper](#)
- [Risoluzione degli errori di configurazione dello scrape](#)
- [Limitazioni dello scraper](#)

## Creare uno scraper

Un raccogliatore del servizio gestito da Amazon per Prometheus è costituito da uno scraper che rileva e raccoglie i parametri da un cluster Amazon EKS. Il servizio gestito da Amazon per Prometheus gestisce lo scraper per te, offrendoti la scalabilità, la sicurezza e l'affidabilità di cui hai bisogno, senza dover gestire personalmente istanze, agenti o scraper.

Uno scraper viene creato automaticamente per te quando crei [un cluster Amazon EKS tramite la console Amazon EKS](#). Tuttavia, in alcune situazioni potresti voler creare uno scraper da solo. Ad esempio, se desideri aggiungere un raccoglitore AWS gestito a un cluster Amazon EKS esistente o se desideri modificare la configurazione di un raccoglitore esistente.

Puoi creare uno scraper utilizzando l' AWS API o il. AWS CLI

Esistono alcuni prerequisiti per creare il proprio scraper:

- Devi avere un cluster Amazon EKS.
- Il tuo cluster Amazon EKS deve avere il [controllo degli accessi agli endpoint del cluster](#) impostato per includere l'accesso privato. Può includere aree private e pubbliche, ma deve includere quelle private.

#### Note

Il cluster verrà associato allo scraper tramite il relativo nome di risorsa Amazon (ARN). Se elimini un cluster e poi ne crei uno nuovo con lo stesso nome, l'ARN verrà riutilizzato per il nuovo cluster. Per questo motivo, lo scraper tenterà di raccogliere le metriche per il nuovo cluster. [Gli scraper vengono eliminati](#) separatamente dall'eliminazione del cluster.

## AWS API

Per creare uno scraper utilizzando l'API AWS

Utilizza l'operazione `CreateScraper` API per creare uno scraper con l' AWS API. Nell'esempio seguente viene creato uno scraper nella `us-west-2` regione. Devi sostituire le informazioni relative all'area di lavoro Account AWS, alla sicurezza e al cluster Amazon EKS con i tuoi ID e fornire la configurazione da utilizzare per il tuo scraper.

#### Note

Devi includere minimo due sottoreti in almeno due zone disponibili.

`scrapeConfiguration` è un file YAML di configurazione Prometheus con codifica base64. È possibile scaricare una configurazione generica con l'operazione API

GetDefaultScraperConfiguration. Per ulteriori informazioni sul formato `discrepeConfiguration`, consulta [Configurazione dello scraper](#)

```
POST /scrapers HTTP/1.1
Content-Length: 415
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: aws-cli/1.18.147 Python/2.7.18 Linux/5.4.58-37.125.amzn2int.x86_64
botocore/1.18.6

{
  "alias": "myScraper",
  "destination": {
    "ampConfiguration": {
      "workspaceArn": "arn:aws:aps:us-west-2:account-id:workspace/
ws-workspace-id"
    }
  },
  "source": {
    "eksConfiguration": {
      "clusterArn": "arn:aws:eks:us-west-2:account-id:cluster/cluster-name",
      "securityGroupIds": ["sg-security-group-id"],
      "subnetIds": ["subnet-subnet-id-1", "subnet-subnet-id-2"]
    }
  },
  "scrapeConfiguration": {
    "configurationBlob": <base64-encoded-blob>
  }
}
```

## AWS CLI

Per creare un raschietto utilizzando il AWS CLI

Utilizzate il `create-scraper` comando per creare un raschietto con AWS CLI. Nell'esempio seguente viene creato uno scraper nella `us-west-2` regione. Devi sostituire le informazioni relative all'area di lavoro Account AWS, alla sicurezza e al cluster Amazon EKS con i tuoi ID e fornire la configurazione da utilizzare per il tuo scraper.

### Note

Devi includere minimo due sottoreti in almeno due zone disponibili.

scrape-configuration è un file YAML di configurazione Prometheus con codifica base64. È possibile scaricare una configurazione generica con il `get-default-scrape-configuration` comando. Per ulteriori informazioni sul formato `discraper-configuration`, vedere [Configurazione dello scraper](#).

```
aws amp create-scrape \
  --source eksConfiguration="{clusterArn='arn:aws:eks:us-west-2:account-
id:cluster/cluster-name', securityGroupIds=['sg-security-group-
id'], subnetIds=['subnet-subnet-id-1', 'subnet-subnet-id-2']}" \
  --scrape-configuration configurationBlob=<base64-encoded-blob> \
  --destination ampConfiguration="{workspaceArn='arn:aws:aps:us-west-2:account-
id:workspace/ws-workspace-id'}"
```

Di seguito è riportato un elenco completo delle operazioni dello scraper che è possibile utilizzare con l'AWS API:

- Crea uno scraper con l'operazione [CreateScraperAPI](#).
- Elenca i tuoi scraper esistenti con l'operazione [ListScrapersAPI](#).
- Elimina uno scraper con l'operazione [DeleteScraperAPI](#).
- Ottieni maggiori dettagli su uno scraper con l'operazione [DescribeScraperAPI](#).
- Ottieni una configurazione generica per gli scraper con l'operazione [GetDefaultScraperConfigurationAPI](#).

#### Note

Il cluster Amazon EKS di cui stai effettuando lo scraping deve essere configurato per consentire al servizio gestito da Amazon per Prometheus di accedere ai parametri. Nell'argomento successivo viene descritto come configurare il cluster.

## Errori comuni durante la creazione di raschietti

Di seguito sono riportati i problemi più comuni che si verificano quando si tenta di creare un nuovo scraper.

- AWS Le risorse richieste non esistono. Il gruppo di sicurezza, la sottorete e il cluster Amazon EKS specificati devono esistere.

- Spazio per indirizzi IP insufficiente. È necessario disporre di almeno un indirizzo IP in ogni sottorete che si passa all'CreateScrapeAPI.

## Configurazione del cluster Amazon EKS

Il cluster Amazon EKS deve essere configurato per consentire allo scraper di accedere ai parametri. Esistono due opzioni per questa configurazione:

- Utilizza le voci di accesso di Amazon EKS per fornire automaticamente ai collezionisti Amazon Managed Service for Prometheus l'accesso al tuo cluster.
- Configura manualmente il tuo cluster Amazon EKS per lo scraping dei parametri gestito.

I seguenti argomenti descrivono ciascuno di questi aspetti in modo più dettagliato.

### Configura Amazon EKS per l'accesso allo scraper con voci di accesso

L'utilizzo delle voci di accesso per Amazon EKS è il modo più semplice per consentire ad Amazon Managed Service for Prometheus di accedere alle metriche del cluster.

Il cluster Amazon EKS di cui stai effettuando lo scraping deve essere configurato per consentire l'autenticazione tramite API. La modalità di autenticazione del cluster deve essere impostata su `API` o `API_AND_CONFIG_MAP`. È visualizzabile nella console Amazon EKS nella scheda di configurazione dell'accesso dei dettagli del cluster. Per ulteriori informazioni, consulta [Consentire ai ruoli o agli utenti IAM di accedere all'oggetto Kubernetes sul tuo cluster Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

Puoi creare lo scraper durante la creazione del cluster o dopo averlo creato:

- Quando crei un cluster: puoi configurare questo accesso quando [crei un cluster Amazon EKS tramite la console Amazon EKS](#) (segui le istruzioni per creare uno scraper come parte del cluster) e verrà creata automaticamente una politica di accesso che consente ad Amazon Managed Service for Prometheus di accedere ai parametri del cluster.
- Aggiunta dopo la creazione di un cluster: se il tuo cluster Amazon EKS esiste già, imposta la modalità di autenticazione su `API` o `API_AND_CONFIG_MAP` e tutti gli scraper creati [tramite l'API o la CLI di Amazon Managed Service for Prometheus](#) avranno automaticamente la politica di accesso corretta creata per te e gli scraper avranno accesso al tuo cluster.

### Politica di accesso creata

Quando crei uno scraper e lasci che Amazon Managed Service for Prometheus generi una politica di accesso per te, genera la seguente politica. Per ulteriori informazioni sulle voci di accesso, consulta [Consentire ai ruoli o agli utenti IAM di accedere a Kubernetes](#) nella Amazon EKS User Guide.

```
{
  "rules": [
    {
      "effect": "allow",
      "apiGroups": [
        ""
      ],
      "resources": [
        "nodes",
        "nodes/proxy",
        "nodes/metrics",
        "services",
        "endpoints",
        "pods",
        "ingresses",
        "configmaps"
      ],
      "verbs": [
        "get",
        "list",
        "watch"
      ]
    },
    {
      "effect": "allow",
      "apiGroups": [
        "extensions",
        "networking.k8s.io"
      ],
      "resources": [
        "ingresses/status",
        "ingresses"
      ],
      "verbs": [
        "get",
        "list",
        "watch"
      ]
    }
  ],
}
```

```
{
  "effect": "allow",
  "nonResourceURLs": [
    "/metrics"
  ],
  "verbs": [
    "get"
  ]
}
```

## Configurazione manuale di Amazon EKS per l'accesso allo scraper

Se preferisci utilizzare l'opzione per controllare l'accesso `aws-auth` ConfigMap al tuo cluster Kubernetes, puoi comunque consentire agli scraper di Amazon Managed Service for Prometheus di accedere alle tue metriche. I seguenti passaggi consentiranno ad Amazon Managed Service for Prometheus di accedere alle metriche di scrape dal tuo cluster Amazon EKS.

### Note

Per ulteriori informazioni ConfigMap e per accedere alle voci, consulta [Consentire ai ruoli o agli utenti IAM di accedere a Kubernetes](#) nella Amazon EKS User Guide.

Questa procedura utilizza `kubectl` e la AWS CLI. Per informazioni sull'installazione di `kubectl`, consulta [Installazione di kubectl](#) nella Guida per l'utente di Amazon EKS.

Per configurare manualmente il cluster Amazon EKS per lo scraping dei parametri gestito

1. Crea un file denominato `clusterrole-binding.yml` con il testo seguente:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: aps-collector-role
rules:
  - apiGroups: [""]
    resources: ["nodes", "nodes/proxy", "nodes/metrics", "services", "endpoints",
      "pods", "ingresses", "configmaps"]
    verbs: ["describe", "get", "list", "watch"]
```

```

- apiGroups: ["extensions", "networking.k8s.io"]
  resources: ["ingresses/status", "ingresses"]
  verbs: ["describe", "get", "list", "watch"]
- nonResourceURLs: ["/metrics"]
  verbs: ["get"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: aps-collector-user-role-binding
subjects:
- kind: User
  name: aps-collector-user
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: aps-collector-role
  apiGroup: rbac.authorization.k8s.io

```

2. Esegui il comando seguente nel tuo cluster.

```
kubectl apply -f clusterrole-binding.yml
```

Ciò creerà l'associazione e la regola del ruolo del cluster. Questo esempio utilizza `aps-collector-role` come nome del ruolo e `aps-collector-user` come nome utente.

3. Il comando seguente fornisce informazioni sullo scraper con l'ID *scraper-id*. Questo è lo scraper creato utilizzando il comando nella sezione precedente.

```
aws amp describe-scraper --scraper-id scraper-id
```

4. Dai risultati di `describe-scraper`, trova il file `roleArn`, che avrà il seguente formato:

```
arn:aws:iam::account-id:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper_unique-id
```

Amazon EKS richiede un formato diverso per questo ARN. È necessario modificare il formato dell'ARN restituito da utilizzare nel passaggio successivo. Modificalo in modo che corrisponda a questo formato:

```
arn:aws:iam::account-id:role/AWSServiceRoleForAmazonPrometheusScraper_unique-id
```

Per esempio, questo ARN:

```
arn:aws:iam::111122223333:role/aws-service-role/scrapper.aps.amazonaws.com/  
AWSServiceRoleForAmazonPrometheusScrapper_1234abcd-56ef-7
```

Deve essere riscritto come:

```
arn:aws:iam::111122223333:role/  
AWSServiceRoleForAmazonPrometheusScrapper_1234abcd-56ef-7
```

5. Esegui il comando seguente nel cluster, utilizzando `roleArn` modificato dal passaggio precedente, oltre al nome e alla regione del cluster.

```
eksctl create iamidentitymapping --cluster cluster-name --region region-id --  
arn roleArn --username aps-collector-user
```

Ciò consente allo scraper di accedere al cluster utilizzando il ruolo e l'utente creati nel `clusterrole-binding.yml` file.

## Trova ed elimina gli scraper

Puoi utilizzare l' AWS API o AWS CLI per elencare gli scraper presenti nel tuo account o eliminarli.

### Note

Assicurati di utilizzare la versione più recente di AWS CLI o SDK. La versione più recente offre le caratteristiche e le funzionalità più recenti, oltre agli aggiornamenti di sicurezza. In alternativa, usa [AWS Cloudshell](#), che fornisce un'esperienza sempre a riga di up-to-date comando, automaticamente.

Per elencare tutti gli scraper del tuo account, utilizza l'[ListScrapers](#) operazione API.

In alternativa, con AWS CLI, chiama:

```
aws amp list-scrapers
```

`ListScrapers` restituisce tutti gli scraper del tuo account, ad esempio:

```

{
  "scrapers": [
    {
      "scrapersId": "s-1234abcd-56ef-7890-abcd-1234ef567890",
      "arn": "arn:aws:aps:us-west-2:123456789012:scraper/s-1234abcd-56ef-7890-
abcd-1234ef567890",
      "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
AWSServiceRoleForAmazonPrometheusScraper_1234abcd-2931",
      "status": {
        "statusCode": "DELETING"
      },
      "createdAt": "2023-10-12T15:22:19.014000-07:00",
      "lastModifiedAt": "2023-10-12T15:55:43.487000-07:00",
      "tags": {},
      "source": {
        "eksConfiguration": {
          "clusterArn": "arn:aws:eks:us-west-2:123456789012:cluster/my-
cluster",
          "securityGroupIds": [
            "sg-1234abcd5678ef90"
          ],
          "subnetIds": [
            "subnet-abcd1234ef567890",
            "subnet-1234abcd5678ab90"
          ]
        },
        "destination": {
          "ampConfiguration": {
            "workspaceArn": "arn:aws:aps:us-west-2:123456789012:workspace/
ws-1234abcd-5678-ef90-ab12-cdef3456a78"
          }
        }
      }
    }
  ]
}

```

Per eliminare un raschietto, individuate quello relativo allo scraper che desiderate eliminare, utilizzando l'`ListScrapers` operazione, quindi utilizzate l'[DeleteScraper](#) operazione per eliminarlo. `scrapersId`

In alternativa, con AWS CLI, chiama:

```
aws amp delete-scraper --scraper-id scraperId
```

## Configurazione dello scraper

Puoi controllare il modo in cui il tuo scraper rileva e raccoglie i parametri con una configurazione dello scraper compatibile con Prometheus. Ad esempio, puoi modificare l'intervallo di invio dei parametri all'area di lavoro. Puoi anche utilizzare la rietichettatura per riscrivere dinamicamente le etichette di un parametro. La configurazione dello scraper è un file YAML che fa parte della definizione dello scraper.

Quando viene creato un nuovo scraper, si specifica una configurazione fornendo un file YAML con codifica base64 nella chiamata API. Puoi scaricare un file di configurazione generico con l'GetDefaultScraperConfigurationoperazione nell'API del servizio gestito da Amazon per Prometheus.

Per modificare la configurazione di uno scraper, elimina lo scraper e ricrealo con la nuova configurazione.

### Configurazione supportata

Per informazioni sul formato di configurazione dello scraper, inclusa una suddivisione dettagliata dei valori possibili, vedere [Configurazione](#) nella documentazione di Prometheus. Le opzioni e le opzioni di configurazione globali descrivono le <scrape\_config> opzioni più comunemente necessarie.

Poiché Amazon EKS è l'unico servizio supportato, l'unico servizio di discovery config (<\*\_sd\_config>) supportato è il <kubernetes\_sd\_config>.

L'elenco completo delle sezioni di configurazione consentite:

- <global>
- <scrape\_config>
- <static\_config>
- <relabel\_config>
- <metric\_relabel\_configs>
- <kubernetes\_sd\_config>

Le limitazioni all'interno di queste sezioni sono elencate dopo il file di configurazione di esempio.

### Esempio di configurazione di un file

Di seguito è riportato un esempio di file di configurazione YAML con un intervallo di scraping di 30 secondi.

```
global:
  scrape_interval: 30s
  external_labels:
    clusterArn: apiserver-test-2
scrape_configs:
  - job_name: pod_exporter
    kubernetes_sd_configs:
      - role: pod
  - job_name: cadvisor
    scheme: https
    authorization:
      type: Bearer
      credentials_file: /var/run/secrets/kubernetes.io/serviceaccount/token
    kubernetes_sd_configs:
      - role: node
    relabel_configs:
      - action: labelmap
        regex: __meta_kubernetes_node_label_(.+)
      - replacement: kubernetes.default.svc:443
        target_label: __address__
      - source_labels: [__meta_kubernetes_node_name]
        regex: (.+)
        target_label: __metrics_path__
        replacement: /api/v1/nodes/$1/proxy/metrics/cadvisor
# apiserver metrics
- scheme: https
  authorization:
    type: Bearer
    credentials_file: /var/run/secrets/kubernetes.io/serviceaccount/token
  job_name: kubernetes-apiservers
  kubernetes_sd_configs:
    - role: endpoints
  relabel_configs:
    - action: keep
      regex: default;kubernetes;https
      source_labels:
        - __meta_kubernetes_namespace
        - __meta_kubernetes_service_name
        - __meta_kubernetes_endpoint_port_name
# kube proxy metrics
```

```
- job_name: kube-proxy
  honor_labels: true
  kubernetes_sd_configs:
  - role: pod
  relabel_configs:
  - action: keep
    source_labels:
    - __meta_kubernetes_namespace
    - __meta_kubernetes_pod_name
    separator: '/'
    regex: 'kube-system/kube-proxy.+'
```

```
- source_labels:
  - __address__
  action: replace
  target_label: __address__
  regex: (.+?)(\\:\\d+)?
  replacement: $1:10249
```

Di seguito sono riportate le limitazioni specifiche dei raccoglitori AWS gestiti:

- Intervallo di scrape: la configurazione dello scraper non può specificare un intervallo inferiore a 30 secondi.
- Destinazioni: le destinazioni in `static_config` devono essere specificate come indirizzi IP.
- Autorizzazione: ometti se non è necessaria alcuna autorizzazione. Se è necessaria, l'autorizzazione deve essere Bearer e deve puntare al file `/var/run/secrets/kubernetes.io/serviceaccount/token`. In altre parole, se utilizzata, la sezione di autorizzazione deve avere il seguente aspetto:

```
authorization:
  type: Bearer
  credentials_file: /var/run/secrets/kubernetes.io/serviceaccount/token
```

#### Note

`type: Bearer` è l'impostazione predefinita, quindi può essere omessa.

## Risoluzione degli errori di configurazione dello scrape

I raccoglitori del servizio gestito da Amazon per Prometheus rilevano e raccolgono automaticamente i parametri. Ma come puoi risolvere i problemi quando non vedi un parametro che ti aspetti di vedere nella tua area di lavoro del servizio gestito da Amazon per Prometheus?

Il `up` parametro è uno strumento utile. Per ogni endpoint rilevato da un raccoglitore del servizio gestito da Amazon per Prometheus, questo parametro viene automaticamente modificato. Esistono tre stati di questo parametro che possono aiutarti a risolvere ciò che accade all'interno del raccoglitore.

- `up` non è presente: se non è presente alcun `up` parametro per un endpoint, significa che il raccoglitore non è riuscito a trovare l'endpoint.

Se sei sicuro che l'endpoint esista, probabilmente dovrai modificare la configurazione dello scrape. `relabel_config` Potrebbe essere necessario modificare il rilevamento oppure è possibile che vi sia un problema con l'oggetto `role` utilizzato per il rilevamento.

- `up` è presente, ma è sempre 0: se `up` è presente ma è 0, il raccoglitore è in grado di scoprire l'endpoint, ma non riesce a trovare alcun parametro compatibile con Prometheus.

In questo caso, si può provare a utilizzare un `curl` comando direttamente sull'endpoint. È possibile verificare che i dettagli siano corretti, ad esempio il protocollo (`http`/`https`), l'endpoint o la porta che si sta utilizzando. Puoi anche verificare che l'endpoint risponda con una `200` risposta valida e segua il formato Prometheus. Infine, il corpo della risposta non può essere più grande della dimensione massima consentita. (Per i limiti relativi ai raccoglitori AWS gestiti, consultate la sezione seguente).

- `up` è presente e maggiore di 0: se `up` è presente ed è maggiore di 0, i parametri vengono inviati al servizio gestito da Amazon per Prometheus.

Verifica che stai cercando i parametri corretti nel servizio gestito da Amazon per Prometheus (o nella tua dashboard alternativa, come Grafana gestito da Amazon). Puoi utilizzare nuovamente `curl` per verificare i dati previsti nel tuo endpoint `/metrics`. Verifica anche di non aver superato altri limiti, come il numero di endpoint per scraper. Puoi controllare il numero di endpoint delle metriche che vengono analizzate controllando il conteggio delle `up` metriche, utilizzando `count(up)`

## Limitazioni dello scraper

Esistono alcune limitazioni agli scraper completamente gestiti forniti da Amazon Managed Service per Prometheus.

- **Regione:** il cluster EKS, lo scraper gestito e l'area di lavoro del servizio gestito da Amazon per Prometheus devono trovarsi tutti nella stessa AWS regione.
- **Account:** il cluster EKS, lo scraper gestito e l'area di lavoro del servizio gestito da Amazon per Prometheus devono trovarsi tutti nello stesso Account AWS.
- **Raccoglitori:** puoi avere un massimo di 10 scraper il servizio gestito da Amazon per Prometheus per regione per account.

### Note

Puoi richiedere un aumento di questo limite [richiedendo un aumento della quota](#).

- **Risposta ai parametri:** il corpo di una risposta da una richiesta di `/metrics` endpoint non può superare i 50 megabyte (MB).
- **Endpoint per scraper:** uno scraper può eseguire lo scraper per un massimo di 30.000 `/metrics` endpoint.
- **Intervallo di scrape:** la configurazione dello scraper non può specificare un intervallo inferiore a 30 secondi.

## Quali sono i parametri compatibili con Prometheus?

Per estrarre i parametri di Prometheus dalle applicazioni e dall'infrastruttura per utilizzarli nel servizio gestito da Amazon per Prometheus, devono monitorare ed esporre i parametri compatibili con Prometheus dagli `/metrics` endpoint compatibili con Prometheus. Puoi inserire i tuoi parametri, ma non è necessario. Kubernetes (incluso Amazon EKS) e molte altre librerie e servizi inseriscono direttamente questi parametri.

Quando i parametri in Amazon EKS vengono esportati su un endpoint compatibile con Prometheus, puoi farli analizzare automaticamente dal raccoglitore del servizio gestito da Amazon per Prometheus.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Per ulteriori informazioni sulle librerie e sui servizi esistenti che esportano i parametri come parametri di Prometheus, consulta [Esportazioni e integrazioni](#) nella documentazione di Prometheus.
- Per ulteriori informazioni sull'esportazione di parametri compatibili con Prometheus dal proprio codice, vedere [Esportazioni di scrittura](#) nella documentazione di Prometheus.
- Per ulteriori informazioni su come configurare un raccoglitore del servizio gestito da Amazon per Prometheus per acquisire automaticamente i parametri dai cluster Amazon EKS, consulta [AWS Utilizzo di un raccoglitore gestito](#).

## Raccoglitori gestiti dal cliente

Questa sezione contiene informazioni sull'importazione di dati mediante la configurazione di raccoglitori personalizzati che inviano parametri al servizio gestito da Amazon per Prometheus utilizzando la scrittura remota di Prometheus.

Quando utilizzi i tuoi raccoglitori per inviare parametri al servizio gestito da Amazon per Prometheus, hai la responsabilità di proteggere i tuoi parametri e assicurarti che il processo di importazione soddisfi le tue esigenze di disponibilità.

La maggior parte dei raccoglitori gestiti dai clienti utilizza uno dei seguenti strumenti:

- **AWS Distro for OpenTelemetry (ADOT):** ADOT è una distribuzione open source completamente supportata, sicura e pronta per la produzione OpenTelemetry che consente agli agenti di raccogliere metriche. Puoi utilizzare ADOT per raccogliere parametri e inviarli alla tua area di lavoro del servizio gestito da Amazon per Prometheus. [Per ulteriori informazioni su ADOT Collector, vedete Distro for.AWS OpenTelemetry](#)
- **Agebte Prometheus:** puoi configurare la tua istanza del server open source Prometheus, in esecuzione come agente, per raccogliere parametri e inoltrarle alla tua area di lavoro del servizio gestito da Amazon per Prometheus.

Gli argomenti seguenti descrivono l'uso di entrambi questi strumenti e includono informazioni generali sulla configurazione dei propri raccoglitori.

### Argomenti

- [Proteggi l'importazione dei tuoi parametri](#)
- [Usare AWS Distro OpenTelemetry come collezionista](#)

- [Utilizzo di un'istanza Prometheus come raccogliitore](#)
- [Configurazione del servizio gestito da Amazon per Prometheus per dati di disponibilità elevata](#)

## Proteggi l'importazione dei tuoi parametri

Il servizio gestito da Amazon per Prometheus offre modi per aiutarti a garantire l'importazione dei tuoi parametri.

### Utilizzo AWS PrivateLink con Amazon Managed Service for Prometheus

Il traffico di rete per l'acquisizione delle metriche in Amazon Managed Service for Prometheus può essere effettuato tramite un endpoint Internet pubblico o tramite un endpoint VPC. AWS PrivateLink L'utilizzo AWS PrivateLink garantisce che il traffico di rete proveniente dai tuoi VPC sia protetto all'interno della rete AWS senza passare attraverso la rete Internet pubblica. Per creare un endpoint AWS PrivateLink VPC per Amazon Managed Service for Prometheus, consulta [Utilizzo di Amazon Managed Service for Prometheus con endpoint VPC di interfaccia](#)

### Autenticazione e autorizzazione

AWS Identity and Access Management (IAM) è un servizio web che consente di controllare in modo sicuro l'accesso alle AWS risorse. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse. Il servizio gestito da Amazon per Prometheus si integra con IAM per aiutarti a proteggere i tuoi dati. Quando configuri il servizio gestito da Amazon per Prometheus, devi creare alcuni ruoli IAM che gli consentano di importare i parametri dai server Prometheus e che consentano ai server Grafana di interrogare i parametri archiviate nelle tue aree di lavoro del servizio gestito da Amazon per Prometheus. Per ulteriori informazioni su IAM, consulta [Che cos'è IAM?](#)

Un'altra funzionalità AWS di sicurezza che può aiutarti a configurare Amazon Managed Service per Prometheus è AWS il processo di firma Signature Version 4 (SigV4).AWS Signature Version 4 è il processo per aggiungere informazioni di autenticazione alle richieste inviate tramite HTTP. AWS Per motivi di sicurezza, la maggior parte delle richieste AWS deve essere firmata con una chiave di accesso, che consiste in un ID della chiave di accesso e una chiave di accesso segreta. Queste due chiavi in genere vengono definite come le tue credenziali di sicurezza. Per ulteriori informazioni su SigV4, consulta [Processo di firma di Signature versione 4.](#)

## Usare AWS Distro OpenTelemetry come collezionista

I seguenti argomenti descrivono diversi modi per configurare AWS Distro OpenTelemetry come raccoglitore per le metriche.

### Argomenti

- [Configura l'inserimento dei parametri utilizzando AWS Distro for Open Telemetry su un cluster Amazon Elastic Kubernetes Service](#)
- [Configura l'inserimento dei parametri da Amazon ECS utilizzando AWS Distro for Open Telemetry](#)
- [Configura l'inserimento di parametri da un'istanza Amazon EC2 utilizzando la scrittura remota](#)

### Configura l'inserimento dei parametri utilizzando AWS Distro for Open Telemetry su un cluster Amazon Elastic Kubernetes Service

Questa sezione descrive come configurare AWS Distro for OpenTelemetry (ADOT) Collector per eseguire lo scraping da un'applicazione basata su Prometheus e inviare i parametri ad Amazon Managed Service for Prometheus. Per ulteriori informazioni [su AWS OpenTelemetry ADOT Collector](#), consulta Distro for.

La raccolta delle metriche di Prometheus con ADOT coinvolge OpenTelemetry tre componenti: il Prometheus Receiver, il Prometheus Remote Write Exporter e l'estensione di autenticazione Sigv4.

È possibile configurare il ricevitore Prometheus utilizzando la configurazione Prometheus esistente per eseguire il rilevamento dei servizi e lo scraping metrico. Il ricevitore Prometheus analizza i parametri nel formato di esposizione Prometheus. Tutte le applicazioni o gli endpoint che si desidera eseguire lo scraping devono essere configurati con la libreria client Prometheus. Il ricevitore Prometheus supporta il set completo di configurazioni di scraping e re-etichettatura di Prometheus descritte in [Configurazione](#) nella documentazione di Prometheus. È possibile incollare queste configurazioni direttamente nelle configurazioni di ADOT Collector.

Prometheus Remote Write Exporter utilizza l'endpoint per inviare i parametri eliminate `remote_write` all'area di lavoro del portale di gestione. Le richieste HTTP per esportare i dati verranno firmate con SigV4, il protocollo per l'autenticazione sicura, con l'estensione di autenticazione Sigv4 AWS . AWS Per ulteriori informazioni, consulta [Processo di firma di Signature versione 4](#).

Il raccoglitore rileva automaticamente gli endpoint delle parametri Prometheus su Amazon EKS e utilizza la configurazione disponibile in [<kubernetes\\_sd\\_config>](#).

La seguente demo è un esempio di questa configurazione su un cluster che esegue Amazon Elastic Kubernetes Service o Kubernetes autogestito. Per eseguire questi passaggi, è necessario disporre AWS delle credenziali di una qualsiasi delle possibili opzioni nella catena di credenziali predefinita. AWS Per ulteriori informazioni, consulta [Configurazione dell' AWS SDK](#) for Go. Questa demo utilizza un'app di esempio utilizzata per i test di integrazione del processo. L'app di esempio espone i parametri sull'/metricsendpoint, come la libreria client Prometheus.

## Prerequisiti

Prima di iniziare i seguenti passaggi di configurazione dell'importazione, devi configurare il tuo ruolo IAM per l'account del servizio e la policy di fiducia.

Per configurare il ruolo IAM per l'account del servizio e la policy di fiducia

1. Crea il ruolo IAM per l'account del servizio seguendo i passaggi riportati in [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS..](#)

ADOT Collector utilizzerà questo ruolo per acquisire ed esportare i parametri.

2. Successivamente, modifica la policy di fiducia. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
3. Nel riquadro di navigazione a sinistra, scegli Ruoli e trova amp-iamproxy-ingest-rolequello che hai creato nel passaggio 1.
4. Seleziona la scheda Relazioni di attendibilità e scegli Modifica relazione di attendibilità.
5. Nella policy di relazione di fiducia JSON, sostituisci aws - amp con adot - col e quindi scegli Aggiorna policy di fiducia. Il risultato della policy di fiducia sarà simile al seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::account-id:oidc-provider/oidc.eks.region.amazonaws.com/id/openid"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "oidc.eks.region.amazonaws.com/id/openid:sub":
            "system:serviceaccount:adot-col:amp-iamproxy-ingest-service-account"
        }
      }
    }
  ]
}
```

```
    }
  }
}
]
```

6. Scegli la scheda Autorizzazioni e assicurati che al ruolo sia associata la seguente policy di autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps:RemoteWrite",
        "aps:GetSeries",
        "aps:GetLabels",
        "aps:GetMetricMetadata"
      ],
      "Resource": "*"
    }
  ]
}
```

## Abilitazione della raccolta di parametri Prometheus

### Note

Quando crei uno spazio dei nomi in Amazon EKS, `alertmanager` e i nodi `Exporter` sono disabilitati per impostazione predefinita.

Per abilitare la raccolta Prometheus su un cluster Amazon EKS o Kubernetes

1. Fork e clona l'app di esempio dal repository all'indirizzo. [aws-otel-community](https://github.com/aws-otel-community)

Quindi, eseguire i seguenti comandi.

```
cd ./sample-apps/prometheus-sample-app
```

```
docker build . -t prometheus-sample-app:latest
```

2. Invia questa immagine a un registro come Amazon ECR o DockerHub.
3. Distribuisci l'app di esempio nel cluster copiando questa configurazione di Kubernetes e applicandola. Cambia l'immagine con quella che hai appena inserito sostituendo `{{PUBLIC_SAMPLE_APP_IMAGE}}` nel file `prometheus-sample-app.yaml`.

```
curl https://raw.githubusercontent.com/aws-observability/aws-otel-collector/main/examples/eks/aws-prometheus/prometheus-sample-app.yaml -o prometheus-sample-app.yaml
kubectl apply -f prometheus-sample-app.yaml
```

4. Esegui il comando seguente per verificare che l'app di prova sia stata avviata. Nell'output del comando, vedrai `prometheus-sample-app` nella NAME colonna.

```
kubectl get all -n aoc-prometheus-pipeline-demo
```

5. Avvia un'istanza predefinita di ADOT Collector. Per fare ciò, inserisci prima il seguente comando per estrarre la configurazione di Kubernetes per ADOT Collector.

```
curl https://raw.githubusercontent.com/aws-observability/aws-otel-collector/main/examples/eks/aws-prometheus/prometheus-daemonset.yaml -o prometheus-daemonset.yaml
```

Quindi modifica il file modello, sostituendo l'endpoint `remote_write` con la tua area di lavoro del servizio gestito da Amazon per Prometheus per `YOUR_ENDPOINT` e la tua regione per `YOUR_REGION`. Usa l'endpoint `remote_write` visualizzato nella console del servizio gestito da Amazon per Prometheus quando esamini i dettagli della tua area di lavoro.

Dovrai inoltre modificare l'ID del tuo account `YOUR_ACCOUNT_ID` nella sezione relativa all'account di servizio della configurazione di Kubernetes. AWS

In questo esempio, la configurazione ADOT Collector utilizza un'annotation (`scrape=true`) per indicare quali endpoint di destinazione eseguire lo scraping. Ciò consente a ADOT Collector di distinguere l'endpoint dell'app di esempio dagli endpoint del sistema kube nel cluster. Puoi rimuoverlo dalle configurazioni di rietichettatura se desideri eliminare un'altra app di esempio.

6. Inserisci il comando seguente per distribuire il raccogliatore ADOT.

```
kubectl apply -f prometheus-daemonset.yaml
```

7. Esegui il comando seguente per verificare che ADOT Collector sia stato avviato. Cerca `adot-col` nella colonna `NAMESPACE`.

```
kubectl get pods -n adot-col
```

8. Verifica che la pipeline funzioni utilizzando il logging exporter. Il nostro modello di esempio è già integrato con il logging exporter. Esegui i comandi seguenti:

```
kubectl get pods -A  
kubectl logs -n adot-col name_of_your_adot_collector_pod
```

Alcune dei parametri estratte dall'app di esempio saranno simili all'esempio seguente.

```
Resource labels:  
  -> service.name: STRING(kubernetes-service-endpoints)  
  -> host.name: STRING(192.168.16.238)  
  -> port: STRING(8080)  
  -> scheme: STRING(http)  
InstrumentationLibraryMetrics #0  
Metric #0  
Descriptor:  
  -> Name: test_gauge0  
  -> Description: This is my gauge  
  -> Unit:  
  -> DataType: DoubleGauge  
DoubleDataPoints #0  
StartTime: 0  
Timestamp: 1606511460471000000  
Value: 0.000000
```

9. Per verificare se il servizio gestito da Amazon per Prometheus ha ricevuto i parametri, usa `awscurl`. [Questo strumento ti consente di inviare richieste HTTP tramite la riga di comando con l'autenticazione AWS Sigv4, quindi devi avere AWS le credenziali configurate localmente con le autorizzazioni corrette per eseguire query da Amazon Managed Service for Prometheus. Per istruzioni sull'installazione, consulta `awscurl`.](#)

Nel comando seguente `AMP_REGION`, sostituisci e `AMP_ENDPOINT` con le informazioni per la tua area di lavoro del servizio gestito da Amazon per Prometheus.

```
awscurl --service="aps" --region="AMP_REGION" "https://AMP_ENDPOINT/api/v1/query?  
query=adot_test_gauge0"
```

```
{"status":"success","data":{"resultType":"vector","result":[{"metric":{"__name__":"adot_test_gauge0"},"value":[1606512592.493,"16.87214000011479"]}]]}}
```

Se ricevi un parametro come risposta, significa che la configurazione della pipeline è stata completata correttamente e il parametro è stato propagato con successo dall'app di esempio al servizio gestito da Amazon per Prometheus.

## Pulizia

Per ripulire questa demo, inserisci i seguenti comandi.

```
kubectl delete namespace aoc-prometheus-pipeline-demo
kubectl delete namespace adot-col
```

## Configurazione avanzata

Il ricevitore Prometheus supporta il set completo di configurazioni di scraping e re-etichettatura di Prometheus descritte in [Configurazione](#) nella documentazione di Prometheus. È possibile incollare queste configurazioni direttamente nelle configurazioni di ADOT Collector.

La configurazione per il ricevitore Prometheus include il rilevamento dei servizi, le configurazioni di scraping e le configurazioni di rietichettatura. La configurazione del ricevitore è simile alla seguente.

```
receivers:
  prometheus:
    config:
      [[Your Prometheus configuration]]
```

Di seguito è riportato un esempio di configurazione.

```
receivers:
  prometheus:
    config:
      global:
        scrape_interval: 1m
        scrape_timeout: 10s

      scrape_configs:
        - job_name: kubernetes-service-endpoints
          sample_limit: 10000
          kubernetes_sd_configs:
```

```
- role: endpoints
tls_config:
  ca_file: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
  insecure_skip_verify: true
  bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
```

Se disponi di una configurazione Prometheus esistente, devi sostituire i caratteri \$ con \$\$ per evitare che i valori vengano sostituiti con variabili di ambiente. \*Questo è particolarmente importante per il valore sostitutivo di relabel\_configurations. Ad esempio, se inizi con la seguente relabel\_configuration:

```
relabel_configs:
- source_labels:
  [__meta_kubernetes_ingress_scheme,__address__,__meta_kubernetes_ingress_path]
  regex: (.+);(.+);(.+)
  replacement: ${1}://${2}${3}
  target_label: __param_target
```

Diventerebbe il seguente:

```
relabel_configs:
- source_labels:
  [__meta_kubernetes_ingress_scheme,__address__,__meta_kubernetes_ingress_path]
  regex: (.+);(.+);(.+)
  replacement: $$${1}://${2}${3}
  target_label: __param_target
```

## Esportatore di scrittura remota Prometheus ed estensione di autenticazione Sigv4

La configurazione for Prometheus Remote Write Exporter e Sigv4 Authentication Extension è più semplice del ricevitore Prometheus. In questa fase della pipeline, i parametri sono già stati inseriti e siamo pronti per esportare questi dati nel servizio gestito da Amazon per Prometheus. Il requisito minimo per una corretta configurazione per comunicare con il servizio gestito da Amazon per Prometheus è illustrato nell'esempio seguente.

```
extensions:
  sigv4auth:
    service: "aps"
    region: "user-region"
exporters:
  prometheusremotewrite:
```

```
endpoint: "https://aws-managed-prometheus-endpoint/api/v1/remote_write"  
auth:  
  authenticator: "sigv4auth"
```

Questa configurazione invia una richiesta HTTPS firmata da SigV4 utilizzando le credenziali della catena di credenziali predefinita AWS . AWS AWS Per ulteriori informazioni, consultare la pagina relativa alla [configurazione di AWS SDK for Go](#). È necessario specificare il servizio come `aps`.

Indipendentemente dal metodo di distribuzione, il raccoglitore ADOT deve avere accesso a una delle opzioni elencate nella catena di credenziali predefinita. AWS L'estensione di autenticazione Sigv4 dipende da e la utilizza per recuperare le AWS SDK for Go credenziali e autenticarsi. Devi assicurarti che queste credenziali dispongano delle autorizzazioni di scrittura remota per il servizio gestito da Amazon per Prometheus.

## Configura l'inserimento dei parametri da Amazon ECS utilizzando AWS Distro for Open Telemetry

Questa sezione spiega come raccogliere metriche da Amazon Elastic Container Service (Amazon ECS) e inserirle in Amazon Managed Service for Prometheus utilizzando Distro for Open Telemetry (ADOT). AWS Descrive anche come visualizzare i tuoi parametri in Grafana gestito da Amazon.

### Prerequisiti

#### Important

Prima di iniziare, devi disporre di un ambiente Amazon ECS su un AWS Fargate cluster con impostazioni predefinite, un'area di lavoro del servizio gestito da Amazon per Prometheus e un'area di lavoro Grafana gestito da Amazon. Partiamo dal presupposto che tu abbia familiarità con i carichi di lavoro dei container, il servizio gestito da Amazon per Prometheus e Grafana gestito da Amazon.

Per ulteriori informazioni, consulta i collegamenti seguenti:

- Per informazioni su come creare un ambiente Amazon ECS su un cluster Fargate con impostazioni predefinite, consulta [Creazione di un cluster](#) nella Guida per lo sviluppatore Amazon ECS.
- Per informazioni su come creare un'area di lavoro del servizio gestito da Amazon per Prometheus, consulta [Creazione di un'area di lavoro](#) nella Guida per l'utente del servizio gestito da Amazon per Prometheus.

- Per informazioni su come creare un'area di lavoro Grafana gestito da Amazon, consulta [Creazione di un'area di lavoro](#) nella Guida per l'utente di Grafana gestito da Amazon.

Definisci un'immagine personalizzata del container ADOT Collector

Utilizza il seguente file di configurazione come modello per definire la tua immagine del container ADOT Collector. Sostituisci *my-remote-URL* e *my-region* con i tuoi valori endpoint e region. Salva la configurazione in un file denominato adot-config.yaml.

### Note

Questa configurazione utilizza l'`sigv4auth` estensione per autenticare le chiamate al servizio gestito da Amazon per Prometheus. [Per ulteriori informazioni sulla configurazione, consulta Authenticator - Sigv4 on. sigv4auth](#) GitHub

```
receivers:
  prometheus:
    config:
      global:
        scrape_interval: 15s
        scrape_timeout: 10s
      scrape_configs:
        - job_name: "prometheus"
          static_configs:
            - targets: [ 0.0.0.0:9090 ]
    awsecscontainermetrics:
      collection_interval: 10s
processors:
  filter:
    metrics:
      include:
        match_type: strict
      metric_names:
        - ecs.task.memory.utilized
        - ecs.task.memory.reserved
        - ecs.task.cpu.utilized
        - ecs.task.cpu.reserved
        - ecs.task.network.rate.rx
        - ecs.task.network.rate.tx
        - ecs.task.storage.read_bytes
```

```
- ecs.task.storage.write_bytes
exporters:
  prometheusremotewrite:
    endpoint: my-remote-URL
    auth:
      authenticator: sigv4auth
  logging:
    loglevel: info
extensions:
  health_check:
  pprof:
    endpoint: :1888
  zpages:
    endpoint: :55679
  sigv4auth:
    region: my-region
    service: aps
service:
  extensions: [pprof, zpages, health_check, sigv4auth]
  pipelines:
    metrics:
      receivers: [prometheus]
      exporters: [logging, prometheusremotewrite]
    metrics/ecs:
      receivers: [awsecscontainermetrics]
      processors: [filter]
      exporters: [logging, prometheusremotewrite]
```

Invia l'immagine del tuo container ADOT Collector a un repository Amazon ECR

Usa un Dockerfile per creare e inviare l'immagine del container a un repository Amazon Elastic Container Registry (ECR).

1. Crea il Dockerfile per copiare e aggiungere l'immagine del container all'immagine Docker di OTEL.

```
FROM public.ecr.aws/aws-observability/aws-otel-collector:latest
COPY adot-config.yaml /etc/ecs/otel-config.yaml
CMD ["--config=/etc/ecs/otel-config.yaml"]
```

2. Crea un repository Amazon ECR.

```
# create repo:
```

```
COLLECTOR_REPOSITORY=$(aws ecr create-repository --repository aws-otel-collector \
    --query repository.repositoryUri --output text)
```

### 3. Crea la tua immagine di container.

```
# build ADOT collector image:
docker build -t $COLLECTOR_REPOSITORY:ecs .
```

#### Note

Ciò presuppone che tu stia costruendo il tuo container nello stesso ambiente in cui verrà eseguito. In caso contrario, potrebbe essere necessario utilizzare il `--platform` parametro durante la creazione dell'immagine.

### 4. Accedi al repository Amazon ECR. Sostituisci *my-region* con il tuo valore *region*.

```
# sign in to repo:
aws ecr get-login-password --region my-region | \
    docker login --username AWS --password-stdin $COLLECTOR_REPOSITORY
```

### 5. Invia l'immagine del container.

```
# push ADOT collector image:
docker push $COLLECTOR_REPOSITORY:ecs
```

Crea una definizione di attività Amazon ECS per eseguire l'importazione del servizio gestito da Amazon per Prometheus

Crea una definizione di attività Amazon ECS per eseguire l'importazione del servizio gestito da Amazon per Prometheus. La definizione dell'attività deve includere un container denominato `adot-collector` e un container denominato `prometheus`. `prometheus` genera parametri e `adot-collector` scrape `prometheus`.

#### Note

Il servizio gestito da Amazon per Prometheus funziona come servizio, raccogliendo parametri dai container. I container in questo caso eseguono Prometheus localmente, in modalità Agente, che invia i parametri locali al servizio gestito da Amazon per Prometheus.

## Esempio: definizione di attività

Di seguito è riportato un esempio di come potrebbe presentarsi la definizione dell'attività. È possibile utilizzare questo esempio come modello per creare la propria definizione di attività. Sostituisci il `image` valore di `adot-collector` con l'URL del repository e il tag dell'immagine (`$COLLECTOR_REPOSITORY:ecs`). Sostituisci i valori di `region` di `adot-collector` e `prometheus` con i tuoi valori `region`.

```
{
  "family": "adot-prom",
  "networkMode": "awsvpc",
  "containerDefinitions": [
    {
      "name": "adot-collector",
      "image": "account_id.dkr.ecr.region.amazonaws.com/image-tag",
      "essential": true,
      "logConfiguration": {
        "logDriver": "awslogs",
        "options": {
          "awslogs-group": "/ecs/ecs-adot-collector",
          "awslogs-region": "my-region",
          "awslogs-stream-prefix": "ecs",
          "awslogs-create-group": "True"
        }
      }
    },
    {
      "name": "prometheus",
      "image": "prom/prometheus:main",
      "logConfiguration": {
        "logDriver": "awslogs",
        "options": {
          "awslogs-group": "/ecs/ecs-prom",
          "awslogs-region": "my-region",
          "awslogs-stream-prefix": "ecs",
          "awslogs-create-group": "True"
        }
      }
    }
  ],
  "requiresCompatibilities": [
    "FARGATE"
  ],
}
```

```
"cpu": "1024"  
}
```

Collega la AWS policy gestita **AmazonPrometheusRemoteWriteAccess** in un ruolo IAM per la tua attività.

Per inviare i parametri eliminati ad Amazon Managed Service for Prometheus, la tua attività Amazon ECS deve disporre delle autorizzazioni corrette per chiamare le operazioni API per te. AWS Devi creare un ruolo IAM e una policy AmazonPrometheusRemoteWriteAccess per le tue attività. Per ulteriori informazioni sulla creazione di un ruolo per i processi, consulta [Creazione di un ruolo e una policy IAM per le attività](#) .

Dopo esserti collegato AmazonPrometheusRemoteWriteAccess al tuo ruolo IAM e aver utilizzato quel ruolo per le tue attività, Amazon ECS può inviare i tuoi parametri eliminati al servizio gestito da Amazon per Prometheus.

Visualizza i tuoi parametri in Grafana gestito da Amazon

#### Important

Prima di iniziare, devi eseguire un processo Fargate nella definizione dell'attività Amazon ECS. Altrimenti, il servizio gestito da Amazon per Prometheus non può utilizzare i tuoi parametri.

1. Dal pannello di navigazione del tuo spazio di lavoro Amazon Managed Grafana, scegli Origini dati sotto l'icona. AWS
2. Nella scheda Origini dati, per Servizio, seleziona Servizio gestito da Amazon per Prometheus e scegli la tua regione predefinita.
3. Scegli Aggiungi origine dati.
4. Usa i prefissi ecs e prometheus per interrogare e visualizzare i tuoi parametri.

## Configura l'inserimento di parametri da un'istanza Amazon EC2 utilizzando la scrittura remota

Questa sezione spiega come eseguire un server Prometheus con scrittura remota in un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Spiega come raccogliere parametri da

un'applicazione demo scritta in Go e inviarle a un'area di lavoro del servizio gestito da Amazon per Prometheus.

## Prerequisiti

### Important

Prima di iniziare, è necessario aver installato Prometheus v2.26 o una versione successiva. Partiamo dal presupposto che tu conosca Prometheus, Amazon EC2 e il servizio gestito da Amazon per Prometheus. Per informazioni su come installare Prometheus, vedi [Guida introduttiva](#) sul sito web di Prometheus.

Se non conosci Amazon EC2 o il servizio gestito da Amazon per Prometheus, ti consigliamo di iniziare leggendo le sezioni seguenti:

- [Cos'è Amazon Elastic Compute Cloud?](#)
- [Cos'è il servizio gestito da Amazon per Prometheus?](#)

## Creazione di un ruolo IAM per Amazon EC2

Per eseguire lo streaming delle metriche, devi prima creare un ruolo IAM con la AWS policy gestita. AmazonPrometheusRemoteWriteAccess. Quindi, puoi avviare un'istanza con il ruolo e i parametri di streaming nella tua area di lavoro del servizio gestito da Amazon per Prometheus.

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione selezionare Roles (Ruoli), quindi Create role (Crea ruolo).
3. Per il tipo di entità attendibile, scegliere AWS service (Servizio). Per il caso d'uso, scegli EC2. Scegli Successivo: autorizzazioni.
4. Nella barra di ricerca inserisci AmazonPrometheusRemoteWriteAccess. Per Nome della policy, seleziona AmazonPrometheusRemoteWriteAccess, quindi scegli Allega policy. Scegli Successivo: Tag.
5. (Facoltativo) Crea tag IAM per il tuo ruolo IAM. Scegli Prossimo: Rivedi.
6. Immetti un nome per il ruolo. Scegli Crea policy.

## Avviare un'istanza Amazon EC2

Per avviare un'istanza Amazon EC2, segui le istruzioni riportate in [Avvio di un'istanza](#) nella Guida per l'utente di Amazon Elastic Compute Cloud per le istanze Linux.

### Esegui l'applicazione demo

Dopo aver creato il tuo ruolo IAM e avviato un'istanza EC2 con il ruolo, puoi eseguire un'applicazione demo per vederlo funzionare.

Per eseguire un'applicazione demo e testare le metriche

1. Utilizza il seguente modello per creare un file Go denominato `main.go`.

```
package main

import (
    "github.com/prometheus/client_golang/prometheus/promhttp"
    "net/http"
)

func main() {
    http.Handle("/metrics", promhttp.Handler())

    http.ListenAndServe(":8000", nil)
}
```

2. Esegui il comando riportato qui di seguito per installare la dipendenza.

```
sudo yum update -y
sudo yum install -y golang
go get github.com/prometheus/client_golang/prometheus/promhttp
```

3. Esegui l'applicazione demo.

```
go run main.go
```

L'applicazione demo dovrebbe funzionare sulla porta 8000 e mostrare tutti i parametri di Prometheus esposte. Di seguito è riportato un esempio di questi parametri.

```
curl -s http://localhost:8000/metrics
...
```

```

process_max_fds 4096# HELP process_open_fds Number of open file descriptors.# TYPE
  process_open_fds gauge
process_open_fds 10# HELP process_resident_memory_bytes Resident memory size in
  bytes.# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes 1.0657792e+07# HELP process_start_time_seconds Start
  time of the process since unix epoch in seconds.# TYPE process_start_time_seconds
  gauge
process_start_time_seconds 1.61131955899e+09# HELP process_virtual_memory_bytes
  Virtual memory size in bytes.# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes 7.77281536e+08# HELP process_virtual_memory_max_bytes
  Maximum amount of virtual memory available in bytes.# TYPE
  process_virtual_memory_max_bytes gauge
process_virtual_memory_max_bytes -1# HELP
  promhttp_metric_handler_requests_in_flight Current number of scrapes being
  served.# TYPE promhttp_metric_handler_requests_in_flight gauge
promhttp_metric_handler_requests_in_flight 1# HELP
  promhttp_metric_handler_requests_total Total number of scrapes by HTTP status
  code.# TYPE promhttp_metric_handler_requests_total counter
promhttp_metric_handler_requests_total{code="200"} 1
promhttp_metric_handler_requests_total{code="500"} 0
promhttp_metric_handler_requests_total{code="503"} 0

```

Creazione di un'area di lavoro del servizio gestito da Amazon per Prometheus.

Per creare un'area di lavoro del servizio gestito da Amazon per Prometheus, segui le istruzioni in [Creazione di un'area di lavoro](#).

Esegui un server Prometheus

1. Utilizza il seguente file YAML di esempio come modello per creare un nuovo file denominato `prometheus.yaml`. Infatti, sostituisce `my-region` con il valore della tua regione e `my-workspace-id` con l'ID dell'area di lavoro che Amazon Managed Service for Prometheus ha generato per te. Per `region`, sostituisce `my-region` con il valore della tua regione.

Esempio: file YAML

```

global:
  scrape_interval: 15s
  external_labels:
    monitor: 'prometheus'

scrape_configs:

```

```
- job_name: 'prometheus'
  static_configs:
    - targets: ['localhost:8000']

remote_write:
-
  url: https://aps-workspaces.my-region.amazonaws.com/workspaces/my-workspace-id/
  api/v1/remote_write
  queue_config:
    max_samples_per_send: 1000
    max_shards: 200
    capacity: 2500
  sigv4:
    region: my-region
```

2. Esegui il server Prometheus per inviare i parametri dell'applicazione demo alla tua area di lavoro del servizio gestito da Amazon per Prometheus.

```
prometheus --config.file=prometheus.yaml
```

Il server Prometheus dovrebbe ora inviare i parametri dell'applicazione demo alla tua area di lavoro del servizio gestito da Amazon per Prometheus.

## Utilizzo di un'istanza Prometheus come raccogliitore

I seguenti argomenti descrivono diversi modi per configurare un'istanza di Prometheus in esecuzione in modalità agente come raccogliitore per i parametri.

### Warning

Evita di esporre gli endpoint Prometheus Scrape alla rete Internet pubblica [abilitando le funzionalità di sicurezza](#).

Se configuri più istanze Prometheus che monitorano lo stesso set di parametri e le invii a un'unica area di lavoro del servizio gestito da Amazon per Prometheus per l'alta disponibilità, devi configurare la deduplicazione. Se non segui i passaggi per configurare la deduplicazione, ti verranno addebitati tutti i campioni di dati inviati al servizio gestito da Amazon per Prometheus, inclusi i campioni duplicati. Per istruzioni sulla configurazione della deduplicazione, consulta [Deduplicazione dei parametri di disponibilità elevata inviati al servizio gestito da Amazon per Prometheus](#).

## Argomenti

- [Configurare l'importazione da un nuovo server Prometheus utilizzando Helm](#)
- [Configura l'importazione da un server Prometheus esistente in Kubernetes su EC2](#)
- [Configurare l'importazione da un server Prometheus esistente in Kubernetes su Fargate](#)

## Configurare l'importazione da un nuovo server Prometheus utilizzando Helm

Le istruzioni in questa sezione ti consentono di iniziare rapidamente a utilizzare il servizio gestito da Amazon per Prometheus. Hai configurato un nuovo server Prometheus in un cluster Amazon EKS e il nuovo server utilizza una configurazione predefinita per inviare i parametri al servizio gestito da Amazon per Prometheus. Questo metodo ha i seguenti prerequisiti:

- È necessario disporre di un cluster Amazon EKS da cui il nuovo server Prometheus raccoglierà i parametri
- È necessario utilizzare Helm CLI 3.0 o una versione successiva
- È necessario utilizzare un computer Linux o macOS per eseguire i passaggi descritti nelle seguenti sezioni.

### Fase 1: aggiunta di nuovi repository del grafico Helm

Immetti i seguenti comandi per aggiungere il nuovo repository del grafico Helm. Per ulteriori informazioni su questi comandi, consulta [Repository Helm](#).

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
helm repo add kube-state-metrics https://kubernetes.github.io/kube-state-metrics
helm repo update
```

### Fase 2: creazione di un namespace Prometheus.

Immetti il seguente comando per creare un namespace Prometheus per il server Prometheus e altri componenti di monitoraggio. Sostituisci *prometheus-namespace* con il nome che desideri per questo namespace.

```
kubectl create namespace prometheus-namespace
```

### Fase 3: configurazione dei ruoli IAM per gli account del servizio.

Per il metodo di onboarding che stiamo documentando, devi utilizzare i ruoli IAM per gli account del servizio nel cluster Amazon EKS in cui è in esecuzione il server Prometheus.

Grazie ai ruoli IAM per gli account del servizio, è possibile associare un ruolo IAM a un account del servizio Kubernetes. Questo account del servizio può quindi fornire le autorizzazioni AWS ai container in qualsiasi pod che utilizza tale account. Per ulteriori informazioni, consulta [Ruoli IAM per gli account del servizio](#).

Se non hai già impostato questi ruoli, segui le istruzioni riportate in [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS](#), per configurare i ruoli. Le istruzioni contenute in quella sezione richiedono l'uso di eksctl. Per ulteriori informazioni, consulta [Nozioni di base su Amazon Elastic Kubernetes Service – eksctl](#).

#### Note

Quando non utilizzi EKS o utilizzi solo la chiave di accesso AWS e la chiave segreta per accedere ad Amazon Managed Service for Prometheus, non puoi usare il SigV4 basato EKS-IAM-ROLE

### Fase 4: configurazione del nuovo server e avvio dell'importazione dei parametri

Per installare il nuovo server Prometheus che invia i parametri alla tua area di lavoro del servizio gestito da Amazon per Prometheus, segui questi passaggi.

Per installare un nuovo server Prometheus per inviare parametri alla tua area di lavoro del servizio gestito da Amazon per Prometheus

1. Utilizza un editor di testo per creare un file denominato `my_prometheus_values.yaml` con il seguente contenuto.
  - Sostituisci `IAM_PROXY_PROMETHEUS_ROLE_ARN` con *l'ARN del file in cui hai creato* `amp-iamproxy-ingest-role` [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS](#).
  - Sostituisci `WORKSPACE_ID` con l'ID della tua area di lavoro del servizio gestito da Amazon per Prometheus.

- Sostituisci **REGION** con la regione della tua area di lavoro del servizio gestito da Amazon per Prometheus.

```
## The following is a set of default values for prometheus server helm chart which
enable remoteWrite to AMP
## For the rest of prometheus helm chart values see: https://github.com/prometheus-
community/helm-charts/blob/main/charts/prometheus/values.yaml
##
serviceAccounts:
  server:
    name: amp-iamproxy-ingest-service-account
    annotations:
      eks.amazonaws.com/role-arn: ${IAM_PROXY_PROMETHEUS_ROLE_ARN}
server:
  remoteWrite:
    - url: https://aps-workspaces.${REGION}.amazonaws.com/workspaces/
      ${WORKSPACE_ID}/api/v1/remote_write
      sigv4:
        region: ${REGION}
      queue_config:
        max_samples_per_send: 1000
        max_shards: 200
        capacity: 2500
```

## 2. Inserisci il seguente comando per creare il server di Prometheus.

- ***prometheus-chart-name*** Sostituiscilo con il nome della versione Prometheus.
- Sostituisci ***prometheus-namespace*** con il nome del tuo namespace Prometheus.

```
helm install prometheus-chart-name prometheus-community/prometheus -n prometheus-
namespace \
-f my_prometheus_values.yaml
```

### Note

È possibile personalizzare il comando `helm install` in molti modi. Per ulteriori informazioni, consulta [Installazione di Helm](#) nella documentazione di Helm.

## Configura l'importazione da un server Prometheus esistente in Kubernetes su EC2

Il servizio gestito da Amazon per Prometheus supporta l'importazione di parametri dai server Prometheus in cluster in esecuzione su Amazon EKS e in cluster Kubernetes autogestiti in esecuzione su Amazon EC2. Le istruzioni dettagliate in questa sezione si riferiscono a un server Prometheus in un cluster Amazon EKS. I passaggi per un cluster Kubernetes autogestito su Amazon EC2 sono gli stessi, tranne per il fatto che dovrai configurare tu stesso il provider OIDC e i ruoli IAM per gli account del servizio nel cluster Kubernetes.

Le istruzioni in questa sezione utilizzano Helm come gestore di pacchetti Kubernetes.

### Argomenti

- [Fase 1: configurazione dei ruoli IAM per gli account del servizio.](#)
- [Fase 2: aggiornamento del server Prometheus esistente mediante Helm](#)

Fase 1: configurazione dei ruoli IAM per gli account del servizio.

Per il metodo di onboarding che stiamo documentando, devi utilizzare i ruoli IAM per gli account del servizio nel cluster Amazon EKS in cui è in esecuzione il server Prometheus. Questi ruoli sono denominati ruoli di servizio.

Con i ruoli di servizio, puoi associare un ruolo IAM a un account del servizio Kubernetes. Questo account di servizio può quindi fornire AWS le autorizzazioni ai contenitori in qualsiasi pod che utilizza quell'account di servizio. Per ulteriori informazioni, consulta [Ruoli IAM per gli account del servizio](#).

Se non hai già impostato questi ruoli, segui le istruzioni riportate in [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS](#), per configurare i ruoli.

Fase 2: aggiornamento del server Prometheus esistente mediante Helm

Le istruzioni in questa sezione includono la configurazione della scrittura remota e di sigv4 per autenticare e autorizzare il server Prometheus alla scrittura remota nell'area di lavoro del servizio gestito da Amazon per Prometheus.

Utilizzo di Prometheus versione 2.26.0 o successiva

Segui questi passaggi se utilizzi un grafico Helm con un'immagine del server Prometheus della versione 2.26.0 o successiva.

## Per configurare la scrittura remota da un server Prometheus utilizzando un grafico Helm

### 1. Crea una nuova sezione di scrittura remota nel tuo file di configurazione Helm:

- Sostituisci `${IAM_PROXY_PROMETHEUS_ROLE_ARN}` con l'ARN del file in `amp-iamproxy-ingest-role` cui hai creato. [Fase 1: configurazione dei ruoli IAM per gli account del servizio](#). Il ruolo ARN dovrebbe avere il formato di `arn:aws:iam::your account ID:role/amp-iamproxy-ingest-role`.
- Sostituisci `${WORKSPACE_ID}` con la tua area di lavoro del servizio gestito da Amazon per Prometheus.
- Sostituisci `${REGION}` con la regione dell'area di lavoro del servizio gestito da Amazon per Prometheus (come `us-west-2`).

```
## The following is a set of default values for prometheus server helm chart which
enable remoteWrite to AMP
## For the rest of prometheus helm chart values see: https://github.com/
prometheus-community/helm-charts/blob/main/charts/prometheus/values.yaml
##
serviceAccounts:
  server:
    name: amp-iamproxy-ingest-service-account
    annotations:
      eks.amazonaws.com/role-arn: ${IAM_PROXY_PROMETHEUS_ROLE_ARN}
  server:
    remoteWrite:
      - url: https://aps-workspaces.${REGION}.amazonaws.com/workspaces/
        ${WORKSPACE_ID}/api/v1/remote_write
      sigv4:
        region: ${REGION}
      queue_config:
        max_samples_per_send: 1000
        max_shards: 200
        capacity: 2500
```

### 2. Aggiorna la configurazione esistente del server Prometheus utilizzando Helm:

- Sostituisci `prometheus-chart-name` con il nome della versione di Prometheus.
- Sostituisci `prometheus-namespace` con il namespace Kubernetes dove è installato il server Prometheus.

- Sostituisci `my_prometheus_values_yaml` con il percorso del file di configurazione Helm.
- Sostituisci `current_helm_chart_version` con la versione corrente del diagramma Prometheus Server del grafico Helm. Puoi trovare la versione attuale della carta utilizzando il comando [helm list](#).

```
helm upgrade prometheus-chart-name prometheus-community/prometheus \
  -n prometheus-namespace \
  -f my_prometheus_values_yaml \
  --version current_helm_chart_version
```

## Utilizzo delle versioni precedenti di Prometheus

Segui questi passaggi se utilizzi una versione di Prometheus precedente alla 2.26.0. Questi passaggi utilizzano un approccio secondario, poiché le versioni precedenti di Prometheus non AWS supportano nativamente il processo di firma Signature Version 4 (SigV4).AWS

Queste istruzioni presuppongono che tu stia usando Helm per implementare Prometheus.

## Come configurare la scrittura remota da un server Prometheus

1. Sul server Prometheus, crea una nuova configurazione di scrittura remota. Innanzitutto, crea un nuovo file di aggiornamento. Chiameremo il file `amp_ingest_override_values.yaml`.

Modifica il file e aggiungi i valori seguenti.

```
serviceAccounts:
  server:
    name: "amp-iamproxy-ingest-service-account"
    annotations:
      eks.amazonaws.com/role-arn:
        "${SERVICE_ACCOUNT_IAM_INGEST_ROLE_ARN}"
  server:
    sidecarContainers:
      - name: aws-sigv4-proxy-sidecar
        image: public.ecr.aws/aws-observability/aws-sigv4-proxy:1.0
        args:
          - --name
          - aps
          - --region
          - ${REGION}
```

```

- --host
- aps-workspaces.${REGION}.amazonaws.com
- --port
- :8005
ports:
- name: aws-sigv4-proxy
  containerPort: 8005
statefulSet:
  enabled: "true"
remoteWrite:
- url: http://localhost:8005/workspaces/${WORKSPACE_ID}/api/v1/
remote_write

```

Sostituisci `${REGION}` con la regione dell'area di lavoro del servizio gestito da Amazon per Prometheus.

Sostituisci `${SERVICE_ACCOUNT_IAM_INGEST_ROLE_ARN}` con l'ARN del file in `amp-iamproxy-ingest-role` cui hai creato. [Fase 1: configurazione dei ruoli IAM per gli account del servizio](#). Il ruolo ARN dovrebbe avere il formato di `arn:aws:iam::your account ID:role/amp-iamproxy-ingest-role`.

Sostituisci `${WORKSPACE_ID}` con il tuo ID dell'area di lavoro.

2. Aggiorna il tuo grafico Prometheus del grafico Helm. Innanzitutto, trova il nome del tuo grafico Helm inserendo il seguente comando. Nell'output di questo comando, cerca un grafico con un nome che includa `prometheus`.

```
helm ls --all-namespaces
```

Quindi, immetti il comando seguente:

```
helm upgrade --install prometheus-helm-chart-name prometheus-community/prometheus -n prometheus-namespace -f ./amp_ingest_override_values.yaml
```

Sostituisci `prometheus-helm-chart-name` con il nome della tabella del timone di Prometheus restituita nel comando precedente. Sostituisci `prometheus-namespace` con il nome del tuo namespace.

## Scaricamento dei grafici Helm

Se non hai già scaricato localmente i grafici Helm, puoi utilizzare il comando seguente per scaricarli.

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
helm pull prometheus-community/prometheus --untar
```

## Configurare l'importazione da un server Prometheus esistente in Kubernetes su Fargate

Il servizio gestito da Amazon per Prometheus supporta l'importazione di parametri dai server di Prometheus in cluster Kubernetes autogestiti in esecuzione su Fargate. Per importare i parametri dai server Prometheus nei cluster Amazon EKS in esecuzione su Fargate, sovrascrivi le configurazioni predefinite in un file di configurazione denominato `amp_ingest_override_values.yaml` come segue:

```
prometheus-node-exporter:
  enabled: false

alertmanager:
  enabled: false

serviceAccounts:
  server:
    name: amp-iamproxy-ingest-service-account
    annotations:
      eks.amazonaws.com/role-arn: ${IAM_PROXY_PROMETHEUS_ROLE_ARN}

server:
  persistentVolume:
    enabled: false
  remoteWrite:
    - url: https://aps-workspaces.${REGION}.amazonaws.com/workspaces/
      ${WORKSPACE_ID}/api/v1/remote_write
      sigv4:
        region: ${REGION}
      queue_config:
        max_samples_per_send: 1000
        max_shards: 200
        capacity: 2500
```

Installa Prometheus utilizzando gli override con il comando seguente:

```
helm install prometheus-for-amp prometheus-community/prometheus \
  -n prometheus \
  -f amp_ingest_override_values.yaml
```

Nota che nella configurazione del grafico Helm abbiamo disabilitato l'esportatore di nodi e l'alert manager, oltre a eseguire l'implementazione del server Prometheus.

È possibile verificare l'installazione con la seguente interrogazione del test di esempio.

```
$ awscurl --region region --service aps "https://aps-
workspaces.region_id.amazonaws.com/workspaces/workspace_id/api/v1/query?
query=prometheus_api_remote_read_queries"
  {"status": "success", "data": {"resultType": "vector", "result": [{"metric":
{"__name__": "prometheus_api_remote_read_queries", "instance": "localhost:9090", "job": "prometheus"
[1648461236.419, "0"]}]}]}21
```

## Configurazione del servizio gestito da Amazon per Prometheus per dati di disponibilità elevata

Quando invii dati al servizio gestito da Amazon per Prometheus, questi vengono replicati AWS automaticamente nelle zone di disponibilità della regione e ti vengono forniti da un cluster di host che forniscono scalabilità, disponibilità e sicurezza. Potresti voler aggiungere ulteriori sistemi di sicurezza ad alta disponibilità, a seconda della configurazione specifica. Esistono due modi comuni per aggiungere sistemi di sicurezza ad alta disponibilità alla configurazione:

- Se disponi di più contenitori o istanze con gli stessi dati, puoi inviare tali dati al servizio gestito da Amazon per Prometheus e deduplicarli automaticamente. Questo aiuta a garantire che i tuoi dati vengano inviati alla tua area di lavoro del servizio gestito da Amazon per Prometheus.

Per ulteriori informazioni sulla deduplicazione dei dati di disponibilità elevata consulta [Deduplicazione dei parametri di disponibilità elevata inviati al servizio gestito da Amazon per Prometheus](#).

- Se vuoi assicurarti di avere accesso ai tuoi dati, anche quando la AWS regione non è disponibile, puoi inviare i parametri a un secondo area di lavoro, in un'altra regione.

Per ulteriori informazioni sull'invio di dati dei parametri a più aree di lavoro, consulta [Disponibilità interregionale](#).

## Argomenti

- [Deduplicazione dei parametri di disponibilità elevata inviati al servizio gestito da Amazon per Prometheus](#)
- [Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con Prometheus](#)
- [Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con l'operatore Prometheus](#)
- [Invia dati ad alta disponibilità ad Amazon Managed Service for AWS Prometheus con Distro for Open Telemetry](#)
- [Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con il grafico Helm della community Prometheus](#)
- [Domande frequenti: Configurazione di elevata disponibilità](#)
- [Disponibilità interregionale](#)

## Deduplicazione dei parametri di disponibilità elevata inviati al servizio gestito da Amazon per Prometheus

Puoi inviare dati da più agenti Prometheus (istanze Prometheus in esecuzione in modalità Agente) alla tua area di lavoro del servizio gestito da Amazon per Prometheus. Se alcune di queste istanze registrano e inviano gli stessi parametri, i tuoi dati avranno una maggiore disponibilità (anche se uno degli agenti interrompe l'invio dei dati, l'area di lavoro del servizio gestito da Amazon per Prometheus continuerà a ricevere i dati da un'altra istanza). Tuttavia, desideri che la tua area di lavoro del servizio gestito da Amazon per Prometheus deduplichi automaticamente i parametri in modo da non visualizzarli più volte e non ricevere più addebiti per l'importazione e l'archiviazione dei dati.

Affinché il servizio gestito da Amazon per Prometheus possa deduplicare automaticamente i dati da più agenti Prometheus, devi assegnare al set di agenti che inviano i dati duplicati un unico nome di cluster e a ciascuna istanza un nome di replica. Il nome del cluster identifica le istanze con dati condivisi e il nome della replica consente al servizio gestito da Amazon per Prometheus di identificare l'origine di ogni parametro. I parametri finali memorizzate includono l'etichetta del cluster, ma non la replica, quindi i parametri sembrano provenire da un'unica fonte.

### Note

Alcune versioni di Kubernetes (1.28 e 1.29) possono emettere una propria metrica con un'etichetta. `cluster` Ciò può causare problemi con la deduplicazione di Amazon Managed

Service for Prometheus. Per ulteriori informazioni, consulta le domande [frequenti sull'alta disponibilità](#).

I seguenti argomenti mostrano come inviare dati e includono le `__replica__` etichette `cluster` e, in modo che Amazon Managed Service for Prometheus deduplica i dati automaticamente.

#### Important

Se non configuri la deduplicazione, ti verranno addebitati tutti i campioni di dati inviati al servizio gestito da Amazon per Prometheus. Questi esempi di dati includono campioni duplicati.

## Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con Prometheus

Per configurare una configurazione di elevata disponibilità con Prometheus, devi applicare etichette esterne su tutte le istanze di un gruppo di elevata disponibilità, in modo che il servizio gestito da Amazon per Prometheus possa identificarle. Utilizza l'`cluster` etichetta per identificare un agente di istanza Prometheus come parte di un gruppo di elevata disponibilità. Utilizza l'`__replica__` etichetta per identificare separatamente ogni replica del gruppo. Affinché la deduplicazione `__replica__` funzioni, è necessario applicare le etichette e `cluster`.

#### Note

L'`__replica__` etichetta è formattata con due simboli di sottolineatura prima e dopo la parola `replica`.

### Esempio: frammenti di codice

Nei seguenti frammenti di codice, l'`cluster` etichetta identifica l'agente dell'istanza Prometheus `prom-team1` e l'`__replica__` etichetta identifica le repliche `replica1` e `replica2`.

```
cluster: prom-team1
__replica__: replica1
```

```
cluster: prom-team1
__replica__: replica2
```

Poiché il servizio gestito da Amazon per Prometheus archivia campioni di dati provenienti da repliche ad alta disponibilità con queste etichette, rimuove `replica` l'etichetta quando i campioni vengono accettati. Ciò significa che avrai solo una mappatura in serie 1:1 per la tua serie attuale anziché una serie per replica. L'`cluster` etichetta viene mantenuta.

### Note

Alcune versioni di Kubernetes (1.28 e 1.29) possono emettere una propria metrica con un'etichetta. `cluster` Ciò può causare problemi con la deduplicazione di Amazon Managed Service for Prometheus. Per ulteriori informazioni, consulta le domande [frequenti sull'alta disponibilità](#).

## Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con l'operatore Prometheus

Per configurare una configurazione ad alta disponibilità con Prometheus Operator, devi applicare etichette esterne su tutte le istanze di un gruppo di elevata disponibilità, in modo che il servizio gestito da Amazon per Prometheus possa identificarle. È inoltre necessario impostare gli attributi `replicaExternalLabelName` e `externalLabels` sulla tabella Prometheus Operator del grafico Helm.

Esempio: intestazione YAML

Nella seguente intestazione YAML, `cluster` viene aggiunto a `externalLabel` per identificare un agente di istanza Prometheus come parte di un gruppo ad alta disponibilità e `replicaExternalLabels` identifica ogni replica del gruppo.

```
replicaExternalLabelName: __replica__
externalLabels:
cluster: prom-dev
```

### Note

Alcune versioni di Kubernetes (1.28 e 1.29) possono emettere una propria metrica con un'etichetta. `cluster` Ciò può causare problemi con la deduplicazione di Amazon Managed

Service for Prometheus. Per ulteriori informazioni, consulta le domande [frequenti sull'alta disponibilità](#).

## Invia dati ad alta disponibilità ad Amazon Managed Service for AWS Prometheus con Distro for Open Telemetry

AWS Distro for Open Telemetry (ADOT) è una distribuzione del progetto sicura e pronta per la produzione. OpenTelemetry ADOT fornisce API, librerie e agenti di origine, in modo da poter raccogliere tracce e parametri distribuiti per il monitoraggio delle applicazioni. [Per informazioni su ADOT, consulta About Distro for Open Telemetry. AWS](#)

Per configurare ADOT con una configurazione ad alta disponibilità, è necessario configurare un'immagine del contenitore ADOT Collector e applicare le etichette esterne e all'esportatore di scrittura `cluster remoto __replica__ Prometheus AWS`. Questo esportatore invia i parametri eliminate all'area di lavoro del servizio gestito da Amazon per Prometheus tramite l'endpoint `remote_write`. Quando imposti queste etichette sull'esportatore di scrittura remota, eviti che i parametri duplicate vengano conservate durante l'esecuzione di repliche ridondanti. Per ulteriori informazioni sull'esportatore di scrittura remota AWS Prometheus, consulta [Guida introduttiva all'esportatore di scrittura remota Prometheus per Amazon Managed Service for Prometheus](#).

### Note

Alcune versioni di Kubernetes (1.28 e 1.29) possono emettere una propria metrica con un'etichetta. `cluster` Ciò può causare problemi con la deduplicazione di Amazon Managed Service for Prometheus. Per ulteriori informazioni, consulta le domande [frequenti sull'alta disponibilità](#).

## Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con il grafico Helm della community Prometheus

Per configurare una configurazione ad alta disponibilità con il grafico Helm della community Prometheus, devi applicare etichette esterne su tutte le istanze di un gruppo di elevata disponibilità, in modo che il servizio gestito da Amazon per Prometheus possa identificarle. Ecco un esempio di come aggiungere `external_labels` a una singola istanza di Prometheus del grafico Helm della comunità Prometheus.

```
server:
global:
  external_labels:
    cluster: monitoring-cluster
    __replica__: replica-1
```

### Note

Se desideri più repliche, devi implementare il grafico più volte con valori di replica diversi, perché il grafico Helm della community di Prometheus non consente di impostare dinamicamente il valore della replica quando si aumenta il numero di repliche direttamente dal gruppo di controller. Se preferisci che l'`replica` etichetta venga impostata automaticamente, usa il grafico Helm dell'operatore Prometheus.

### Note

Alcune versioni di Kubernetes (1.28 e 1.29) possono emettere una propria metrica con un'etichetta. `cluster` Ciò può causare problemi con la deduplicazione di Amazon Managed Service for Prometheus. Per ulteriori informazioni, consulta le domande [frequenti sull'alta disponibilità](#).

## Domande frequenti: Configurazione di elevata disponibilità

Devo includere il valore `__replica__` in un'altra etichetta per tracciare i punti di campionamento?

In un ambiente a elevata disponibilità, il servizio gestito da Amazon per Prometheus garantisce che i campioni di dati non vengano duplicati eleggendo un leader nel cluster di istanze Prometheus. Se la replica leader interrompe l'invio di campioni di dati per 30 secondi, il servizio gestito da Amazon per Prometheus trasforma automaticamente un'altra istanza Prometheus in una replica leader e inserisce i dati dal nuovo leader, inclusi i dati persi. Pertanto, la risposta è no, non è consigliato. Ciò potrebbe causare problemi come:

- L'interrogazione di un count in PromQL può restituire un valore superiore al previsto durante il periodo di elezione di un nuovo leader.
- Il numero di `active series` aumenta durante il periodo di elezione di un nuovo leader e raggiunge il `active series limits`. Per ulteriori informazioni, consulta [Quote AMP](#).

Sembra che Kubernetes abbia la propria etichetta di cluster e non stia deduplicando le mie metriche. Come è possibile risolvere il problema?

Una nuova metrica `apiserver_storage_size_bytes` è stata introdotta in Kubernetes 1.28, con un'etichetta `cluster`. Ciò può causare problemi di deduplicazione in Amazon Managed Service for Prometheus, che dipende dall'etichetta `cluster`. In Kubernetes 1.3, l'etichetta viene rinominata in `storage-cluster_id` (viene rinominata anche nelle patch successive 1.28 e 1.29). Se il tuo cluster emette questa metrica con l'etichetta `cluster`, Amazon Managed Service for Prometheus non può deduplicare le serie temporali associate. Ti consigliamo di aggiornare il tuo cluster Kubernetes all'ultima versione con patch per evitare questo problema. In alternativa, puoi rietichettare l'etichetta sulla tua `apiserver_storage_size_bytes` metrica prima di inserirla in Amazon Managed Service for Prometheus.

### Note

Per maggiori dettagli sulla modifica a Kubernetes, consulta [Rename Label cluster to storage\\_cluster\\_id](#) per la metrica `apiserver_storage_size_bytes` nel progetto Kubernetes. [GitHub](#)

## Disponibilità interregionale

Per aggiungere la disponibilità interregionale ai tuoi dati, puoi inviare metriche a più AWS aree di lavoro in diverse regioni. Prometheus supporta sia più scrittori che la scrittura interregionale.

L'esempio seguente mostra come configurare un server Prometheus in esecuzione in modalità Agente per inviare parametri a due aree di lavoro in regioni diverse con Helm.

```
extensions:
  sigv4auth:
    service: "aps"

receivers:
  prometheus:
    config:
      scrape_configs:
        - job_name: 'kubernetes-kubelet'
          scheme: https
          tls_config:
            ca_file: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
```

```
    insecure_skip_verify: true
    bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
    kubernetes_sd_configs:
      - role: node
    relabel_configs:
      - action: labelmap
        regex: __meta_kubernetes_node_label_(.+)
      - target_label: __address__
        replacement: kubernetes.default.svc.cluster.local:443
      - source_labels: [__meta_kubernetes_node_name]
        regex: (.+)
        target_label: __metrics_path__
        replacement: /api/v1/nodes/${1}/proxy/metrics

exporters:
  prometheusremotewrite/one:
    endpoint: "https://aps-workspaces.workspace_1_region.amazonaws.com/workspaces/
ws-workspace_1_id/api/v1/remote_write"
    auth:
      authenticator: sigv4auth
  prometheusremotewrite/two:
    endpoint: "https://aps-workspaces.workspace_2_region.amazonaws.com/workspaces/
ws-workspace_2_id/api/v1/remote_write"
    auth:
      authenticator: sigv4auth

service:
  extensions: [sigv4auth]
  pipelines:
    metrics/one:
      receivers: [prometheus]
      exporters: [prometheusremotewrite/one]
    metrics/two:
      receivers: [prometheus]
      exporters: [prometheusremotewrite/two]
```

# Esegui una ricerca sui parametri Prometheus

Ora che i parametri vengono inseriti nell'area di lavoro, puoi interrogarli. Puoi usare un servizio come Grafana per interrogare i parametri oppure puoi usare le API di Amazon Managed Service per Prometheus.

Le interrogazioni vengono eseguite utilizzando Prometheus, il linguaggio di interrogazione standard di Prometheus, PromQL. Per ulteriori informazioni su PromQL e sulla sua sintassi, consulta [Interrogazione a Prometheus](#) nella documentazione di Prometheus.

## Argomenti

- [Protezione delle interrogazioni dei parametri](#)
- [Configurazione di Grafana gestito da Amazon per l'utilizzo con il servizio gestito da Amazon per Prometheus](#)
- [Configurazione di Grafana open source o Grafana Enterprise per l'utilizzo con il servizio gestito da Amazon per Prometheus](#)
- [Interrogazione tramite Grafana in esecuzione in un cluster Amazon EKS](#)
- [Interrogazione tramite API compatibili con Prometheus](#)
- [Informazioni sulle statistiche nella risposta di interrogazione dell'API](#)

## Protezione delle interrogazioni dei parametri

Il servizio gestito da Amazon per Prometheus offre modi per aiutarti a rendere sicura l'interrogazione dei tuoi parametri.

## Utilizzo AWS PrivateLink con Amazon Managed Service for Prometheus

Il traffico di rete per l'interrogazione delle metriche in Amazon Managed Service for Prometheus può essere eseguito su un endpoint Internet pubblico o tramite un endpoint VPC. AWS PrivateLink. Quando lo utilizzi AWS PrivateLink, il traffico di rete proveniente dai tuoi VPC è protetto all'interno della rete senza passare attraverso la rete Internet pubblica. AWS Per creare un endpoint AWS PrivateLink VPC per Amazon Managed Service for Prometheus, consulta [Utilizzo di Amazon Managed Service for Prometheus con endpoint VPC di interfaccia](#)

## Autenticazione e autorizzazione

AWS Identity and Access Management è un servizio web che ti aiuta a controllare in modo sicuro l'accesso alle risorse. AWS Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse. Il servizio gestito da Amazon per Prometheus si integra con IAM per aiutarti a proteggere i tuoi dati. Quando configuri Amazon Managed Service per Prometheus, dovrai creare alcuni ruoli IAM che consentano ai server Grafana di interrogare i parametri archiviati nelle aree di lavoro del servizio gestito da Amazon per Prometheus. Per ulteriori informazioni su IAM, consulta [Che cos'è IAM?](#)

Un'altra funzionalità AWS di sicurezza che può aiutarti a configurare Amazon Managed Service per Prometheus è AWS il processo di firma Signature Version 4 (SigV4).AWS Signature Version 4 è il processo per aggiungere informazioni di autenticazione alle richieste inviate tramite HTTP. AWS Per motivi di sicurezza, la maggior parte delle richieste AWS deve essere firmata con una chiave di accesso, che consiste in un ID della chiave di accesso e una chiave di accesso segreta. Queste due chiavi in genere vengono definite come le tue credenziali di sicurezza. Per ulteriori informazioni su SigV4, consulta [Processo di firma di Signature versione 4](#).

## Configurazione di Grafana gestito da Amazon per l'utilizzo con il servizio gestito da Amazon per Prometheus

Amazon Managed Grafana è un servizio completamente gestito per Grafana open source che semplifica la connessione a ISV open source di terze parti AWS e servizi per la visualizzazione e l'analisi delle fonti di dati su larga scala.

Il servizio gestito da Amazon per Prometheus supporta l'utilizzo di Grafana gestito da Amazon per interrogare i parametri in un'area di lavoro. Nella console Grafana gestito da Amazon, puoi aggiungere un'area di lavoro del servizio gestito da Amazon per Prometheus come origine dati scoprendo i tuoi account del servizio gestito da Amazon per Prometheus esistenti. Grafana gestito da Amazon gestisce la configurazione delle credenziali di autenticazione necessarie per accedere al servizio gestito da Amazon per Prometheus. Per istruzioni dettagliate sulla creazione di una connessione al servizio gestito da Amazon per Prometheus da Grafana gestito da Amazon, consulta le istruzioni nella [Guida per l'utente di Grafana gestito da Amazon](#).

Puoi inoltre visualizzare gli avvisi del servizio gestito da Amazon per Prometheus in Grafana gestito da Amazon. Per istruzioni su come configurare l'integrazione con gli avvisi, consulta [Integrazione degli avvisi con Amazon Managed Grafana o Grafana open source](#).

## Connessione ad Grafana gestito da Amazon in un VPC privato

Il servizio gestito da Amazon per Prometheus fornisce un endpoint del servizio a cui Grafana gestito da Amazon può connettersi quando si eseguono interrogazioni su parametri e avvisi.

Puoi configurare Grafana gestito da Amazon per utilizzare un VPC privato (per i dettagli sulla configurazione di un VPC privato a Grafana, consulta [Connessione ad Amazon VPC](#) nella Guida per l'utente di Grafana gestito da Amazon User Guide). A seconda delle impostazioni, questo VPC potrebbe non avere accesso all'endpoint del servizio gestito da Amazon per Prometheus.

Per aggiungere il servizio gestito da Amazon per Prometheus come origine dati a un'area di lavoro Grafana gestito da Amazon configurato per utilizzare uno specifico VPC privato, devi prima connettere il tuo servizio gestito da Amazon per Prometheus allo stesso VPC creando un endpoint VPC. Per maggiori informazioni su come creare un endpoint VPC, consulta [Creazione di un endpoint VPC di interfaccia per Amazon Managed Service per Prometheus](#).

## Configurazione di Grafana open source o Grafana Enterprise per l'utilizzo con il servizio gestito da Amazon per Prometheus

Il servizio gestito da Amazon per Prometheus supporta l'uso di Grafana versione 7.3.5 e successive per interrogare i parametri in un'area di lavoro. Le versioni 7.3.5 e successive includono il supporto per l'autenticazione Signature Version 4 (SigV4). AWS

Per istruzioni sulla configurazione di un Grafana autonomo utilizzando il file tar.gz o zip, consulta [Installazione di Grafana](#) nella documentazione di Grafana. Se installi una nuova Grafana standalone, ti verranno richiesti nome utente e password. Il valore predefinito è **admin/admin**. Ti verrà richiesto di cambiare la password dopo il primo accesso. Per ulteriori informazioni, consulta [Introduzione a Grafana](#) nella documentazione di Grafana.

Per controllare la versione di Grafana, esegui il seguente comando.

```
grafana_install_directory/bin/grafana-server -v
```

Per configurare Grafana in modo che funzioni con Amazon Managed Service for Prometheus, devi accedere a un account con la policy o le AmazonPrometheusQueryAccessautorizzazioni, e. `aps:QueryMetrics` `aps:GetMetricMetadata` `aps:GetSeries` `aps:GetLabels` Per ulteriori informazioni, consulta [Autorizzazioni e policy IAM](#).

## Configurazione di AWS SigV4

Amazon Managed Service for Prometheus funziona AWS Identity and Access Management con (IAM) per proteggere tutte le chiamate alle API Prometheus con credenziali IAM. Per impostazione predefinita, l'origine dati Prometheus in Grafana presuppone che Prometheus non richieda alcuna autenticazione. Per consentire a Grafana di sfruttare le funzionalità di autenticazione e autorizzazione del servizio gestito da Amazon per Prometheus, dovrai abilitare il supporto per l'autenticazione SigV4 nell'origine dati Grafana. Segui i passaggi in questa pagina quando utilizzi un server Grafana open source autogestito o un server aziendale Grafana. Se utilizzi Grafana gestito da Amazon, l'autenticazione SigV4 è completamente automatizzata. Per ulteriori informazioni su Grafana gestito da Amazon, consulta [Cos'è Grafana gestito da Amazon?](#)

Per abilitare SigV4 su Grafana, avvia Grafana con le `AWS_SDK_LOAD_CONFIG` e `GF_AUTH_SIGV4_AUTH_ENABLED` variabili di ambiente e impostate su `true`. La `GF_AUTH_SIGV4_AUTH_ENABLED` variabile di ambiente sovrascrive la configurazione predefinita per Grafana per abilitare il supporto SigV4. Per ulteriori informazioni, consulta [Configurazione](#) nella documentazione di Grafana.

### Linux

Per abilitare SigV4 su un server Grafana standalone su Linux, inserisci i seguenti comandi.

```
export AWS_SDK_LOAD_CONFIG=true
```

```
export GF_AUTH_SIGV4_AUTH_ENABLED=true
```

```
cd grafana_install_directory
```

```
./bin/grafana-server
```

### Windows

Per abilitare SigV4 su una Grafana autonoma su Windows utilizzando il prompt dei comandi di Windows, inserisci i seguenti comandi.

```
set AWS_SDK_LOAD_CONFIG=true
```

```
set GF_AUTH_SIGV4_AUTH_ENABLED=true
```

```
cd grafana_install_directory
```

```
.\bin\grafana-server.exe
```

## Aggiungi l'origine dati Prometheus a Grafana

I passaggi seguenti spiegano come configurare l'origine dati Prometheus a Grafana per interrogare i parametri del servizio gestito da Amazon per Prometheus.

Come aggiungere l'origine dati Prometheus nel server Grafana

1. Apri la console Grafana.
2. In Configurazioni, scegli Origini dati.
3. Scegli Aggiungi origine dati
4. Scegli Prometheus.
5. Per l'URL HTTP, specifica l'URL Endpoint - query visualizzato nella pagina dei dettagli dell'area di lavoro nella console del servizio gestito da Amazon per Prometheus.
6. Nell'URL HTTP che hai appena specificato, rimuovi la `/api/v1/query` stringa aggiunta all'URL, perché l'origine dati Prometheus la aggiungerà automaticamente.

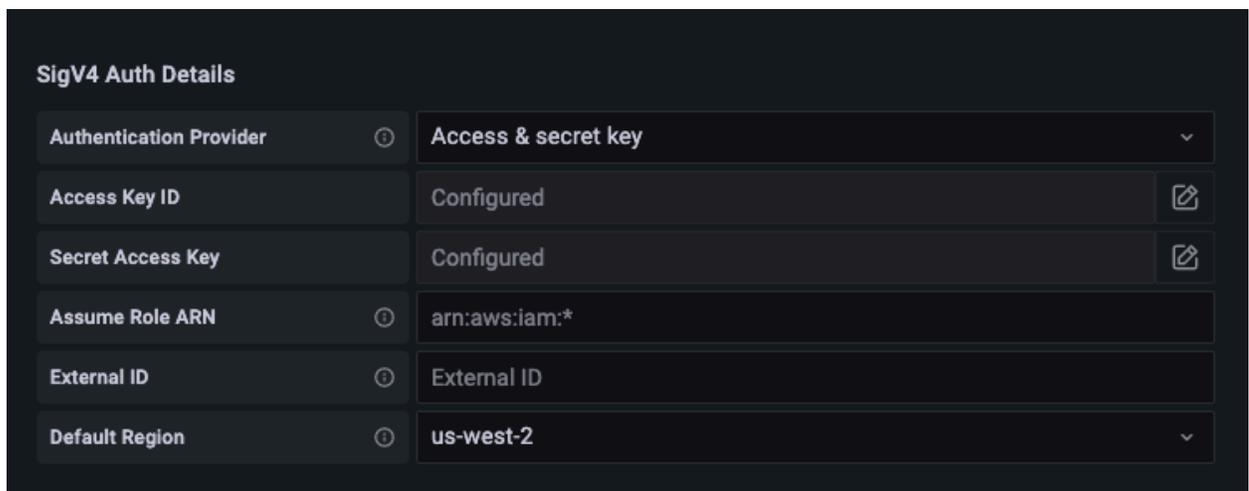
L'URL corretto dovrebbe essere simile all'indirizzo `https://aps-workspaces.us-west-2.amazonaws.com/workspaces/ws-1234a5b6-78cd-901e-2fgh-3i45j6k178l9`.

7. In Autenticazione, seleziona l'interruttore per l'autenticazione SigV4 per abilitarlo.
8. Puoi configurare l'autorizzazione SigV4 specificando le tue credenziali a lungo termine direttamente in Grafana o utilizzando una catena di provider predefinita. Specificando direttamente le credenziali a lungo termine è possibile iniziare più rapidamente e i passaggi seguenti forniscono innanzitutto queste istruzioni. Una volta acquisita maggiore familiarità con l'uso di Grafana con il servizio gestito da Amazon per Prometheus, ti consigliamo di utilizzare una catena di provider predefinita, perché offre maggiore flessibilità e sicurezza. Per ulteriori informazioni sulla configurazione della catena di provider predefinita, consulta [Specificazione delle credenziali](#).
  - Per utilizzare direttamente le tue credenziali a lungo termine, procedi come segue:
    - a. In Dettagli di autenticazione SigV4, per Provider di autenticazione scegli Accesso e chiave segreta.
    - b. Per ID della chiave di accesso, inserisci il tuo AWS ID della chiave di accesso.

- c. Per Chiave di accesso segreta, inserisci la tua AWS chiave di accesso segreta.
- d. Lascia vuoti i campi Assumi ruolo ARN and ID esterno.
- e. Per Regione predefinita, scegli la regione della tua area di lavoro del servizio gestito da Amazon per Prometheus. Questa regione deve corrispondere alla regione contenuta nell'URL che hai elencato nella fase 5.
- f. Seleziona Salva ed esegui test.

Apri il messaggio seguente: l'origine dati funziona

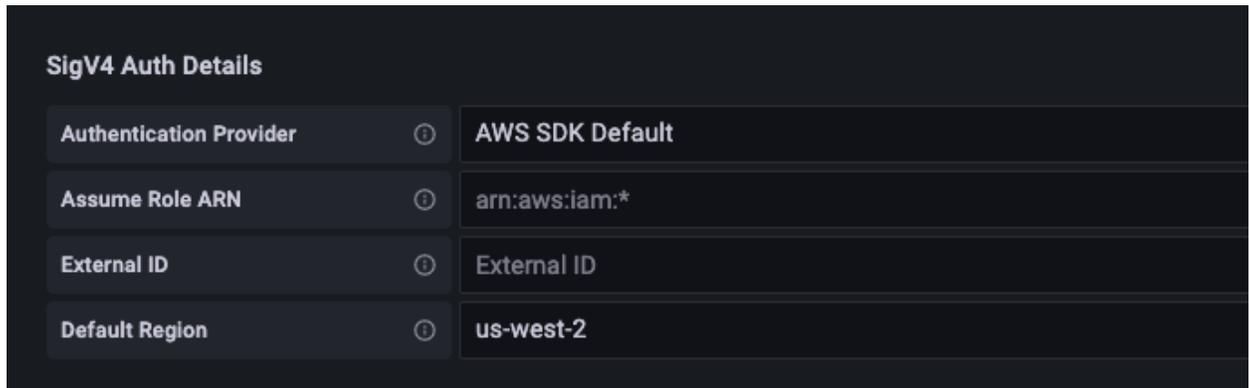
La schermata seguente mostra l'impostazione dei dettagli di autenticazione della chiave di accesso, della chiave segreta SigV4.



- Per utilizzare invece una catena di provider predefinita (consigliata per un ambiente di produzione), procedi come segue:
  - a. In Dettagli di autenticazione SigV4, per Provider di autenticazione seleziona AWS SDK predefinito.
  - b. Lascia vuoti i campi Assumi ruolo ARN and ID esterno.
  - c. Per Regione predefinita, scegli la regione della tua area di lavoro del servizio gestito da Amazon per Prometheus. Questa regione deve corrispondere alla regione contenuta nell'URL che hai elencato nella fase 5.
  - d. Seleziona Salva ed esegui test.

Apri il messaggio seguente: l'origine dati funziona

L'immagine seguente mostra l'impostazione di dettaglio di autenticazione SigV4 predefinita SDK.



The screenshot shows a configuration panel titled "SigV4 Auth Details" with a dark background. It contains four rows of configuration items, each with a label, an information icon, and a value:

SigV4 Auth Details		
Authentication Provider	ⓘ	AWS SDK Default
Assume Role ARN	ⓘ	arn:aws:iam:*
External ID	ⓘ	External ID
Default Region	ⓘ	us-west-2

9. Prova un'interrogazione PromQL sulla nuova origine dati:
  - a. Scegli Esplora.
  - b. Esegui un'interrogazione PromQL di esempio come:

```
prometheus_tsdb_head_series
```

## Risoluzione dei problemi se l'opzione Salva ed esegui test non funziona

Nella procedura precedente, se visualizzi un errore quando scegli Salva ed esegui test, verifica quanto segue.

Errore HTTP non trovato

Assicurati che l'ID dell'area di lavoro nell'URL sia corretto.

Errore HTTP vietato

Questo errore indica che le credenziali non sono valide. Verifica quanto segue:

- Verifica che la regione specificata in Regione predefinita sia corretta.
- Controlla le tue credenziali per eventuali errori di battitura.
- Assicurati che la credenziale che stai utilizzando abbia la policy. `AmazonPrometheusQueryAccess`  
Per ulteriori informazioni, consulta [Autorizzazioni e policy IAM](#).
- Assicurati che la credenziale che stai utilizzando abbia accesso a questa area di lavoro del servizio gestito da Amazon per Prometheus.

Errore HTTP: Bad Gateway

Guarda il log del server Grafana per risolvere questo errore. Per ulteriori informazioni, consulta [Risoluzione dei problemi](#) nella documentazione di Grafana.

Se vedi **Error http: proxy error: NoCredentialProviders: no valid providers in chain**, la catena di provider di credenziali predefinita non è riuscita a trovare una AWS credenziale valida da utilizzare. Assicurati di aver impostato le credenziali come documentato in [Specificazione delle credenziali](#). Se desideri utilizzare una configurazione condivisa, assicurati che l'`AWS_SDK_LOAD_CONFIG` ambiente sia impostato su `true`.

## Interrogazione tramite Grafana in esecuzione in un cluster Amazon EKS

Il servizio gestito da Amazon per Prometheus supporta l'uso di Grafana versione 7.3.5 e successive per interrogare i parametri in un'area di lavoro del servizio gestito da Amazon per Prometheus. Le versioni 7.3.5 e successive includono il supporto per l'autenticazione AWS Signature Version 4 (SigV4).

Per configurare Grafana in modo che funzioni con Amazon Managed Service for Prometheus, devi accedere a un account con la policy o le AmazonPrometheusQueryAccess autorizzazioni, e. `aps:QueryMetrics` `aps:GetMetricMetadata` `aps:GetSeries` `aps:GetLabels` Per ulteriori informazioni, consulta [Autorizzazioni e policy IAM](#).

### AWS Configura SigV4

Grafana ha aggiunto una nuova funzionalità per supportare l'autenticazione AWS Signature Version 4 (SigV4). Per ulteriori informazioni, consulta [Processo di firma di Signature versione 4](#). Questa funzionalità non è abilitata in Grafana per impostazione predefinita. Le seguenti istruzioni per abilitare questa funzionalità presuppongono che tu stia utilizzando Helm per distribuire Grafana su un cluster Kubernetes.

Per abilitare SigV4 sul tuo server Grafana 7.3.5 o una versione successiva

1. Crea un nuovo file di aggiornamento per sovrascrivere la configurazione Grafana e assegnagli un nome `amp_query_override_values.yaml`.
2. Incolla il seguente contenuto nel file e salva il file. Sostituisci `account-id` con l'ID dell' AWS account su cui è in esecuzione il server Grafana.

```
serviceAccount:
```

```
name: "amp-iamproxy-query-service-account"
annotations:
  eks.amazonaws.com/role-arn: "arn:aws:iam::account-id:role/amp-iamproxy-
query-role"
grafana.ini:
  auth:
    sigv4_auth_enabled: true
```

In quel contenuto del file YAML, `amp-iamproxy-query-role` c'è il nome del ruolo che creerai nella sezione successiva, [Imposta ruoli IAM per gli account del servizio](#). Puoi sostituire questo ruolo con il tuo nome se hai già creato un ruolo per interrogare la tua area di lavoro.

Utilizzerai questo file più tardi, in [Aggiorna il server Grafana utilizzando Helm](#).

## Imposta ruoli IAM per gli account del servizio

Se utilizzi un server Grafana in un cluster Amazon EKS, ti consigliamo di utilizzare i ruoli IAM per gli account del servizio, noti anche come ruoli di servizio, per il controllo degli accessi. Quando esegui questa operazione per associare un ruolo IAM a un account di servizio Kubernetes, l'account di servizio può quindi fornire AWS le autorizzazioni ai contenitori in qualsiasi pod che utilizza quell'account di servizio. Per ulteriori informazioni, consulta [Ruoli IAM per gli account del servizio](#).

Se non hai già impostato questi ruoli di servizio per l'interrogazione, segui le istruzioni riportate [Imposta ruoli IAM per gli account di servizio per le domande delle metriche](#) per configurare i ruoli.

È quindi necessario aggiungere l'account del servizio Grafana nelle condizioni del rapporto di fiducia.

Come aggiungere l'account del servizio Grafana nelle condizioni del rapporto di fiducia

1. Da una finestra del terminale, determina il namespace e il nome dell'account del servizio per il tuo server Grafana. Ad esempio, puoi utilizzare il seguente comando.

```
kubectl get serviceaccounts -n grafana_namespace
```

2. Nella console Amazon EKS, apri il ruolo IAM per gli account del servizio associati al cluster EKS.
3. Seleziona Modifica relazione di attendibilità.
4. Aggiorna la Condizione per includere il namespace Grafana e il nome dell'account del servizio Grafana che hai trovato nell'output del comando nella fase 1. Di seguito è riportato un esempio.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Federated": "arn:aws:iam::account-id:oidc-provider/
oidc.eks.aws_region.amazonaws.com/id/openid"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "oidc.eks.region.amazonaws.com/id/openid:sub": [
          "system:serviceaccount:aws-amp:amp-iamproxy-query-service-account",
          "system:serviceaccount:grafana-namespace:grafana-service-account-name"
        ]
      }
    }
  }
]
}

```

5. Scegliere Update trust Policy (Aggiorna policy di attendibilità).

## Aggiorna il server Grafana utilizzando Helm

Questo passaggio aggiorna il server Grafana per utilizzare le voci aggiunte al file `amp_query_override_values.yaml` nella sezione precedente.

Esegui i comandi seguenti. Per ulteriori informazioni sui grafici Helm per Grafana, consulta [Grafici Helm Grafana Community Kubernetes](#).

```
helm repo add grafana https://grafana.github.io/helm-charts
```

```
helm upgrade --install grafana grafana/grafana -n grafana_namespace -f ./
amp_query_override_values.yaml
```

## Aggiungi l'origine dati Prometheus a Grafana

I passaggi seguenti spiegano come configurare l'origine dati Prometheus a Grafana per interrogare i parametri del servizio gestito da Amazon per Prometheus.

## Come aggiungere l'origine dati Prometheus nel server Grafana

1. Apri la console Grafana.
2. In Configurazioni, scegli Origini dati.
3. Scegli Aggiungi origine dati
4. Scegli Prometheus.
5. Per l'URL HTTP, specifica l'URL Endpoint - query visualizzato nella pagina dei dettagli dell'area di lavoro nella console del servizio gestito da Amazon per Prometheus.
6. Nell'URL HTTP che hai appena specificato, rimuovi la `/api/v1/query` stringa aggiunta all'URL, perché l'origine dati Prometheus la aggiungerà automaticamente.
7. In Autenticazione, seleziona l'interruttore per l'autenticazione SigV4 per abilitarlo.

Lascia vuoti i campi Assumi ruolo ARN and ID esterno. Quindi, per Regione predefinita, seleziona la regione in cui si trova l'area di lavoro del servizio gestito da Amazon per Prometheus.

8. Seleziona Salva ed esegui test.

Apri il messaggio seguente: l'origine dati funziona

9. Prova un'interrogazione PromQL sulla nuova origine dati:
  - a. Scegli Esplora.
  - b. Esegui un'interrogazione PromQL di esempio come:

```
prometheus_tsdb_head_series
```

## Interrogazione tramite API compatibili con Prometheus

Sebbene utilizzare uno strumento come [Grafana gestito da Amazon](#) sia il modo più semplice per visualizzare e interrogare i parametri, il servizio gestito da Amazon per Prometheus supporta anche diverse API compatibili con Prometheus che puoi utilizzare per interrogare i tuoi parametri. Per ulteriori informazioni su tutte le API compatibili con Prometheus disponibili, consulta [API compatibili con Prometheus](#).

Quando utilizzi queste API per interrogare le tue metriche, le richieste devono essere firmate con il processo di firma Signature Version 4. AWS Puoi configurare [AWS Signature Version 4](#) per semplificare il processo di firma. Per ulteriori informazioni, consulta [aws-sigv4-proxy](#).

La firma tramite il proxy AWS SigV4 può essere eseguita utilizzando `awscurl`. L'argomento seguente [Uso di awscurl per interrogare le API compatibili con Prometheus](#), illustra come `awscurl` configurare AWS SigV4.

## Utilizzo di awscurl per interrogare le API compatibili con Prometheus

Le richieste API per il servizio gestito da Amazon per Prometheus devono essere firmate con [SigV4](#). Puoi usare [awscurl](#) per semplificare il processo di interrogazione.

Per l'installazione `awscurl`, è necessario che Python 3 e il gestore di pacchetti pip siano installati.

Su un'istanza basata su Linux, viene installato il seguente comando `awscurl`.

```
$ pip3 install awscurl
```

Su un computer macOS, viene installato il seguente comando `awscurl`.

```
$ brew install awscurl
```

L'esempio seguente è una query di esempio `awscurl`. Sostituisci gli input *Region*, *Workspace-ID* e *QUERY* con i valori appropriati per il tuo caso d'uso:

```
# Define the Prometheus query endpoint URL. This can be found in the Amazon Managed
  Service for Prometheus console page
# under the respective workspace.

$ export AMP_QUERY_ENDPOINT=https://aps-workspaces.Region.amazonaws.com/
workspaces/Workspace-id/api/v1/query

# credentials are inferred from the default profile
$ awscurl -X POST --region Region \
          --service aps "${AMP_QUERY_ENDPOINT}" -d 'query=QUERY' --header
'Content-Type: application/x-www-form-urlencoded'
```

### Note

La stringa di query deve essere codificata con URL.

Per una query come `query=up`, potresti ottenere risultati come:

```
{
  "status": "success",
  "data": {
    "resultType": "vector",
    "result": [
      {
        "metric": {
          "__name__": "up",
          "instance": "localhost:9090",
          "job": "prometheus",
          "monitor": "monitor"
        },
        "value": [
          1652452637.636,
          "1"
        ]
      },
    ]
  }
}
```

`awscurl` Per firmare le richieste fornite, è necessario passare le credenziali valide in uno dei seguenti modi:

- Fornisci l'ID chiave di accesso e la chiave segreta per il ruolo IAM. Puoi trovare la chiave di accesso e la chiave segreta per il ruolo all'indirizzo <https://console.aws.amazon.com/iam/>.

Per esempio:

```
$ export AMP_QUERY_ENDPOINT=https://aps-workspaces.Region.amazonaws.com/
workspaces/Workspace_id/api/v1/query

$ awscurl -X POST --region <Region> \
          --access_key <ACCESS_KEY> \
          --secret_key <SECRET_KEY> \
          --service aps "$AMP_QUERY_ENDPOINT?query=<QUERY>"
```

- Fai riferimento ai file di configurazione memorizzati nei file `/aws/config` e `.aws/credentials`. Puoi anche scegliere di specificare il nome del profilo da utilizzare. Se non specificato, verrà utilizzato il `default` file. Per esempio:

```
$ export AMP_QUERY_ENDPOINT=https://aps-workspaces.<Region>.amazonaws.com/workspaces/
<Workspace_ID>/api/v1/query
$ awscur1 -X POST --region <Region> \
           --profile <PROFILE_NAME>
           --service aps "$AMP_QUERY_ENDPOINT?query=<QUERY>"
```

- Sostituzione del profilo dell'istanza associato all'istanza EC2.

## Esecuzione di richieste di interrogazione utilizzando il contenitore awscur1

Quando non è possibile installare una versione diversa di Python e le dipendenze associate, è possibile utilizzare un contenitore per impacchettare l'`awscur1` applicazione e le sue dipendenze. L'esempio seguente utilizza un runtime Docker per la distribuzione `awscur1`, ma qualsiasi runtime e immagine conformi a OCI funzioneranno.

```
$ docker pull okigan/awscur1
$ export AMP_QUERY_ENDPOINT=https://aps-workspaces.<Region>.amazonaws.com/
workspaces/<Workspace_id>/api/v1/query
$ docker run --rm -it okigan/awscur1 --access_key $AWS_ACCESS_KEY_ID --secret_key
$AWS_SECRET_ACCESS_KEY \ --region <Region> --service aps "$AMP_QUERY_ENDPOINT?
query=<QUERY>"
```

## Informazioni sulle statistiche nella risposta di interrogazione dell'API

I [prezzi](#) delle interrogazioni si basano sul numero totale di esempi di interrogazioni elaborate in un mese a partire dalle interrogazioni eseguite. La risposta all'interrogazione per una query o un'queryRangeAPI include i dati statistici sugli esempi di interrogazioni elaborate. Quando il parametro di interrogazione `stats=all` viene inviato nella richiesta, viene creato un `samples` oggetto nell'`stats` oggetto e i `stats` dati vengono restituiti nella risposta.

L'oggetto `samples` ha i seguenti attributi:

Attributo	Descrizione
<code>totalQueryableSamples</code>	Numero totale di esempi di interrogazioni elaborate. Queste sono le informazioni da utilizzare per la fatturazione.

Attributo	Descrizione
<code>totalQueryableSamplesPerStep</code>	Il numero totale di esempi di interrogazioni elaborate per ogni fase. È strutturato come un array di array con il timestamp in epoch e il numero di campioni caricati nella fase specifica.

Di seguito sono riportate le richieste e le risposte di esempio che includono le stats informazioni contenute nella risposta:

Esempio per query:

GET

```
endpoint/api/v1/query?query=up&time=1652382537&stats=all
```

Risposta

```
{
  "status": "success",
  "data": {
    "resultType": "vector",
    "result": [
      {
        "metric": {
          "__name__": "up",
          "instance": "localhost:9090",
          "job": "prometheus"
        },
        "value": [
          1652382537,
          "1"
        ]
      }
    ],
    "stats": {
      "timings": {
        "evalTotalTime": 0.00453349,
        "resultSortTime": 0,
        "queryPreparationTime": 0.000019363,
        "innerEvalTime": 0.004508405,

```

```

        "execQueueTime": 0.000008786,
        "execTotalTime": 0.004554219
    },
    "samples": {
        "totalQueryableSamples": 1,
        "totalQueryableSamplesPerStep": [
            [
                1652382537,
                1
            ]
        ]
    }
}
}
}

```

Esempio per `queryRange`:

GET

```

endpoint/api/v1/query_range?query=sum+%28rate+%28go_gc_duration_seconds_count%5B1m%5D%29%29&start=1652382537&end=1652384705&step=1000&stats=all

```

Risposta

```

{
  "status": "success",
  "data": {
    "resultType": "matrix",
    "result": [
      {
        "metric": {},
        "values": [
          [
            1652383000,
            "0"
          ],
          [
            1652384000,
            "0"
          ]
        ]
      }
    ]
  }
}

```

```
],
  "stats": {
    "samples": {
      "totalQueryableSamples": 8,
      "totalQueryableSamplesPerStep": [
        [
          1652382000,
          0
        ],
        [
          1652383000,
          4
        ],
        [
          1652384000,
          4
        ]
      ]
    }
  }
}
```

# Regole di registrazione e regole di avviso

Il servizio gestito da Amazon per Prometheus supporta due tipi regole che valuta a intervalli regolari:

- Le regole di registrazione consentono di precalcolare le espressioni più necessarie o che richiedono risorse computazionalmente costose e di salvarne i risultati in un nuovo set di serie temporali. L'interrogazione del risultato precalcolato è spesso molto più veloce rispetto all'esecuzione dell'espressione originale ogni volta che è necessario.
- Le regole di avviso consentono di definire le condizioni di avviso in base a PromQL e a una soglia. Quando la regola attiva la soglia, viene inviata una notifica ad alert manager, che inoltra la notifica a valle a destinatari come Amazon Simple Notification Service.

Per utilizzare le regole nel servizio gestito da Amazon per Prometheus, devi creare uno o più file di regole YAML che definiscono le regole. Un file delle regole del servizio gestito da Amazon per Prometheus ha lo stesso formato di un file di regole nella versione standalone di Prometheus. Per ulteriori informazioni, vedere [Definizione delle regole di registrazione](#) e delle [regole di avviso](#) nella documentazione di Prometheus.

È possibile avere più file di regole in un'area di lavoro. Ogni file di regole separato è contenuto in un namespace separato. La presenza di più file di regole consente di importare file di regole di Prometheus esistenti in un'area di lavoro senza doverli modificare o combinare. Namespace di gruppi di regole diversi possono avere anche tag diversi.

## Sequenza di regole

All'interno di un file di regole, le regole sono contenute all'interno di gruppi di regole. Le regole all'interno di un singolo gruppo di regole in un file di regole vengono sempre valutate in ordine dall'alto verso il basso. Pertanto, nelle regole di registrazione, il risultato di una regola di registrazione può essere utilizzato nel calcolo di una regola di registrazione successiva o in una regola di avviso nello stesso gruppo di regole. Tuttavia, poiché non è possibile specificare l'ordine in cui eseguire file di regole separati, non è possibile utilizzare i risultati di una regola di registrazione per calcolare una regola in un gruppo di regole diverso o in un file di regole diverso.

## Argomenti

- [Autorizzazioni IAM necessarie](#)
- [Creazione di un file di regole](#)

- [Caricamento di un file di configurazione delle regole nel servizio gestito da Amazon per Prometheus](#)
- [Modifica di un file di configurazione delle regole](#)
- [Risoluzione dei problemi per ruler](#)

## Autorizzazioni IAM necessarie

Devi concedere agli utenti le autorizzazioni per utilizzare le regole nel servizio gestito da Amazon per Prometheus. Crea una policy AWS Identity and Access Management (IAM) con le seguenti autorizzazioni e assegnala ai tuoi utenti, gruppi o ruoli.

### Note

Per ulteriori informazioni su IAM, consulta [Identity and Access Management per il servizio gestito da Amazon per Prometheus](#).

### Policy per concedere l'accesso alle regole d'uso

La seguente policy consente di accedere alle regole di utilizzo per tutte le risorse del tuo account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps: CreateRuleGroupsNamespace",
        "aps: ListRuleGroupsNamespaces",
        "aps: DescribeRuleGroupsNamespace",
        "aps: PutRuleGroupsNamespace",
        "aps: DeleteRuleGroupsNamespace",
      ],
      "Resource": "*"
    }
  ]
}
```

### Policy per consentire l'accesso a un solo namespace

È inoltre possibile creare una policy che consenta l'accesso solo a politiche specifiche. La seguente policy di esempio consente l'accesso solo alle policy RuleGroupNamespace specificate. Per utilizzare questa policy, sostituisci *<account>*, *<region>*, *<workspace-id>* e *<namespace-name>* con i valori appropriati per il tuo account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps:ListRules",
        "aps:ListTagsForResource",
        "aps:GetLabels",
        "aps:CreateRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:DescribeRuleGroupsNamespace",
        "aps:PutRuleGroupsNamespace",
        "aps>DeleteRuleGroupsNamespace"
      ],
      "Resource": [
        "arn:aws:aps:*:<account>:workspace/*",
        "arn:aws:aps:<region>:<account>:rulegroupnamespace/<workspace-id>/<namespace-name>"
      ]
    }
  ]
}
```

## Creazione di un file di regole

Per utilizzare le regole nel servizio gestito da Amazon per Prometheus, devi creare un file di regole che definisce le regole. Un file delle regole del servizio gestito da Amazon per Prometheus ha lo stesso formato di un file di regole nella versione standalone di Prometheus. Per ulteriori informazioni, consulta [Regole di registrazione](#) e [Regole di avviso](#).

Di seguito è riportato un esempio di un file di regole:

```
groups:
  - name: test
    rules:
```

```
- record: metric:recording_rule
  expr: avg(rate(container_cpu_usage_seconds_total[5m]))
- name: alert-test
  rules:
  - alert: metric:alerting_rule
    expr: avg(rate(container_cpu_usage_seconds_total[5m])) > 0
    for: 2m
```

Per altri esempi di regole di avviso, consulta [Esempi di regole di avviso](#).

### Note

Puoi creare un file di definizione delle regole localmente e poi caricarlo su Amazon Managed Service for Prometheus oppure puoi creare, modificare e caricare la definizione direttamente all'interno della console Amazon Managed Service for Prometheus. In entrambi i casi, si applicano le stesse regole di formattazione. Per ulteriori informazioni sul caricamento e la modifica del file, consulta [Caricamento di un file di configurazione delle regole nel servizio gestito da Amazon per Prometheus](#)

## Caricamento di un file di configurazione delle regole nel servizio gestito da Amazon per Prometheus

Una volta individuate le modifiche da apportare al file di configurazione delle regole, puoi modificarlo all'interno della console oppure caricare un file sostitutivo con la console o AWS CLI.

### Note

Se utilizzi un cluster Amazon EKS, puoi anche caricare un file di configurazione delle regole utilizzando [AWS Controllers for Kubernetes](#).

Per utilizzare la console Amazon Managed Service for Prometheus per modificare o sostituire la configurazione delle regole e creare lo spazio dei nomi

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.

2. Nell'angolo in alto a sinistra della pagina, scegli l'icona del menu, quindi scegli Tutte le aree di lavoro.
3. Scegli l'ID dell'area di lavoro, quindi scegli la scheda Gestione delle regole.
4. Scegli Aggiungi namespace.
5. Seleziona Scegli file e seleziona il file di definizione delle regole.

In alternativa, puoi creare e modificare un file di definizione delle regole direttamente nella console Amazon Managed Service for Prometheus selezionando Definisci configurazione. Questo creerà un file di definizione predefinito di esempio che modificherai prima del caricamento.

6. (Facoltativo) Per aggiungere tag al namespace, scegli Aggiungi nuovo tag.

Poi, per Chiave, inserire un nome per il tag. È possibile aggiungere un valore facoltativo al tag in Value (Valore).

Per aggiungere un altro tag, scegli Aggiungi nuovo tag.

7. Scegli Continua. Il servizio gestito da Amazon per Prometheus crea un nuovo namespace con lo stesso nome del file delle regole che hai selezionato.

Da utilizzare per AWS CLI caricare una configurazione di Alert Manager in un'area di lavoro in un nuovo spazio dei nomi

1. Base64 codifica il contenuto del tuo file di alert manager. In Linux, puoi utilizzare il seguente comando:

```
base64 input-file output-file
```

In macOS, puoi utilizzare il seguente comando:

```
openssl base64 input-file output-file
```

2. Inserisci uno dei comandi seguenti per creare il namespace e caricare il file.

Nella AWS CLI versione 2, inserisci:

```
aws amp create-rule-groups-namespace --data file://path_to_base_64_output_file --  
name namespace-name --workspace-id my-workspace-id --region region
```

Nella AWS CLI versione 1, inserisci:

```
aws amp create-rule-groups-namespace --data fileb://path_to_base_64_output_file --  
name namespace-name --workspace-id my-workspace-id --region region
```

3. Sono necessari alcuni secondi per rendere attiva la configurazione di alert manager. Per controllare lo stato, immetti il comando seguente:

```
aws amp describe-rule-groups-namespace --workspace-id workspace_id --  
name namespace-name --region region
```

In caso status affermativo ACTIVE, il file delle regole ha avuto effetto.

## Modifica di un file di configurazione delle regole

Puoi caricare un nuovo file di regole per sostituire una configurazione esistente oppure modificare la configurazione corrente direttamente nella console. Facoltativamente, puoi scaricare il file corrente, modificarlo in un editor di testo, quindi caricare la nuova versione.

Per utilizzare la console del servizio gestito da Amazon per Prometheus per modificare la configurazione delle regole

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nell'angolo in alto a sinistra della pagina, scegli l'icona del menu, quindi scegli Tutte le aree di lavoro.
3. Scegli l'ID dell'area di lavoro, quindi scegli la scheda Gestione delle regole.
4. Seleziona il nome del file di configurazione delle regole che desideri modificare.
5. (Facoltativo) Se desideri scaricare il file di configurazione delle regole corrente, scegli Scarica o Copia.
6. Scegliete Modifica per modificare la configurazione direttamente all'interno della console. Al termine, scegli Salva.

In alternativa, puoi scegliere Sostituisci configurazione per caricare un nuovo file di configurazione. In tal caso, seleziona il nuovo file di definizione delle regole e scegli Continua per caricarlo.

## Per utilizzarlo AWS CLI per modificare un file di configurazione delle regole

1. Base64 codifica il contenuto del file delle regole. In Linux, puoi utilizzare il seguente comando:

```
base64 input-file output-file
```

In macOS, puoi utilizzare il seguente comando:

```
openssl base64 input-file output-file
```

2. Utilizza uno dei comandi seguenti per caricare il nuovo file.

Nella AWS CLI versione 2, inserisci:

```
aws amp put-rule-groups-namespace --data file://path_to_base_64_output_file --  
name namespace-name --workspace-id my-workspace-id --region region
```

Nella AWS CLI versione 1, inserisci:

```
aws amp put-rule-groups-namespace --data fileb://path_to_base_64_output_file --  
name namespace-name --workspace-id my-workspace-id --region region
```

3. Sono necessari alcuni secondi per rendere attivo il file delle regole. Per controllare lo stato, immetti il comando seguente:

```
aws amp describe-rule-groups-namespace --workspace-id workspace_id --  
name namespace-name --region region
```

In caso status affermativo ACTIVE, il file delle regole ha avuto effetto. Fino ad allora, la versione precedente di questo file di regole è ancora attiva.

## Risoluzione dei problemi per ruler

Utilizzando [CloudWatch Registri](#), è possibile risolvere i problemi relativi ad Alert Manager e Ruler. Questa sezione contiene argomenti relativi alla risoluzione dei problemi relativi al ruler.

Quando il registro contiene il seguente errore di errore del ruler

```
{
```



# Alert Manager

Quando le [regole di avviso](#) eseguite dal servizio gestito da Amazon per Prometheus sono attive, alert manager gestisce gli avvisi inviati. Deduplica, raggruppa e indirizza gli avvisi ai ricevitori downstream. Il servizio gestito da Amazon per Prometheus supporta solo Amazon Simple Notification Service come ricevitore e può indirizzare i messaggi verso argomenti di Amazon SNS nello stesso account. Puoi anche utilizzare alert manager per silenziare e inibire gli avvisi.

alert manager offre funzionalità simili a Alertmanager di Prometheus.

È possibile utilizzare il file di configurazione di alert manager per quanto segue:

- **Raggruppamento:** il raggruppamento raccoglie avvisi simili in un'unica notifica. Ciò è particolarmente utile durante le interruzioni più ampie, quando molti sistemi si guastano contemporaneamente e centinaia di avvisi potrebbero essere attivati contemporaneamente. Ad esempio, supponiamo che un errore di rete provochi il malfunzionamento di molti nodi contemporaneamente. Se questi tipi di avvisi sono raggruppati, alert manager invia un'unica notifica.

Il raggruppamento degli avvisi e la tempistica delle notifiche raggruppate sono configurati da un albero di routing nel file di configurazione di alert manager. Per ulteriori informazioni, consulta [<route>](#)

- **Inibizione:** l'inibizione sopprime le notifiche per determinati avvisi se altri avvisi sono già attivi. Ad esempio, se viene emesso un avviso relativo all'irraggiungibile di un cluster, è possibile configurare l>alert manager per disattivare tutti gli altri avvisi relativi a questo cluster. In questo modo si evitano le notifiche relative a centinaia o migliaia di avvisi di attivazione non correlati al problema reale. Per ulteriori informazioni su come scrivere le regole di inibizione, consulta [<inhibit\\_rule>](#).
- **Silenzi:** disattiva gli avvisi di silenziamento per un periodo di tempo specificato, ad esempio durante una finestra di manutenzione. Gli avvisi in arrivo vengono controllati per verificare se corrispondono a tutti i parametri di uguaglianza o di espressione regolare di un silenzio attivo. In caso affermativo, non viene inviata alcuna notifica per quell'avviso.

Per creare silenziare, si utilizza l'`PutAlertManagerSilencesAPI`. Per ulteriori informazioni, consulta [PutAlertManagerSilences](#).

## Modello Prometheus

La versione standalone di Prometheus supporta la creazione di modelli, utilizzando file modello di separazione. I modelli possono utilizzare condizionali e formattare dati, tra le altre cose.

[In Amazon Managed Service for Prometheus, inserisci il modello nello stesso file di configurazione del gestore degli avvisi della configurazione del gestore degli avvisi.](#)

## Argomenti

- [Autorizzazioni IAM necessarie](#)
- [Creazione di un file di configurazione di alert manager](#)
- [Configurazione del ricevitore di avvisi](#)
- [Caricamento del file di configurazione di alert manager per il servizio gestito da Amazon per Prometheus](#)
- [Integrazione degli avvisi con Amazon Managed Grafana o Grafana open source](#)
- [Risoluzione dei problemi di alert manager](#)

## Autorizzazioni IAM necessarie

Devi concedere agli utenti le autorizzazioni per utilizzare le regole nel servizio gestito da Amazon per Prometheus. Crea una policy AWS Identity and Access Management (IAM) con le seguenti autorizzazioni e assegnala ai tuoi utenti, gruppi o ruoli.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps: CreateAlertManagerDefinition",
        "aps: DescribeAlertManagerSilence",
        "aps: DescribeAlertManagerDefinition",
        "aps: PutAlertManagerDefinition",
        "aps: DeleteAlertManagerDefinition",
        "aps: ListAlerts",
        "aps: ListRules",
        "aps: ListAlertManagerReceivers",
        "aps: ListAlertManagerSilences",
        "aps: ListAlertManagerAlerts",
        "aps: ListAlertManagerAlertGroups",

```

```
        "aps: GetAlertManagerStatus",
        "aps: GetAlertManagerSilence",
        "aps: PutAlertManagerSilences",
        "aps: DeleteAlertManagerSilence",
        "aps: CreateAlertManagerAlerts"
    ],
    "Resource": "*"
}
]
```

## Creazione di un file di configurazione di alert manager

Per utilizzare la gestione degli avvisi e la creazione di modelli nel servizio gestito da Amazon per Prometheus, devi creare un file YAML di configurazione di alert manager. Un file di alert manager del servizio gestito da Amazon per Prometheus è composto da due sezioni principali:

- `template_files`: contiene i modelli utilizzati per i messaggi inviati dai destinatari. Per ulteriori informazioni, vedere [Modello di riferimento](#) ed [Esempi di modello](#) nella documentazione di Prometheus.
- `alertmanager_config`: contiene la configurazione di alert manager. Questo utilizza la stessa struttura di un file di configurazione di alert manager in Prometheus autonomo. Per ulteriori informazioni, consulta [Configurazione](#) nella documentazione di Alertmanager.

### Note

La `repeat_interval` configurazione descritta nella documentazione di Prometheus sopra riportata presenta un'ulteriore limitazione nel servizio gestito da Amazon per Prometheus. Il valore massimo consentito è cinque giorni. Se lo imposti per un periodo superiore a cinque giorni, verrà considerato come un periodo di cinque giorni e le notifiche verranno inviate nuovamente dopo la scadenza del periodo di cinque giorni.

### Note

Puoi anche modificare il file di configurazione direttamente nella console Amazon Managed Service for Prometheus, ma deve comunque seguire il formato specificato qui. Per ulteriori

informazioni sul caricamento o la modifica di un file di configurazione, consulta. [Caricamento del file di configurazione di alert manager per il servizio gestito da Amazon per Prometheus](#)

Nel servizio gestito da Amazon per Prometheus, il file di configurazione di alert manager deve avere tutto il contenuto di configurazione di alert manager all'interno di `alertmanager_config` una chiave nella radice del file YAML.

Di seguito è riportato un esempio di file di configurazione di alert manager di base:

```
alertmanager_config: |
  route:
    receiver: 'default'
  receivers:
  - name: 'default'
    sns_configs:
    - topic_arn: arn:aws:sns:us-east-2:123456789012:My-Topic
      sigv4:
        region: us-east-2
      attributes:
        key: key1
        value: value1
```

L'unico ricevitore attualmente supportato è Amazon Simple Notification Service (Amazon SNS). Se nella configurazione sono elencati altri tipi di ricevitori, questi verranno rifiutati.

Ecco un altro esempio di file di configurazione di alert manager che utilizza sia il blocco `template_files` sia il blocco `alertmanager_config`.

```
template_files:
  default_template: |
    {{ define "sns.default.subject" }}[{{ .Status | toUpper }}]{{ if eq .Status
"firing" }}:{{ .Alerts.Firing | len }}{{ end }}]{{ end }}
    {{ define "__alertmanager" }}AlertManager{{ end }}
    {{ define "__alertmanagerURL" }}[{{ .ExternalURL }}]#/alerts?receiver={{ .Receiver |
urlquery }}]{{ end }}
alertmanager_config: |
  global:
  templates:
  - 'default_template'
  route:
```

```

receiver: default
receivers:
- name: 'default'
  sns_configs:
  - topic_arn: arn:aws:sns:us-east-2:accountid:My-Topic
    sigv4:
      region: us-east-2
    attributes:
      key: severity
      value: SEV2

```

## Blocco modello Amazon SNS predefinito

La configurazione predefinita di Amazon SNS utilizza il seguente modello, a meno che tu non lo sostituisca esplicitamente.

```

{{ define "sns.default.message" }}{{ .CommonAnnotations.SortedPairs.Values | join "
" }}
{{ if gt (len .Alerts.Firing) 0 -}}
Alerts Firing:
  {{ template "__text_alert_list" .Alerts.Firing }}
{{- end }}
{{ if gt (len .Alerts.Resolved) 0 -}}
Alerts Resolved:
  {{ template "__text_alert_list" .Alerts.Resolved }}
{{- end }}
{{- end }}

```

## Configurazione del ricevitore di avvisi

L'unico ricevitore di avvisi attualmente supportato nel servizio gestito da Amazon per Prometheus è Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni, consulta [Cos'è Amazon SNS?](#)

### Argomenti

- [\(Facoltativo\) Creazione di un nuovo argomento Amazon SNS](#)
- [Autorizzazione al servizio gestito da Amazon per Prometheus per inviare messaggi al tuo argomento Amazon SNS](#)
- [Specificare l'argomento di Amazon SNS nel file di configurazione di alert manager](#)

- [\(Facoltativo\) Configurazione di alert manager per inviare JSON ad Amazon SNS](#)
- [\(Facoltativo\) Invio da Amazon SNS verso altre destinazioni](#)
- [Regole di convalida e troncamento dei messaggi del ricevitore SNS](#)

## (Facoltativo) Creazione di un nuovo argomento Amazon SNS

Puoi utilizzare un argomento Amazon SNS esistente o crearne uno nuovo. Ti consigliamo di utilizzare un argomento di tipo Standard, in modo da poter inoltrare gli avvisi dall'argomento a e-mail, SMS o HTTP.

Per creare un nuovo argomento Amazon SNS da utilizzare come ricevitore di alert manager, segui la procedura descritta nel [Passaggio 1: Creare un argomento](#). Assicurati di scegliere Standard per il tipo di argomento.

Se desideri ricevere email ogni volta che viene inviato un messaggio a quell'argomento di Amazon SNS, segui la procedura descritta nel [Fase 2: crea un abbonamento all'argomento](#).

## Autorizzazione al servizio gestito da Amazon per Prometheus per inviare messaggi al tuo argomento Amazon SNS

Devi autorizzare il servizio gestito da Amazon per Prometheus a inviare messaggi al tuo argomento Amazon SNS. La seguente dichiarazione sulla policy include una Condition dichiarazione per aiutare a prevenire il problema di sicurezza confused deputy. L'Conditionistruzione limita l'accesso all'argomento Amazon SNS per consentire solo le operazioni provenienti da questo account specifico e dall'area di lavoro del servizio gestito da Amazon per Prometheus. Per ulteriori informazioni sul problema del "confused deputy", consulta [Prevenzione del confused deputy tra servizi](#).

Per autorizzare il servizio gestito da Amazon per Prometheus a inviare messaggi al tuo argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo <https://console.aws.amazon.com/sns/v3/home>.
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Scegli il nome dell'argomento da utilizzare per il servizio gestito da Amazon per Prometheus.
4. Scegli Modifica.
5. Scegli policy di accesso e aggiungi la seguente istruzione di policy alla policy esistente.

```
{
```

```

    "Sid": "Allow_Publish_Alarms",
    "Effect": "Allow",
    "Principal": {
      "Service": "aps.amazonaws.com"
    },
    "Action": [
      "sns:Publish",
      "sns:GetTopicAttributes"
    ],
    "Condition": {
      "ArnEquals": {
        "aws:SourceArn": "workspace_ARN"
      },
      "StringEquals": {
        "AWS:SourceAccount": "account_id"
      }
    },
    "Resource": "arn:aws:sns:region:account_id:topic_name"
  }

```

[Facoltativo] Se il tuo argomento SNS è abilitato alla crittografia lato servizio (SSE), devi aggiungere le seguenti autorizzazioni alla policy della chiave KMS nel blocco "Action". Per ulteriori informazioni, consulta [AWS Autorizzazioni KMS per argomenti SNS](#).

```

kms:GenerateDataKey
kms:Decrypt

```

## 6. Seleziona Salvataggio delle modifiche.

### Note

Per impostazione predefinita, Amazon SNS crea la policy di accesso con la condizione attiva `AWS:SourceOwner`. Per ulteriori informazioni sui punti di accesso, consulta [Policy di accesso SNS](#).

### Note

IAM segue la prima regola della [policy più restrittiva](#). Nel tuo argomento SNS, se esiste un blocco di policy più restrittivo del blocco di policy di Amazon SNS documentato,

l'autorizzazione per tale policy non viene concessa. Per valutare la tua policy e scoprire cosa è stata concessa, consulta [Logica di valutazione della policy](#).

## Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS mette a disposizione strumenti che consentono di proteggere i dati relativi a tutti i servizi con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account.

Ti consigliamo di utilizzare le chiavi di contesto delle condizioni globali [aws:SourceArn](#) e [aws:SourceAccount](#) nelle policy delle risorse per limitare le autorizzazioni con cui il servizio gestito da Amazon per Prometheus fornisce a Amazon SNS una risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il valore di `aws:SourceArn` deve essere l'ARN dell'area di lavoro del servizio gestito da Amazon per Prometheus.

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 si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (\*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:service::123456789012:*`.

L'esempio seguente mostra in [Autorizzazione al servizio gestito da Amazon per Prometheus per inviare messaggi al tuo argomento Amazon SNS](#) mostra il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` in Microsoft AD gestito per prevenire il problema "confused deputy".

## Specificare l'argomento di Amazon SNS nel file di configurazione di alert manager

Ora puoi aggiungere il ricevitore Amazon SNS alla configurazione di alert manager. A tale scopo, devi conoscere l'Amazon Resource Name (ARN) dell'argomento Amazon SNS.

Per ulteriori informazioni sulla configurazione del ricevitore Amazon SNS, consulta la documentazione di configurazione [<sns\\_configs>](#) di Prometheus.

### Proprietà non supportate

Il servizio gestito da Amazon per Prometheus supporta Amazon SNS come ricevitore di avvisi. Tuttavia, a causa dei vincoli del servizio, non tutte le proprietà del ricevitore Amazon SNS sono supportate. Le seguenti proprietà non sono consentite in un file di configurazione di alert manager del servizio gestito da Amazon per Prometheus:

- `api_url`: – Il servizio gestito da Amazon per Prometheus lo imposta `api_url` per te, quindi questa proprietà non è consentita.
- `Http_config` – Questa proprietà consente di impostare proxy esterni. Al momento il servizio gestito da Amazon per Prometheus non lo supporta.

Inoltre, le impostazioni SigV4 sono necessarie per avere una proprietà Regione. Senza la proprietà Regione, il servizio gestito da Amazon per Prometheus non dispone di informazioni sufficienti per effettuare la richiesta di autorizzazione.

Per configurare il alert manager con il tuo argomento Amazon SNS come ricevitore

1. Se si utilizza un file di configurazione di alert manager esistente, aprirlo in un editor di testo.
2. Se nel blocco sono presenti ricevitori correnti diversi da Amazon SNS nel blocco `receivers`, rimuovili. Puoi configurare più argomenti di Amazon SNS come destinatari inserendoli in `sns_config` blocchi separati all'interno del blocco `receivers`.
3. Aggiungi il seguente blocco YAML all'interno della sezione `receivers`.

```
- name: name_of_receiver
  sns_configs:
    - sigv4:
        region: region
        topic_arn: ARN_of_SNS_topic
        subject: somesubject
```

```
attributes:
  key: somekey
  value: somevalue
```

Se un `subject` non è specificato, per impostazione predefinita, viene generato un oggetto con il modello predefinito con il nome e i valori dell'etichetta, il che potrebbe risultare in un valore troppo lungo per SNS. Per modificare il modello applicato all'oggetto, consulta [\(Facoltativo\) Configurazione di alert manager per inviare JSON ad Amazon SNS](#) in questa guida.

Ora devi caricare il tuo file di configurazione di alert manager per il servizio gestito da Amazon per Prometheus. Per ulteriori informazioni, consulta [Caricamento del file di configurazione di alert manager per il servizio gestito da Amazon per Prometheus](#).

## (Facoltativo) Configurazione di alert manager per inviare JSON ad Amazon SNS

Puoi configurare Alert Manager per inviare avvisi in formato JSON, in modo che possano essere elaborati a valle da Amazon SNS all'interno o negli AWS Lambda endpoint di ricezione di webhook. Il modello predefinito fornito con alert manager del servizio gestito da Amazon per Prometheus genera il payload dei messaggi in un formato di elenco di testo, che potrebbe non essere facile da analizzare. Invece di utilizzare il modello predefinito, puoi definire un modello personalizzato per l'output del contenuto del messaggio in JSON, semplificando l'analisi nelle funzioni downstream.

Per inviare messaggi da alert manager ad Amazon SNS in formato JSON, aggiorna la configurazione di alert manager in modo che contenga il seguente codice all'interno della sezione principale `template_files`:

```
default_template: |
  {{ define "sns.default.message" }}{{ "{" }}"receiver": "{{ .Receiver }}", "status":
  "{{ .Status }}", "alerts": [{{ range $alertIndex, $alerts := .Alerts }}{{ if
  $alertIndex }} , {{ end }}{{ "{" }}"status": "{{ $alerts.Status }}"{{ if
  gt (len $alerts.Labels.SortedPairs) 0 -}}, "labels": {{ "{" }}{{ range
  $index, $label := $alerts.Labels.SortedPairs }}{{ if $index }} ,
  {{ end }}{{ $label.Name }}": "{{ $label.Value }}"{{ end }}
  {{ "{" }}{{- end }}{{ if gt (len $alerts.Annotations.SortedPairs )
  0 -}}, "annotations": {{ "{" }}{{ range $index, $annotations :=
  $alerts.Annotations.SortedPairs }}{{ if $index }} , {{ end }}{{ $annotations.Name }}":
  "{{ $annotations.Value }}"{{ end }}{{ "{" }}{{- end }} , "startsAt":
  "{{ $alerts.StartsAt }}", "endsAt": "{{ $alerts.EndsAt }}", "generatorURL":
```

```

"{{ $alerts.GeneratorURL }}", "fingerprint": "{{ $alerts.Fingerprint }}"{{ " " }}
{{ end }}{{ if gt (len .GroupLabels) 0 -}}, "groupLabels": {{ " " }}{{ range
  $index, $groupLabels := .GroupLabels.SortedPairs }}{{ if $index }},
  {{ end }}"{{ $groupLabels.Name }}": "{{ $groupLabels.Value }}"{{ end }}
{{ " " }}{{- end }}{{ if gt (len .CommonLabels) 0 -}}, "commonLabels": {{ " " }}
{{ range $index, $commonLabels := .CommonLabels.SortedPairs }}{{ if $index }},
  {{ end }}"{{ $commonLabels.Name }}": "{{ $commonLabels.Value }}"{{ end }}{{ " " }}{{-
  end }}{{ if gt (len .CommonAnnotations) 0 -}}, "commonAnnotations": {{ " " }}{{ range
  $index, $commonAnnotations := .CommonAnnotations.SortedPairs }}{{ if $index }},
  {{ end }}"{{ $commonAnnotations.Name }}": "{{ $commonAnnotations.Value }}"{{ end }}
{{ " " }}{{- end }}{{ " " }}{{ end }}
  {{ define "sns.default.subject" }}[{{ .Status | toUpper }}{{ if eq .Status
  "firing" }}:{{ .Alerts.Firing | len }}]{{ end }}]{{ end }}

```

### Note

Questo modello crea JSON da dati alfanumerici. Se i tuoi dati contengono caratteri speciali, codificali prima di utilizzare questo modello.

Per assicurarti che questo modello venga utilizzato nelle notifiche in uscita, fai riferimento ad esso nel tuo blocco `alertmanager_config` come segue:

```

alertmanager_config: |
  global:
  templates:
    - 'default_template'

```

### Note

Questo modello è per l'intero corpo del messaggio in formato JSON. Questo modello sovrascrive l'intero corpo del messaggio. Non è possibile sovrascrivere il corpo del messaggio se desideri utilizzare questo modello specifico. Tutte le sostituzioni eseguite manualmente avranno la precedenza sul modello.

Per ulteriori informazioni su:

- Il file di configurazione di alert manager, consulta [Creazione di un file di configurazione di alert manager](#).

- Caricamento del file di configurazione, consulta [Caricamento del file di configurazione di alert manager per il servizio gestito da Amazon per Prometheus](#).

## (Facoltativo) Invio da Amazon SNS verso altre destinazioni

Attualmente, il servizio gestito da Amazon per Prometheus può inviare messaggi di avviso direttamente solo ad Amazon SNS. Puoi configurare Amazon SNS per inviare questi messaggi ad altre destinazioni come e-mail, webhook, Slack e. OpsGenie

### E-mail

Per configurare un argomento Amazon SNS per inviare messaggi via email, crea un abbonamento. Nella console Amazon SNS, scegli la scheda Abbonamenti per aprire la pagina con l'elenco degli abbonamenti. Scegli Crea abbonamento e seleziona Email. Amazon SNS invia un'email di conferma all'indirizzo email indicato. Dopo aver accettato la conferma, potrai ricevere le notifiche di Amazon SNS come email dall'argomento a cui ti sei abbonato. Per ulteriori informazioni, consulta [Iscrizione a un argomento Amazon SNS](#).

### Webhook

Per configurare un argomento Amazon SNS per inviare messaggi a un endpoint webhook, crea un abbonamento. Nella console Amazon SNS, scegli la scheda Abbonamenti per aprire la pagina con l'elenco degli abbonamenti. Scegli Crea abbonamento e seleziona HTTP/HTTPS. Dopo aver creato l'abbonamento, devi seguire i passaggi di conferma per attivarlo. Quando è attivo, il tuo endpoint HTTP dovrebbe ricevere le notifiche di Amazon SNS. Per ulteriori informazioni, consulta [Iscrizione a un argomento Amazon SNS](#). Per ulteriori informazioni sull'utilizzo dei webhook di Slack per pubblicare messaggi verso varie destinazioni, consulta [Come faccio a utilizzare i webhook per pubblicare messaggi Amazon SNS su Amazon Chime, Slack o Microsoft Teams?](#)

### Slack

Per configurare un argomento Amazon SNS per inviare messaggi a Slack, hai due opzioni. Puoi integrarti con email-to-channel l'integrazione di Slack, che consente a Slack di accettare messaggi e-mail e inoltrarli a un canale Slack, oppure puoi utilizzare una funzione Lambda per riscrivere la notifica di Amazon SNS su Slack. [Per ulteriori informazioni sull'inoltro delle e-mail ai canali Slack, consulta Confirming SNS Topic Subscription for Slack Webhook. AWS](#) Per ulteriori informazioni sulla creazione di una funzione Lambda per convertire i messaggi Amazon SNS in Slack, consulta [Come integrare il servizio gestito da Amazon per Prometheus con Slack](#).

## OpsGenie

Per informazioni su come configurare un argomento di Amazon SNS su cui inviare messaggi OpsGenie, consulta [Integrare Opsgenie con Amazon SNS in entrata](#).

## Regole di convalida e troncamento dei messaggi del ricevitore SNS

I messaggi SNS verranno convalidati, troncati o modificati, se necessario, dal ricevitore SNS in base alle seguenti regole:

- Il messaggio contiene caratteri non utf.
  - Il messaggio verrà sostituito da "Errore: stringa codificata UTF-8 non valida".
  - Verrà aggiunto un attributo del messaggio con la chiave "truncated" e il valore "true"
  - Verrà aggiunto un attributo messaggio con la chiave "modified" e il valore "Message: Errore - stringa non valida codificata UTF-8".
- Il messaggio è vuoto.
  - Il messaggio verrà sostituito da "Errore - il messaggio non deve essere vuoto".
  - Verrà aggiunto un attributo del messaggio con la chiave "modified" e il valore "Messaggio: Errore - Il messaggio non dovrebbe essere vuoto".
- Il messaggio è stato troncato.
  - Il contenuto del messaggio sarà troncato.
  - Verrà aggiunto un attributo del messaggio con la chiave "truncated" e il valore "true"
  - Verrà aggiunto un attributo del messaggio con la chiave "modified" e il valore "Messaggio: Errore - Il messaggio è stato troncato da **X** KB, perché supera il limite di dimensione di 256 KB".
- L'oggetto non è ASCII.
  - L'oggetto verrà sostituito da "Errore - contiene caratteri ASCII non stampabili".
  - Verrà aggiunto un attributo del messaggio con la chiave "modified" e il valore di "Oggetto: Errore - contiene caratteri ASCII non stampabili".
- L'oggetto è stato troncato.
  - L'oggetto avrà il contenuto troncato.
  - Verrà aggiunto un attributo del messaggio con la chiave "modified" e il valore "Oggetto: Errore - L'oggetto è stato troncato da **X** caratteri perché supera il limite di 100 caratteri".
- L'attributo del messaggio ha una chiave/valore non valido.
  - L'attributo del messaggio non valido verrà rimosso.

- Verrà aggiunto un attributo del messaggio con la chiave «modificato» e il valore "MessageAttribute: Errore - *X* degli attributi del messaggio sono stati rimossi a causa di un or non valido». MessageAttributeKey MessageAttributeValue
- L'attributo Message è stato troncato.
- Gli attributi aggiuntivi del messaggio verranno rimossi.
- Verrà aggiunto un attributo del messaggio con la chiave «modificato» e il valore "MessageAttribute: Errore - *X* degli attributi del messaggio sono stati rimossi, perché supera il limite di 256 KB.

## Caricamento del file di configurazione di alert manager per il servizio gestito da Amazon per Prometheus

Una volta individuate le modifiche da apportare al file di configurazione di Alert Manager, è possibile modificarlo all'interno della console oppure caricare un file sostitutivo con la console o. AWS CLI

### Note

Se utilizzi un cluster Amazon EKS, puoi anche caricare un file di configurazione di Alert Manager utilizzando [AWS Controllers for Kubernetes](#).

Per utilizzare la console Amazon Managed Service for Prometheus per modificare o sostituire la configurazione del gestore degli avvisi

1. Apri la console del servizio gestito da Amazon per Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nell'angolo in alto a sinistra della pagina, scegli l'icona del menu, quindi scegli Tutte le aree di lavoro.
3. Scegli l'ID dell'area di lavoro, quindi scegli la scheda Alert manager.
4. Se l'area di lavoro non dispone già di una definizione di alert manager, scegli Aggiungi definizione.

**Note**

Se l'area di lavoro ha una definizione di gestore degli avvisi che desideri sostituire, scegli invece Modifica.

5. Seleziona Scegli file, seleziona il file di definizione di alert manager e scegli Continua.

**Note**

In alternativa, puoi creare un nuovo file e modificarlo direttamente nella console, scegliendo l'opzione Crea definizione. In questo modo verrà creata una configurazione predefinita di esempio che modificherai prima del caricamento.

Da utilizzare per AWS CLI caricare una configurazione di Alert Manager in un'area di lavoro per la prima volta

1. Base64 codifica il contenuto del tuo file di alert manager. In Linux, puoi utilizzare il seguente comando:

```
base64 input-file output-file
```

In macOS, puoi utilizzare il seguente comando:

```
openssl base64 input-file output-file
```

2. Per caricare il file, inserisci uno dei seguenti comandi.

Nella AWS CLI versione 2, inserisci:

```
aws amp create-alert-manager-definition --data file://path_to_base_64_output_file  
--workspace-id my-workspace-id --region region
```

Nella AWS CLI versione 1, inserisci:

```
aws amp create-alert-manager-definition --data fileb://path_to_base_64_output_file  
--workspace-id my-workspace-id --region region
```

3. Sono necessari alcuni secondi per rendere attiva la configurazione di alert manager. Per controllare lo stato, immetti il comando seguente:

```
aws amp describe-alert-manager-definition --workspace-id workspace_id --  
region region
```

In caso status affermativo ACTIVE, la nuova definizione di alert manager ha effetto.

Per utilizzare per AWS CLI sostituire la configurazione del gestore degli avvisi di un'area di lavoro con una nuova

1. Base64 codifica il contenuto del tuo file di alert manager. In Linux, puoi utilizzare il seguente comando:

```
base64 input-file output-file
```

In macOS, puoi utilizzare il seguente comando:

```
openssl base64 input-file output-file
```

2. Per caricare il file, inserisci uno dei seguenti comandi.

Nella AWS CLI versione 2, inserisci:

```
aws amp put-alert-manager-definition --data file://path_to_base_64_output_file --  
workspace-id my-workspace-id --region region
```

Nella AWS CLI versione 1, inserisci:

```
aws amp put-alert-manager-definition --data fileb://path_to_base_64_output_file --  
workspace-id my-workspace-id --region region
```

3. Sono necessari alcuni secondi per rendere attiva la nuova configurazione di alert manager. Per controllare lo stato, immetti il comando seguente:

```
aws amp describe-alert-manager-definition --workspace-id workspace_id --  
region region
```

In caso `status` affermativo `ACTIVE`, la nuova definizione di alert manager ha effetto. Fino a quel momento, la configurazione precedente di alert manager è ancora attiva.

## Integrazione degli avvisi con Amazon Managed Grafana o Grafana open source

Le regole di avviso che hai creato in Alertmanager all'interno di Amazon Managed Service for Prometheus possono essere inoltrate e visualizzate in [Amazon Managed Grafana](#) e [Grafana](#), unificando le regole di avviso e gli avvisi in un unico ambiente. All'interno di Amazon Managed Grafana, puoi visualizzare le regole di avviso e gli avvisi generati.

### Prerequisiti

Prima di iniziare a integrare Amazon Managed Service for Prometheus in Amazon Managed Grafana, devi aver completato i seguenti prerequisiti:

- È necessario disporre di credenziali Account AWS e IAM esistenti per creare i ruoli Amazon Managed Service for Prometheus e ruoli IAM a livello di codice.

Per informazioni sulle credenziali Account AWS e IAM, consulta [Configurazione](#).

- Devi disporre di un'area di lavoro Amazon Managed Service for Prometheus e inserirvi dati. Per configurare un nuovo spazio di lavoro, consulta [Creare un'area di lavoro](#). Dovresti anche avere familiarità con i concetti di Prometheus come Alertmanager e Ruler. Per informazioni su questi argomenti, consulta la [documentazione di Prometheus](#).
- Hai una configurazione Alertmanager e un file di regole già configurati in Amazon Managed Service for Prometheus. Per ulteriori informazioni su Alertmanager in Amazon Managed Service for Prometheus, consulta [Alert Manager](#). Per ulteriori informazioni sulle regole, consulta [Regole di registrazione e regole di avviso](#).
- Devi avere configurato Amazon Managed Grafana o la versione open source di Grafana in esecuzione.
  - Se utilizzi Amazon Managed Grafana, devi utilizzare gli avvisi Grafana. Per ulteriori informazioni, consulta [Migrazione degli avvisi della dashboard legacy agli avvisi Grafana](#).
  - Se utilizzi la versione open source di Grafana, è necessario utilizzare la versione 9.1 o superiore.

**Note**

Puoi usare versioni precedenti di Grafana, ma devi [abilitare la funzionalità di avviso unificato](#) (Avviso Grafana) e potresti dover configurare [un proxy sigv4](#) per effettuare chiamate da Grafana verso Amazon Managed Service for Prometheus. Per ulteriori informazioni, consulta [Configurazione di Grafana open source o Grafana Enterprise per l'utilizzo con il servizio gestito da Amazon per Prometheus](#).

- Amazon Managed Grafana deve avere i seguenti permessi per le tue risorse Prometheus. È necessario aggiungerle alle politiche gestite dal servizio o gestite dal cliente descritte in <https://docs.aws.amazon.com/grafana/latest/userguide/AMG-manage-permissions.html>.
  - `aps:ListRules`
  - `aps:ListAlertManagerSilences`
  - `aps:ListAlertManagerAlerts`
  - `aps:GetAlertManagerStatus`
  - `aps:ListAlertManagerAlertGroups`
  - `aps:PutAlertManagerSilences`
  - `aps>DeleteAlertManagerSilence`

## Configurazione di Amazon Managed Grafana

Se hai già configurato regole e avvisi nella tua istanza di Amazon Managed Service for Prometheus, la configurazione per utilizzare Amazon Managed Grafana come dashboard per tali avvisi viene eseguita interamente all'interno di Amazon Managed Grafana.

Per configurare Amazon Managed Grafana come dashboard degli avvisi

1. Apri la console Grafana per la tua area di lavoro.
2. In Configurazioni, scegli Origini dati.
3. Crea o apri la tua origine dati Prometheus. Se non hai precedentemente configurato un'origine dati Prometheus, consulta [Aggiungi l'origine dati Prometheus a Grafana](#) per ulteriori informazioni.
4. Nell'origine dati Prometheus, seleziona Gestisci avvisi tramite l'interfaccia utente di Alertmanager.
5. Torna all'interfaccia delle origini dati.

6. Crea una nuova origine dati Alertmanager.
7. Nella pagina di configurazione dell'origine dati Alertmanager, aggiungi le seguenti impostazioni:
  - Imposta l'implementazione su Prometheus.
  - Per l'impostazione dell'URL, usa l'URL dell'area di lavoro Prometheus, rimuovi tutto dopo l'ID dell'area di lavoro e aggiungi `/alertmanager` alla fine. Ad esempio, `https://aps-workspaces.us-east1.amazonaws.com/workspaces/ws-example-1234-5678-abcd-xyz00000001/alertmanager`.
  - In Auth, attiva Sigv4Auth. In questo modo Grafana userà l'[AWSautenticazione](#) per le richieste.
  - In Sigv4Auth Details, per Regione predefinita, fornisci la regione dell'istanza Prometheus, ad esempio `us-east-1`.
  - Imposta l'opzione Predefinito su `true`.
8. Seleziona Save and test (Salva ed esegui test).
9. Gli avvisi di Amazon Managed Service for Prometheus dovrebbero ora essere configurati per funzionare con la tua istanza Grafana. Verifica di poter visualizzare tutte le regole di avviso, i gruppi di avvisi (inclusi gli avvisi attivi) e i silenzi dalla tua istanza di Amazon Managed Service for Prometheus nella pagina degli avvisi Grafana.

## Risoluzione dei problemi di alert manager

Utilizzando [CloudWatch Registri](#), è possibile risolvere i problemi relativi ad alert manager e Ruler. Questa sezione contiene argomenti relativi alla risoluzione dei problemi relativi ad alert manager.

### Argomenti

- [Avviso di contenuto vuoto](#)
- [Avviso non ASCII](#)
- [Avviso non valido key/value](#)
- [Avviso di limite dei messaggi](#)
- [Nessun errore di policy basata su risorse](#)

## Avviso di contenuto vuoto

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "Message has been modified because the content was empty."
    "level": "WARN"
  },
  "component": "alertmanager"
}
```

Ciò significa che il modello di gestione degli avvisi ha risolto l'avviso in uscita in un messaggio vuoto.

### Operazione da eseguire

Convalida il modello di alert manager e assicurati di disporre di un modello valido per tutti i percorsi dei destinatari.

## Avviso non ASCII

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "Subject has been modified because it contains control or non-ASCII
characters."
    "level": "WARN"
  },
  "component": "alertmanager"
}
```

Ciò significa che l'oggetto contiene caratteri non ASCII.

### Operazione da eseguire

Rimuovi i riferimenti nel campo dell'oggetto del modello alle etichette che potrebbero contenere caratteri non ASCII.

## Avviso non valido **key/value**

Quando il registro contiene il seguente avviso

```
{
```

```
"workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
"message": {
  "log": "MessageAttributes has been removed because of invalid key/value,
numberOfRemovedAttributes=1"
  "level": "WARN"
},
"component": "alertmanager"
}
```

Ciò significa che alcuni attributi del messaggio sono stati rimossi perché chiavi/valori non sono validi.

### Operazione da eseguire

Valuta nuovamente i modelli che stai utilizzando per compilare gli attributi del messaggio e assicurati che si risolva in un attributo di messaggio SNS valido. Per ulteriori informazioni sulla convalida di un messaggio per un argomento Amazon SNS, consulta [l'argomento Convalida di SNS](#)

## Avviso di limite dei messaggi

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "Message has been truncated because it exceeds size limit,
originSize=266K, truncatedSize=12K"
    "level": "WARN"
  },
  "component": "alertmanager"
}
```

Ciò significa che parte della dimensione del messaggio è troppo grande.

### Operazione da eseguire

Guarda il modello di messaggio del destinatario dell'avviso e rielaboralo per adattarlo al limite di dimensione.

## Nessun errore di policy basata su risorse

Quando il registro contiene il seguente errore

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "Notify for alerts failed, AMP is not authorized to perform: SNS:Publish
on resource: arn:aws:sns:us-west-2:12345:testSnsReceiver because no resource-based
policy allows the SNS:Publish action"
    "level": "ERROR"
  },
  "component": "alertmanager"
}
```

Ciò significa che il servizio gestito da Amazon per Prometheus non dispone delle autorizzazioni per inviare l'avviso all'argomento SNS specificato.

### Operazione da eseguire

Verifica che la policy di accesso sull'argomento Amazon SNS conceda ad Amazon Managed Service for Prometheus la possibilità di inviare messaggi SNS all'argomento. Crea una politica di accesso SNS che dia al servizio `aps.amazonaws.com` (Amazon Managed Service for Prometheus) l'accesso al tuo argomento Amazon SNS. Per ulteriori informazioni sulle politiche di accesso a SNS, consulta [Using the Access Policy Language](#) e [Casi di esempio per il controllo degli accessi di Amazon SNS nella Amazon Simple Notification Service Developer Guide](#).

## Registrazione di log e monitoraggio

Puoi gestire l'utilizzo delle risorse di Amazon Managed Service for Prometheus con le funzionalità di registrazione e monitoraggio di CloudWatch Amazon.

- Utilizza [CloudWatch metriche](#) per monitorare Managed Service for Prometheus.
- Utilizza [CloudWatch Registri](#) per interrogare e visualizzare gli eventi di gestione degli avvisi e righe del servizio gestito da Amazon per Prometheus.

## CloudWatch metriche

Amazon Managed Service for Prometheus fornisce metriche di utilizzo a CloudWatch. Questi parametri forniscono visibilità sull'utilizzo dell'area di lavoro. Le metriche fornite sono disponibili nei namespace e in `AWS/Usage` `AWS/Prometheus` CloudWatch. Queste metriche sono disponibili gratuitamente. CloudWatch. Per ulteriori informazioni sulle metriche di utilizzo, consulta [Metriche di CloudWatch utilizzo](#).

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount	IngestionRate	AWS/Usage	Frequenza di acquisizione del campione  Unità: conta al secondo  Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ResourceCount	ActiveSeries	AWS/Usage	Numero di serie attive per area di lavoro  Unità: conteggio

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
			Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ResourceCount	ActiveAlerts	AWS/Usage	<p>Numero di avvisi attivi per area di lavoro</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
ResourceCount	SizeOfAvvisi	AWS/Usage	<p>Dimensione totale di tutti gli avvisi nell'area di lavoro, in byte</p> <p>Unità: byte</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount	SuppressedAlerts	AWS/Usage	<p>Numero di avvisi in stato soppresso per area di lavoro. Un avviso può essere soppresso mediante un silenzio o un'inibizione.</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
ResourceCount	UnprocessedAlerts	AWS/Usage	<p>Numero di avvisi in stato non elaborato per area di lavoro. Un avviso è in stato non elaborato una volta ricevuto da AlertManager, ma è in attesa della successiva valutazione del gruppo di aggregazione.</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount	AllAlerts	AWS/Usage	<p>Numero di avvisi in qualsiasi stato per area di lavoro.</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
AlertManagerAlertsReceived	-	AWS/Prometheus	<p>Totale degli avvisi ricevuti con successo dal gestore degli avvisi</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
AlertManagerNotificationsFailed	-	AWS/Prometheus	<p>Numero di consegne di avvisi non andate a buon fine</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
AlertManagerNotificationsThrottled	-	AWS/Prometheus	<p>Numero di avvisi limitati</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
DiscardedSamples*	-	AWS/Prometheus	<p>Numero di campioni scartati per motivo</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
RuleEvaluations	-	AWS/Prometheus	<p>Numero totale di valutazioni delle regole</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
RuleEvaluationErrors	-	AWS/Prometheus	<p>Numero di errori di valutazione delle regole nell'intervallo</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>
RuleGroupIterationsMissed	-	AWS/Prometheus	<p>Numero di iterazioni del gruppo di regole mancate nell'intervallo.</p> <p>Unità: conteggio</p> <p>Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)</p>

\* Alcuni dei motivi che causano l'eliminazione dei campioni sono i seguenti.

Motivo	Significato
greater_than_max_sample_age	Eliminare campioni più vecchi di un'ora.
new-value-for-timestamp	I campioni duplicati vengono inviati con un timestamp diverso da quello registrato in precedenza.
per_metric_series_limit	L'utente ha raggiunto il limite delle serie attive per metrica.

Motivo	Significato
per_user_series_limit	L'utente ha raggiunto il limite totale di serie attive.
rate_limited	Tasso di ingestione limitato.
sample-out-of-order	I campioni vengono inviati fuori servizio e non possono essere elaborati.
label_value_too_long	Il valore dell'etichetta è superiore al limite di caratteri consentito.
max_label_names_per_series	L'utente ha raggiunto i nomi delle etichette per metrica.
missing_metric_name	Il nome della metrica non è fornito.
metric_name_invalid	Nome metrico fornito non valido.
label_invalid	Etichetta fornita non valida.
duplicate_label_names	Sono stati forniti nomi di etichetta duplicati.

#### Note

Un parametro non esistente o mancante è uguale al valore di quella metrica pari a 0.

#### Note

`RuleGroupIterationsMissed`, `RuleEvaluations` e `RuleEvaluationFailures` hanno la `RuleGroup` dimensione della seguente struttura:

*`RuleGroupNamespace`; `RuleGroup`*

## Impostazione di un CloudWatch allarme su Prometheus vended metrics

È possibile monitorare l'utilizzo delle risorse di Prometheus utilizzando gli allarmi. CloudWatch

## Per impostare un allarme sul numero di ActiveSeriesPrometheus

1. Scegli la scheda **Metriche grafiche** e scorri verso il basso fino all'etichetta **ActiveSeries**.  
  
Nella vista **Parametri grafici**, verranno visualizzati solo i parametri attualmente in fase di importazione.
2. Scegli l'icona di notifica nella colonna **Azioni**.
3. In **Specificare parametri e condizioni**, inserisci la condizione di soglia nel campo **Valore condizioni** e scegli **Avanti**.
4. In **Configura azioni**, seleziona un argomento SNS esistente o crea un nuovo argomento SNS a cui inviare la notifica.
5. In **Aggiungi nome e descrizione**, aggiungi il nome dell'allarme e una descrizione facoltativa.
6. Scegli **Crea allarme**.

## CloudWatch Registri

Amazon Managed Service for Prometheus registra gli errori e gli avvisi di Alert Manager e Ruler in gruppi di log in Amazon Logs. CloudWatch Per ulteriori informazioni su Alert Manager e Rulers, consulta l'argomento [Alert Manager](#) in questa guida. Puoi pubblicare i dati dei log dell'area di lavoro per registrare i flussi in Logs. CloudWatch Puoi configurare i log che desideri monitorare nella console del servizio gestito da Amazon per Prometheus o utilizzando AWS CLI. È possibile visualizzare o interrogare questi registri nella console. CloudWatch Per ulteriori informazioni sulla visualizzazione dei flussi di CloudWatch log nella console, consulta [Lavorare con i gruppi di log e i flussi di log CloudWatch nella](#) guida per l'utente. CloudWatch

Il livello CloudWatch gratuito consente di pubblicare fino a 5 GB di log in Logs. CloudWatch [I log che superano il limite consentito dal piano gratuito verranno addebitati in base al piano tariffario.](#) [CloudWatch](#)

### Argomenti

- [Configurazione dei registri CloudWatch](#)

## Configurazione dei registri CloudWatch

Amazon Managed Service for Prometheus registra gli errori e gli avvisi di Alert Manager e Ruler in gruppi di log in Amazon Logs. CloudWatch

Puoi impostare la configurazione della registrazione CloudWatch dei log nella console Amazon Managed Service for Prometheus o chiamando la richiesta API. AWS CLI `create-logging-configuration`

## Prerequisiti

Prima di chiamare `create-logging-configuration`, allega la seguente policy o autorizzazioni equivalenti all'ID o al ruolo che utilizzerai per configurare Logs. CloudWatch

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps>DeleteLoggingConfiguration"
      ],
      "Resource": "*"
    }
  ]
}
```

## Per configurare i registri CloudWatch

Puoi configurare la registrazione in Amazon Managed Service for Prometheus utilizzando la console o il. AWS CLI

### Console

Come configurare la registrazione nella console del servizio gestito da Amazon per Prometheus

1. Vai alla scheda Log nel pannello dei dettagli dell'area di lavoro.

2. Scegli Gestisci i log nella parte superiore destra del pannello Log.
3. Scegli tutto nell'elenco a discesa a livello di log.
4. Scegli il gruppo di log in cui vuoi pubblicare i log nell'elenco a discesa Gruppo di log.

Puoi anche creare un nuovo gruppo di log nella console. CloudWatch

5. Seleziona Salvataggio delle modifiche.

## AWS CLI

È possibile impostare la configurazione di registrazione utilizzando. AWS CLI

Per configurare la registrazione utilizzando il AWS CLI

- Utilizzando il AWS CLI, esegui il comando seguente.

```
aws amp create-logging-configuration --workspace-id my_workspace_ID
                                     --log-group-arn my-log-group-arn
```

## Limitazioni

- Non tutti gli eventi sono registrati

Il servizio gestito da Amazon per Prometheus registra solo gli eventi al livello `warning` o `error`.

- Limite di dimensione della policy

CloudWatch Le politiche relative alle risorse dei log sono limitate a 5120 caratteri. Quando CloudWatch Logs rileva che una policy si avvicina a questo limite di dimensione, abilita automaticamente i gruppi di log che iniziano con. `/aws/vendedlogs/`

Quando crei una regola di avviso con la registrazione abilitata, Amazon Managed Service for Prometheus deve aggiornare la politica delle risorse Logs con CloudWatch il gruppo di log specificato. Per evitare di raggiungere il limite di dimensione della politica delle risorse CloudWatch Logs, inserisci come prefisso i nomi dei gruppi di log Logs con. CloudWatch `/aws/vendedlogs/` Quando crei un gruppo di log nella console del servizio gestito da Amazon per Prometheus, i nomi dei gruppi di log hanno il prefisso `/aws/vendedlogs/`. Per ulteriori informazioni, vedere [Abilitazione della registrazione da determinati AWS servizi](#) nella Guida per l' CloudWatch utente di Logs.

## Comprendi e ottimizza i costi

Le seguenti domande frequenti e le relative risposte possono essere utili per comprendere e ottimizzare i costi associati al servizio gestito da Amazon per Prometheus.

### Cosa contribuisce ai miei costi?

Per la maggior parte dei clienti, l'acquisizione dei parametri contribuisce alla maggior parte dei costi. I clienti con un elevato utilizzo delle query vedranno inoltre aumentare i costi in base agli esempi di domande elaborati, mentre l'archiviazione dei parametri rappresenterà un fattore secondario dei costi complessivi. Per ulteriori informazioni sui prezzi di ciascuno di questi, consulta la pagina [Prezzi](#) nella pagina del prodotto Servizio gestito da Amazon per Prometheus.

### Qual è il modo migliore per ridurre i miei costi? Come posso ridurre i costi di acquisizione?

I tassi di acquisizione (non l'archiviazione dei parametri) rappresentano la maggior parte dei costi per la maggior parte dei clienti. È possibile ridurre i tassi di acquisizione riducendo la frequenza di raccolta (aumentando l'intervallo di raccolta) o riducendo il numero di serie attive ingerite.

Puoi aumentare l'intervallo di raccolta (scraping) dal tuo agente di raccolta: sia il server Prometheus (in esecuzione in modalità Agente) che il raccoglitore AWS Distro for (ADOT) supportano la configurazione. OpenTelemetry `scrape_interval` Ad esempio, aumentando l'intervallo di raccolta da 30 secondi a 60 secondi si ridurrà della metà l'utilizzo di importazione.

Puoi anche filtrare le parametri inviate al servizio gestito da Amazon per Prometheus utilizzando il `<relabel_config>`. Per ulteriori informazioni sulla rietichettatura nella configurazione dell'agente Prometheus, consulta [https://prometheus.io/docs/prometheus/latest/configuration/configuration/#relabel\\_config](https://prometheus.io/docs/prometheus/latest/configuration/configuration/#relabel_config) nella documentazione di Prometheus.

### Qual è il modo migliore per ridurre i costi delle mie richieste?

I costi delle domande si basano sul numero di campioni elaborati. È possibile ridurre la frequenza delle domande per ridurre i costi delle domande.

Per avere maggiore visibilità sulle domande che contribuiscono maggiormente ai costi delle richieste, puoi contattare il tuo contatto di assistenza per presentare un ticket. Il team del servizio gestito da

Amazon per Prometheus può aiutarti a comprendere le domande che contribuiscono maggiormente ai tuoi costi.

## Se riduco il periodo di conservazione dei miei parametri, ciò contribuirà a ridurre la mia fattura totale?

È possibile ridurre il periodo di conservazione, tuttavia è improbabile che ciò riduca in modo sostanziale i costi.

Se desideri ridurre (o aumentare) il periodo di conservazione, puoi presentare una [richiesta di limitazione del servizio](#) per modificare la Retention time for ingested data quota.

## Come posso mantenere bassi i costi delle mie richieste di avviso?

Gli avvisi creano interrogazioni sui dati, che si aggiungono ai costi delle query. Ecco alcune strategie che puoi utilizzare per ottimizzare le richieste di avviso e ridurre i costi.

- Usa Amazon Managed Service per gli avvisi Prometheus: i sistemi di avviso esterni ad Amazon Managed Service for Prometheus potrebbero richiedere query aggiuntive per aggiungere resilienza o alta disponibilità, poiché il servizio esterno richiede le metriche da più zone o regioni di disponibilità. Ciò include avvisi in Grafana per l'alta disponibilità. Ciò può moltiplicare i costi per tre o più volte. Gli avvisi in Amazon Managed Service for Prometheus sono ottimizzati e ti offriranno disponibilità e resilienza elevate con il minor numero di query.

Ti consigliamo di utilizzare gli avvisi nativi in Amazon Managed Service for Prometheus anziché sistemi di avviso esterni.

- Ottimizzazione dell'intervallo di avviso: un modo rapido per ottimizzare le richieste di avviso consiste nell'aumentare l'intervallo di aggiornamento automatico. Se hai un avviso che viene interrogato ogni minuto, ma è necessario solo ogni cinque minuti, l'aumento dell'intervallo di aggiornamento automatico potrebbe farti risparmiare cinque volte i costi delle query per quell'avviso.
- Utilizza un lookback ottimale: una finestra di lookback più ampia nella query aumenta i costi della query, poiché richiama più dati. Assicurati che la finestra di lookback nella tua query PromQL sia di dimensioni ragionevoli per i dati che devi avvisare. Ad esempio, nella regola seguente, l'espressione include una finestra di lookback di dieci minuti:

```
- alert: metric:alerting_rule
```

```
expr: avg(rate(container_cpu_usage_seconds_total[10m])) > 0
for: 2m
```

La modifica dell'espressione `avg(rate(container_cpu_usage_seconds_total[5m])) > 0` può contribuire a ridurre i costi delle query.

In generale, consulta le tue regole di avviso e assicurati di utilizzare le metriche migliori per il tuo servizio. È facile creare avvisi sovrapposti sulla stessa metrica o più avvisi che forniscono le stesse informazioni, soprattutto se aggiungi avvisi nel tempo. Se ti accorgi di vedere spesso gruppi di avvisi che si verificano contemporaneamente, è possibile ottimizzare gli avvisi e non includerli tutti.

Questi suggerimenti possono aiutarti a ridurre i costi. In definitiva, è necessario bilanciare i costi con la creazione del giusto set di avvisi per comprendere lo stato del sistema.

Per ulteriori informazioni sugli avvisi in Amazon Managed Service for Prometheus, consulta [Alert Manager](#)

## Quali parametri posso utilizzare per monitorare i miei costi?

Monitora `IngestionRate` in Amazon CloudWatch per tenere traccia dei costi di ingestione. Per ulteriori informazioni sul monitoraggio dei parametri di Amazon Managed Service for Prometheus in, consulta [CloudWatch CloudWatch metriche](#)

## Posso controllare la mia fattura in qualsiasi momento?

AWS Cost and Usage Report Tiene traccia del tuo AWS utilizzo e fornisce una stima dei costi associati al tuo account entro un periodo di fatturazione. Per ulteriori informazioni, consulta [Cosa sono i report AWS sui costi e sull'utilizzo?](#) nella Guida per l'utente dei report sui AWS costi e sull'utilizzo

## Perché la mia fattura è più alta all'inizio del mese rispetto alla fine del mese?

Il servizio gestito da Amazon per Prometheus ha un modello di prezzo a più livelli per l'acquisizione, che comporta costi di utilizzo iniziale più elevati. Man mano che l'utilizzo raggiunge livelli di importazione più elevati, con costi inferiori, i costi diminuiscono. Per ulteriori informazioni sui prezzi,

compresi i livelli di acquisizione, consulta la pagina [Prezzi](#) nella pagina del prodotto Servizio gestito da Amazon per Prometheus.

#### Note

- I livelli possono essere utilizzati all'interno di una regione, non tra aree geografiche diverse. L'utilizzo all'interno di una regione deve raggiungere il livello successivo per utilizzare la tariffa più bassa.
- In un'organizzazione in AWS Organizations, l'utilizzo del livello viene conteggiato per account pagante, non per account (l'account del pagante è sempre l'account di gestione dell'organizzazione). Quando il totale delle metriche inserite (all'interno di una regione) per tutti gli account di un'organizzazione raggiunge il livello successivo, a tutti gli account viene addebitata la tariffa più bassa.

## Ho eliminato tutte le mie aree di lavoro Amazon Managed Service for Prometheus, ma sembra che continuino a ricevere degli addebiti. Cosa potrebbe succedere?

Una possibilità in questo caso è che disponiate ancora di scraper AWS gestiti configurati per inviare metriche alle aree di lavoro eliminate. Segui le istruzioni per. [Trova ed elimina gli scraper](#)

# Integrazione con altri servizi AWS

Amazon Managed Service for Prometheus prevede l'integrazione di altri AWS servizi. Questa sezione descrive l'integrazione con il monitoraggio dei costi di Amazon Elastic Kubernetes Service (Amazon EKS) (con Kubecost) e l'utilizzo dei moduli Terraform per creare una soluzione di osservabilità completa per i tuoi progetti EKS con AWS Observability Accelerator.

## Argomenti

- [L'integrazione con Amazon EKS per il monitoraggio dei costi](#)
- [Utilizzo di AWS Observability Accelerator](#)
- [Integrazione con i AWS controller per Kubernetes](#)
- [Integrazione delle CloudWatch metriche con Firehose](#)

## L'integrazione con Amazon EKS per il monitoraggio dei costi

Amazon Managed Service for Prometheus si integra con il monitoraggio dei costi di Amazon Elastic Kubernetes Service (Amazon EKS) (con Kubecost) per eseguire calcoli di allocazione dei costi e fornire informazioni sull'ottimizzazione dei cluster Kubernetes. Utilizzando Amazon Managed Service for Prometheus con Kubecost, puoi scalare in modo affidabile il monitoraggio dei costi per supportare cluster più grandi.

L'integrazione con Kubecost ti offre una visibilità granulare sui costi dei cluster Amazon EKS. Puoi aggregare i costi in base alla maggior parte dei contesti Kubernetes, dal livello di container fino al livello di cluster e persino a livello di più cluster. Puoi generare report su più contenitori o cluster per tenere traccia dei costi a fini di showback o chargeback.

Di seguito vengono fornite istruzioni per l'integrazione con Kubecost in uno scenario a cluster singolo o multiplo:

- Integrazione a cluster singolo: per scoprire come integrare il monitoraggio dei costi di Amazon EKS con un singolo cluster, consulta il AWS post sul blog [Integrating Kubecost with Amazon Managed Service for Prometheus](#).
- Integrazione multi-cluster: per scoprire come integrare il monitoraggio dei costi di Amazon EKS con più cluster, consulta il AWS post del blog [Monitoraggio dei costi multicluster per Amazon EKS utilizzando Kubecost e Amazon Managed Service for Prometheus](#).

### Note

Per ulteriori informazioni sull'uso di KubeCost, consulta [il monitoraggio dei costi](#) nella Guida per l'utente di Amazon EKS.

## Utilizzo di AWS Observability Accelerator

AWS fornisce strumenti di osservabilità, tra cui monitoraggio, registrazione, avvisi e dashboard, per i tuoi progetti Amazon Elastic Kubernetes Service (Amazon EKS). Ciò include Amazon Managed Service for Prometheus, [Amazon Managed Grafana](#), [AWSDistro per OpenTelemetry](#) e altri strumenti. Per aiutarti a utilizzare questi strumenti insieme, AWS fornisce moduli Terraform che configurano l'osservabilità con questi servizi, chiamati [AWSObservability Accelerator](#).

AWSObservability Accelerator fornisce esempi per il monitoraggio dell'infrastruttura, delle implementazioni [NGINX](#) e di altri scenari. Questa sezione fornisce un esempio di infrastruttura di monitoraggio all'interno del cluster Amazon EKS.

I modelli Terraform e le istruzioni dettagliate sono disponibili nella pagina [AWSObservability Accelerator for Terraform GitHub](#). Puoi anche leggere il [post sul blog che annuncia AWSObservability Accelerator](#).

## Prerequisiti

Per utilizzare AWS Observability Accelerator, è necessario disporre di un cluster Amazon EKS esistente e dei seguenti prerequisiti:

- [AWS CLI](#): utilizzato per richiamare AWS funzionalità dalla riga di comando.
- [kubectl](#): utilizzato per controllare il cluster EKS dalla riga di comando.
- [Terraform](#): utilizzato per automatizzare la creazione delle risorse per questa soluzione. Devi avere il AWS provider configurato con un ruolo IAM che abbia accesso per creare e gestire Amazon Managed Service for Prometheus, Amazon Managed Grafana e IAM all'interno del tuo AWS account. Per ulteriori informazioni su come configurare il AWS provider per Terraform, consulta [AWSprovider](#) nella documentazione di Terraform.

## Utilizzo dell'esempio di monitoraggio dell'infrastruttura

AWS Observability Accelerator fornisce modelli di esempio che utilizzano i moduli Terraform inclusi per impostare e configurare l'osservabilità per il tuo cluster Amazon EKS. Questo esempio dimostra l'utilizzo di AWS Observability Accelerator per configurare il monitoraggio dell'infrastruttura. Per maggiori dettagli sull'utilizzo di questo modello e sulle funzionalità aggiuntive che include, consulta il [cluster esistente con la pagina AWS Observability Accelerator di base e monitoraggio dell'infrastruttura](#) su GitHub.

Per utilizzare il modulo Terraform per il monitoraggio dell'infrastruttura

1. Dalla cartella in cui vuoi creare il tuo progetto, clona il repository usando il seguente comando.

```
git clone https://github.com/aws-observability/terraform-aws-observability-accelerator.git
```

2. Inizializza Terraform con i seguenti comandi.

```
cd examples/existing-cluster-with-base-and-infra  
  
terraform init
```

3. Crea un nuovo `terraform.tfvars` file, come nell'esempio seguente. Usa la AWS regione e l'ID del cluster Amazon EKS.

```
# (mandatory) AWS Region where your resources will be located  
aws_region = "eu-west-1"  
  
# (mandatory) EKS Cluster name  
eks_cluster_id = "my-eks-cluster"
```

4. Crea uno spazio di lavoro Amazon Managed Grafana, se non ne hai già creato uno da utilizzare. Per informazioni su come creare un nuovo spazio di lavoro, consulta [Come creare la tua prima area di lavoro](#) nella Guida utente di Amazon Managed Grafana.
5. Crea due variabili per consentire a Terraform di utilizzare l'area di lavoro Grafana eseguendo i seguenti comandi dalla riga di comando. Dovrai sostituire `grafana-workspace-id` con l'ID della tua area di lavoro Grafana.

```
export TF_VAR_managed_grafana_workspace_id=grafana-workspace-id
```

```
export TF_VAR_grafana_api_key=`aws grafana create-workspace-api-key --key-name
"observability-accelerator-$(date +%s)" --key-role ADMIN --seconds-to-live 1200 --
workspace-id $TF_VAR_managed_grafana_workspace_id --query key --output text`
```

6. [Facoltativo] Per utilizzare un'area di lavoro esistente di Amazon Managed Service for Prometheus, aggiungi l'ID al `terraform.tfvars` file, come nell'esempio seguente, sostituendo *prometheus-workspace-id* con il tuo ID dello spazio di lavoro Prometheus. Se non specifichi uno spazio di lavoro esistente, verrà creato automaticamente una nuova area di lavoro Prometheus.

```
# (optional) Leave it empty for a new workspace to be created
managed_prometheus_workspace_id = "prometheus-workspace-id"
```

7. Implementa la soluzione mediante il comando seguente.

```
terraform apply -var-file=terraform.tfvars
```

In questo modo verranno create risorse nel tuo AWS account, tra cui:

- Una nuova area di lavoro Amazon Managed Service for Prometheus (a meno che tu non abbia scelto di utilizzare uno spazio di lavoro esistente).
- Configurazione, avvisi e regole di alert manager nell'area di lavoro di Prometheus.
- Nuova fonte di dati e dashboard Amazon Managed Grafana nella tua area di lavoro attuale. La fonte di dati verrà chiamata `aws-observability-accelerator`. Le dashboard verranno elencate nelle dashboard di Observability Accelerator.
- Un operatore [AWSDistro for OpenTelemetry](#) configurato nel cluster Amazon EKS fornito per inviare metriche alla tua area di lavoro Amazon Managed Service for Prometheus.

Per visualizzare le tue nuove dashboard, apri la dashboard specifica nella tua area di lavoro Amazon Managed Grafana. Per ulteriori informazioni sull'uso di Amazon Managed Grafana, consulta [Lavorare nell'area di lavoro di Grafana](#), nella Guida utente di Amazon Managed Grafana.

## Integrazione con i AWS controller per Kubernetes

Amazon Managed Service for Prometheus è integrato con [AWS Controllers for Kubernetes \(ACK\)](#), con supporto per la gestione della tua area di lavoro, Alert Manager e risorse Ruler in Amazon EKS.

Puoi utilizzare le definizioni di risorse personalizzate (CRD) di AWS Controllers for Kubernetes e gli oggetti Kubernetes nativi senza dover definire risorse al di fuori del cluster.

Questa sezione descrive come configurare AWS i controller per Kubernetes e Amazon Managed Service for Prometheus in un cluster Amazon EKS esistente.

Puoi anche leggere i post del blog che [introducono AWS Controller for Kubernetes](#) e [introducono il controller ACK per Amazon Managed Service for Prometheus](#).

## Prerequisiti

Prima di iniziare a integrare AWS Controller for Kubernetes e Amazon Managed Service for Prometheus con il tuo cluster Amazon EKS, devi avere i seguenti prerequisiti.

- È necessario disporre di un account [Account AWS e delle autorizzazioni esistenti](#) per creare i ruoli Amazon Managed Service for Prometheus e IAM a livello di codice.
- È necessario disporre di un [cluster Amazon EKS](#) esistente con OpenID Connect (OIDC) abilitato.

Se l'OIDC non è abilitato, è possibile utilizzare il comando seguente per abilitarlo. Ricordati di sostituire *YOUR\_CLUSTER\_NAME* e *AWS\_REGION* con i valori corretti per il tuo account.

```
eksctl utils associate-iam-oidc-provider \
  --cluster ${YOUR_CLUSTER_NAME} --region ${AWS_REGION} \
  --approve
```

Per ulteriori informazioni sull'utilizzo di OIDC con Amazon EKS, consulta [Autenticazione tramite provider di identità OIDC](#) e [Creazione di un provider IAM OIDC](#) nella Guida per l'utente di Amazon EKS.

- È necessario che il [driver CSI di Amazon EBS sia installato](#) nel cluster Amazon EKS.
- È necessaria l'installazione di [AWS CLI](#). AWS CLI Viene utilizzato per richiamare funzionalità dalla riga di comando AWS .
- È necessario installare [Helm](#), il gestore di pacchetti per Kubernetes.
- [I parametri del piano di controllo con Prometheus](#) devono essere configurate nel tuo cluster Amazon EKS.
- È necessario disporre di un argomento [Amazon Simple Notification Service \(Amazon SNS\)](#) a cui desideri inviare gli avvisi dalla nuova area di lavoro. Assicurati di aver [autorizzato Amazon Managed Service for Prometheus a inviare messaggi sull'argomento](#).

Quando il tuo cluster Amazon EKS è configurato correttamente, dovresti essere in grado di vedere i parametri formattati per Prometheus chiamando `kubectl get --raw /metrics`. Ora sei pronto per installare un AWS controller di servizio Controllers for Kubernetes e utilizzarlo per distribuire le risorse di Amazon Managed Service for Prometheus.

## Implementazione di uno spazio di lavoro con Controllers for Kubernetes AWS

Per distribuire un nuovo spazio di lavoro Amazon Managed Service for Prometheus, installerai AWS un controller Controllers for Kubernetes e lo utilizzerai per creare l'area di lavoro.

Implementare un nuovo spazio di lavoro Amazon Managed Service per Prometheus con Controllers for Kubernetes AWS

1. Usa i seguenti comandi per utilizzare Helm per installare il controller di servizio Amazon Managed Service for Prometheus. Per ulteriori informazioni, consulta [Installare un controller ACK](#) nella documentazione di Controllers for Kubernetes su AWS GitHub Usa la *regione* corretta per il tuo sistema, ad esempio `us-east-1`.

```
export SERVICE=prometheusservice
export RELEASE_VERSION=`curl -sL https://api.github.com/repos/aws-controllers-k8s/
$SERVICE-controller/releases/latest | grep '"tag_name":' | cut -d'"' -f4`
export ACK_SYSTEM_NAMESPACE=ack-system
export AWS_REGION=region

aws ecr-public get-login-password --region us-east-1 | helm registry login --
username AWS --password-stdin public.ecr.aws
helm install --create-namespace -n $ACK_SYSTEM_NAMESPACE ack-$SERVICE-controller \
oci://public.ecr.aws/aws-controllers-k8s/$SERVICE-chart --version=
$RELEASE_VERSION --set=aws.region=$AWS_REGION
```

Dopo alcuni istanti, si avrà una risposta simile alla seguente, che indica che la risposta è stata completata.

```
You are now able to create Amazon Managed Service for Prometheus (AMP) resources!
The controller is running in "cluster" mode.
The controller is configured to manage AWS resources in region: "us-east-1"
```

Facoltativamente, puoi verificare che il AWS controller Controllers for Kubernetes sia stato installato correttamente con il seguente comando.

```
helm list --namespace $ACK_SYSTEM_NAMESPACE -o yaml
```

Ciò restituirà informazioni sul controller `ack-prometheusservice-controller`, incluso il `status: deployed`.

2. Crea un file denominato `workspace.yaml`, con il testo seguente. Verrà utilizzato come configurazione per l'area di lavoro che stai creando.

```
apiVersion: prometheusservice.services.k8s.aws/v1alpha1
kind: Workspace
metadata:
  name: my-amp-workspace
spec:
  alias: my-amp-workspace
  tags:
    ClusterName: EKS-demo
```

3. Esegui il comando seguente per creare la tua area di lavoro (questo comando dipende dalle variabili di sistema che hai impostato nel passaggio 1).

```
kubectl apply -f workspace.yaml -n $ACK_SYSTEM_NAMESPACE
```

Entro pochi istanti, dovresti essere in grado di vedere una nuova area di lavoro, denominata `my-amp-workspace` nel tuo account.

Esegui il seguente comando per visualizzare i dettagli e lo stato della tua area di lavoro, incluso l'ID dell'area di lavoro. In alternativa, puoi visualizzare la nuova area di lavoro nella console [Amazon Managed Service for Prometheus](#).

```
kubectl describe workspace my-amp-workspace -n $ACK_SYSTEM_NAMESPACE
```

#### Note

Puoi anche [utilizzare un'area di lavoro esistente](#) anziché crearne una nuova.

4. Crea due nuovi file yaml come configurazione per i Rulegroups e AlertManager creerai successivamente utilizzando la seguente configurazione.

Salva questa configurazione come `rulegroup.yaml`. Sostituisci *WORKSPACE-ID* con l'ID dell'area di lavoro della fase precedente.

```
apiVersion: prometheusservice.services.k8s.aws/v1alpha1
kind: RuleGroupsNamespace
metadata:
  name: default-rule
spec:
  workspaceID: WORKSPACE-ID
  name: default-rule
  configuration: |
    groups:
    - name: example
      rules:
      - alert: HostHighCpuLoad
        expr: 100 - (avg(rate(node_cpu_seconds_total{mode="idle"}[2m])) * 100) > 60
        for: 5m
        labels:
          severity: warning
          event_type: scale_up
        annotations:
          summary: Host high CPU load (instance {{ $labels.instance }})
          description: "CPU load is > 60%\n VALUE = {{ $value }}\n LABELS =
{{ $labels }}"
      - alert: HostLowCpuLoad
        expr: 100 - (avg(rate(node_cpu_seconds_total{mode="idle"}[2m])) * 100) < 30
        for: 5m
        labels:
          severity: warning
          event_type: scale_down
        annotations:
          summary: Host low CPU load (instance {{ $labels.instance }})
          description: "CPU load is < 30%\n VALUE = {{ $value }}\n LABELS =
{{ $labels }}"
```

Salva la seguente configurazione come `alertmanager.yaml`. Sostituisci *WORKSPACE-ID* con l'ID dell'area di lavoro della fase precedente. *Sostituisci TOPIC-ARN con l'ARN per l'argomento Amazon SNS a cui inviare notifiche e REGION con quello che*

*stai utilizzando*. Regione AWS Ricorda che Amazon Managed Service for Prometheus [deve disporre delle autorizzazioni](#) per l'argomento Amazon SNS.

```
apiVersion: prometheusservice.services.k8s.aws/v1alpha1
kind: AlertManagerDefinition
metadata:
  name: alert-manager
spec:
  workspaceID: WORKSPACE-ID
  configuration: |
    alertmanager_config: |
      route:
        receiver: default_receiver
      receivers:
        - name: default_receiver
          sns_configs:
            - topic_arn: TOPIC-ARN
              sigv4:
                region: REGION
          message: |
            alert_type: {{ .CommonLabels.alertname }}
            event_type: {{ .CommonLabels.event_type }}
```

#### Note

Per ulteriori informazioni sui formati di questi file di configurazione, consulta [RuleGroupsNamespaceData](#) e [AlertManagerDefinitionData](#).

5. Esegui i seguenti comandi per creare la configurazione del gruppo di regole e di alert manager (questo comando dipende dalle variabili di sistema impostate nel passaggio 1).

```
kubectl apply -f rulegroup.yaml -n $ACK_SYSTEM_NAMESPACE
kubectl apply -f alertmanager.yaml -n $ACK_SYSTEM_NAMESPACE
```

Le modifiche saranno disponibili in pochi istanti.

#### Note

Per aggiornare una risorsa, anziché crearla, è sufficiente aggiornare il file yaml ed eseguire nuovamente il `kubectl apply` comando.

Per eliminare una risorsa, esegui il seguente comando. Sostituisci *ResourceType* con il tipo di risorsa che desideri eliminare, oppure. `Workspace AlertManagerDefinition RuleGroupNamespace` Sostituisci *ResourceName* con il nome della risorsa da eliminare.

```
kubectl delete ResourceType ResourceName -n $ACK_SYSTEM_NAMESPACE
```

Ciò completa la distribuzione della nuova area di lavoro. La sezione successiva descrive la configurazione del cluster per l'invio di parametri a quell'area di lavoro.

## Configurazione del cluster Amazon EKS per la scrittura nell'area di lavoro di Amazon Managed Service for Prometheus

Questa sezione descrive come usare Helm per configurare Prometheus in esecuzione nel tuo cluster Amazon EKS per la scrittura remota dei parametri nell'area di lavoro Amazon Managed Service for Prometheus che hai creato nella sezione precedente.

Per questa procedura, avrai bisogno del nome del ruolo IAM che hai creato da utilizzare per inserire i parametri. Se non l'hai già fatto, consulta [Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS](#). per ulteriori informazioni e istruzioni. Se segui queste istruzioni, il ruolo IAM verrà denominato `amp-iamproxy-ingest-role`.

Per configurare il cluster Amazon EKS per la scrittura da remoto

1. Utilizza il comando seguente per ottenere la relativa `prometheusEndpoint` area di lavoro. Sostituisci *WORKSPACE-ID* con l'ID dell'area di lavoro della sezione precedente.

```
aws amp describe-workspace --workspace-id WORKSPACE-ID
```

Il `prometheusEndpoint` sarà presente nei risultati restituiti e sarà formattato in questo modo:

```
https://aps-workspaces.us-west-2.amazonaws.com/workspaces/ws-a1b2c3d4-a123-b456-c789-ac1234567890/
```

Salva questo URL per utilizzarlo nei prossimi passaggi.

2. Crea un nuovo file con il seguente testo e chiamalo `prometheus-config.yaml`. Sostituisci *account* con l'ID dell'account, *WorkspaceURL/* con l'URL appena trovato e la *regione* con quella appropriata Regione AWS per il tuo sistema.

```
serviceAccounts:
  server:
    name: "amp-iamproxy-ingest-service-account"
    annotations:
      eks.amazonaws.com/role-arn: "arn:aws:iam::account:role/amp-iamproxy-ingest-role"
  server:
    remoteWrite:
      - url: workspaceURL/api/v1/remote_write
      sigv4:
        region: region
    queue_config:
      max_samples_per_send: 1000
      max_shards: 200
      capacity: 2500
```

3. Trova i nomi del grafico e del namespace di Prometheus, nonché la versione del grafico, con il seguente comando Helm.

```
helm ls --all-namespaces
```

In base ai passaggi precedenti, il grafico e lo spazio dei nomi di Prometheus dovrebbero avere entrambi un nome `prometheus`, e la versione del grafico potrebbe essere `15.2.0`

4. Esegui il comando seguente, utilizzando *PrometheusChartNamePrometheusNamespace*, e *PrometheusChartVersion* trovato nel passaggio precedente.

```
helm upgrade PrometheusChartName prometheus-community/prometheus -n PrometheusNamespace -f prometheus-config.yaml --version PrometheusChartVersion
```

Dopo alcuni minuti, verrà visualizzato un messaggio che indica che l'aggiornamento è stato completato.

5. Facoltativamente, verifica che i parametri vengano inviati correttamente interrogando l'endpoint Amazon Managed Service for Prometheus tramite `aws curl`. Sostituisci *Region* con Regione AWS quello che stai utilizzando e *workspaceURL/* con l'URL che hai trovato nel passaggio 1.

```
awscurl --service="aps" --region="Region" "workspaceURL/api/v1/query?  
query=node_cpu_seconds_total"
```

Ora hai creato un'area di lavoro Amazon Managed Service per Prometheus e ti sei connesso ad esso dal tuo cluster Amazon EKS, utilizzando i file YAML come configurazione. Questi file, denominati Custom Resource Definitions (CRD), risiedono all'interno del tuo cluster Amazon EKS. Puoi utilizzare il AWS controller Controllers for Kubernetes per gestire tutte le tue risorse Amazon Managed Service for Prometheus direttamente dal cluster.

## Integrazione delle CloudWatch metriche con Firehose

Questa sezione descrive come strumentare un [flusso di CloudWatch parametri Amazon](#) e utilizzare [Amazon Data AWS LambdaFirehose](#) e come inserire i parametri in Amazon Managed Service for Prometheus.

Configurerai uno stack utilizzando [AWS Cloud Development Kit \(CDK\)](#) per creare un Firehose Delivery Stream, un Lambda e un bucket Amazon S3 per dimostrare uno scenario completo.

### Infrastruttura

La prima cosa da fare è configurare l'infrastruttura per questa ricetta.

CloudWatch [i flussi di metriche consentono l'inoltro dei dati metrici di streaming a un endpoint HTTP o a un bucket Amazon S3.](#)

La configurazione dell'infrastruttura consisterà in 4 passaggi:

- Configurazione dei prerequisiti
- Creare un'area di lavoro Amazon Managed Service per Prometheus.
- Installazione delle dipendenze
- Implementazione dello stack

### Prerequisiti

- [Viene AWS CLI installato e configurato nel tuo ambiente.](#)

- Il [AWS CDK Typescript](#) è installato nell'ambiente in uso.
- Node.js e Go sono installati nell'ambiente in uso.
- L'[esportatore AWS di CloudWatch metriche di osservabilità github repository](#) (CWMetricsStreamExporter) è stato clonato sul computer locale.

Come creare un'area di lavoro Amazon Managed Service per Prometheus.

1. L'applicazione demo di questa ricetta verrà eseguita su Amazon Managed Service for Prometheus. Crea la tua area di lavoro per Amazon Managed Service for Prometheus tramite il comando seguente:

```
aws amp create-workspace --alias prometheus-demo-recipe
```

2. Assicurati che la tua area di lavoro sia stata creata con il seguente comando:

```
aws amp list-workspaces
```

Per ulteriori informazioni su Amazon Managed Service for Prometheus, consulta la Guida utente di [Amazon Managed Service for Prometheus](#).

Per installare dipendenze

1. Installare le dipendenze

Dalla radice del `aws-o11y-recipes` repository, modifica la directory `CWMetricStreamExporter` utilizzando il comando:

```
cd sandbox/CWMetricStreamExporter
```

Questa sarà ora considerata la radice del repository, d'ora in poi.

2. Cambia le directory in `/cdk` ed esegui il seguente comando:

```
cd cdk
```

3. Esegui il comando riportato qui di seguito per installare la dipendenza.

```
npm install
```

4. Riporta la directory alla radice del repository, quindi modifica la directory `/lambda` utilizzando il seguente comando:

```
cd lambda
```

5. Una volta nella `/lambda` cartella, installa le dipendenze Go usando:

```
go get
```

Tutte le dipendenze sono ora installate.

Per distribuire lo stack

1. Nella radice del repository, apri `config.yaml` e modifica l'URL dell'area di lavoro di Amazon Managed Service for Prometheus sostituendolo con l'ID dello spazio di lavoro appena creato e `{workspace}` la regione in cui si trova l'area di lavoro Amazon Managed Service for Prometheus.

Ad esempio, modifica di seguito con:

```
AMP:
  remote_write_url: "https://aps-workspaces.us-east-2.amazonaws.com/workspaces/
  {workspaceId}/api/v1/remote_write"
  region: us-east-2
```

Cambia i nomi del flusso di distribuzione Firehose e del bucket Amazon S3 a tuo piacimento.

2. Per creare il codice AWS CDK e Lambda, nella radice del repository esegui il comando seguente:

```
npm run build
```

Questa fase di compilazione garantisce la creazione del binario Go Lambda e la distribuzione del CDK su CloudFormation

3. Per completare l'implementazione, esamina e accetta le modifiche IAM richieste dallo stack.
4. (Facoltativo) Puoi verificare se lo stack è stato creato eseguendo il comando seguente.

```
aws cloudformation list-stacks
```

Uno stack denominato CDK Stack sarà presente nell'elenco.

## Creazione di uno CloudWatch stream Amazon

Ora che disponi di una funzione lambda per gestire le metriche, puoi creare il flusso di metriche da Amazon CloudWatch.

Per creare un flusso di metriche CloudWatch

1. Vai alla CloudWatch console, all'indirizzo <https://console.aws.amazon.com/cloudwatch/home#metric-streams:streamsList> e seleziona Crea flusso di metriche.
2. Seleziona i parametri necessari, tutte le metriche o solo da namespace selezionati.
3. In Configuration, scegli Seleziona un Firehose esistente di proprietà del tuo account.
4. Utilizzerai il Firehose creato in precedenza dal CDK. Nel menu a discesa Seleziona il tuo filtro di dati Kinesis Firehose, seleziona il filtro creato in precedenza. Avrà un nome simile a CdkStack-KinesisFirehoseStream123456AB-sample1234.
5. Imposta l'output sul formato JSON.
6. Assegna al filtro parametri un nome significativo per te.
7. Scegli Create metric stream (Crea filtro parametri).
8. (Facoltativo) Per verificare l'invocazione della funzione Lambda, accedi alla console [Lambda](#) e scegli la funzione KinesisMessageHandler. Seleziona la scheda Monitor e la sottoscheda Registri e in Richiamazioni recenti dovrebbero essere visualizzate le voci della funzione Lambda che viene attivata.

### Note

Potrebbero essere necessari fino a 5 minuti prima che le chiamate inizino a essere visualizzate nella scheda Monitor.

Le tue metriche vengono ora trasmesse in streaming da Amazon ad Amazon CloudWatch Amazon Managed Service for Prometheus.

## Rimozione

Potresti voler eliminare le risorse che sono state utilizzate in questo esempio. La procedura seguente illustra come farlo. Ciò interromperà il filtro parametri che hai creato.

Per eliminare le risorse

1. Inizia eliminando lo stack con i seguenti comandi CloudFormation :

```
cd cdk
cdk destroy
```

2. Rimuovere un'area di lavoro Amazon Managed Service per Prometheus:

```
aws amp delete-workspace --workspace-id \  
  `aws amp list-workspaces --alias prometheus-sample-app --query  
  'workspaces[0].workspaceId' --output text`
```

3. Infine, rimuovi lo stream di CloudWatch parametri Amazon utilizzando la [CloudWatch console Amazon](#).

# La sicurezza in Amazon Managed Service for Prometheus

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 AWS e l'utente. Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei [Programmi di conformità AWS](#). Per informazioni sui programmi di conformità applicabili ad Amazon Managed Service for Prometheus, consulta [AWS Servizi coperti dal programma di conformità](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Amazon Managed Service for Prometheus. Gli argomenti seguenti descrivono come configurare Amazon Managed Service for Prometheus per soddisfare gli obiettivi di sicurezza e conformità. È inoltre illustrato come utilizzare altri AWS servizi che consentono di monitorare e proteggere le risorse Amazon Managed Service for Prometheus.

## Argomenti

- [Protezione dei dati di Prometheus nel servizio gestito da Amazon per Prometheus](#)
- [Identity and Access Management per il servizio gestito da Amazon per Prometheus](#)
- [Autorizzazioni e policy IAM](#)
- [Convalida di conformità per Amazon Managed Service per Prometheus](#)
- [La resilienza in Amazon Managed Service for Prometheus](#)
- [Sicurezza dell'infrastruttura in Amazon Managed Service for Prometheus](#)
- [Utilizzo di ruoli collegati ai servizi per il servizio gestito da Amazon per Prometheus](#)
- [Registrazione delle chiamate API di Amazon Managed Service for Prometheus tramite AWS CloudTrail](#)

- [Imposta ruoli IAM per gli account di servizio.](#)
- [Utilizzo di Amazon Managed Service for Prometheus con endpoint VPC di interfaccia](#)

## Protezione dei dati di Prometheus nel servizio gestito da Amazon per Prometheus

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in Amazon Managed Service for Prometheus. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i. Cloud AWS L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

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

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

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Managed Service for Prometheus o Servizi AWS altro utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero

utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

## Argomenti

- [Dati raccolti da Amazon Managed Service per Prometheus](#)
- [Crittografia a riposo](#)

## Dati raccolti da Amazon Managed Service per Prometheus

Il servizio gestito da Amazon per Prometheus raccoglie e archivia i parametri operativi che configuri per essere inviati dai server Prometheus in esecuzione nel tuo account al servizio gestito da Amazon per Prometheus. I dati includono quanto segue:

- Valore dei parametri
- Etichette dei parametri (o coppie chiave-valore arbitrarie) che aiutano a identificare e classificare i dati
- Timestamp per campioni di dati

Gli ID tenant univoci isolano i dati di diversi clienti. Questi ID limitano i dati dei clienti accessibili. I clienti non possono modificare gli ID dei detentori.

Amazon Managed Service for Prometheus crittografa i dati archiviati con le chiavi (`{}_aws_managed_key`). AWS Key Management Service AWS KMS Amazon Managed Service per Prometheus gestisce queste chiavi.

### Note

Amazon Managed Service for Prometheus supporta la creazione di chiavi gestite dai clienti per la crittografia dei dati. Per ulteriori informazioni sulle chiavi utilizzate di default da Amazon Managed Service for Prometheus e su come utilizzare le tue chiavi gestite dai clienti, consulta [Crittografia a riposo](#)

I dati in transito vengono crittografati con HTTPS. Amazon Managed Service for Prometheus protegge le connessioni tra le zone di disponibilità all'interno di una regione utilizzando HTTPS internamente. AWS

## Crittografia a riposo

Per impostazione predefinita, Amazon Managed Service for Prometheus fornisce automaticamente la crittografia a riposo e lo fa utilizzando chiavi di crittografia di proprietà. AWS

- **AWS chiavi possedute:** Amazon Managed Service for Prometheus utilizza queste chiavi per crittografare automaticamente i dati caricati nel tuo spazio di lavoro. Non puoi visualizzare, gestire o utilizzare chiavi di AWS proprietà o controllarne l'utilizzo. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta la pagina [chiavi di proprietàAWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

La crittografia dei dati a riposo aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili dei clienti, come le informazioni di identificazione personale. Consente di creare applicazioni ad alto livello di sicurezza che rispettano rigorosi requisiti normativi e di conformità per la crittografia.

In alternativa, puoi scegliere di utilizzare una chiave gestita dal cliente quando crei il tuo spazio di lavoro:

- **Chiavi gestite dal cliente:** Amazon Managed Service for Prometheus supporta l'uso di una chiave simmetrica gestita dal cliente che puoi creare, possedere e gestire per crittografare i dati nel tuo spazio di lavoro. Poiché hai il pieno controllo di questo tipo di crittografia, puoi eseguire attività come:
  - Stabilire e mantenere le policy delle chiavi
  - Stabilire e mantenere le policy e le sovvenzioni IAM
  - Abilitare e disabilitare le policy delle chiavi
  - Ruotare i materiali crittografici delle chiavi
  - Aggiungere tag
  - Creare alias delle chiavi
  - Pianificare l'eliminazione delle chiavi

Per ulteriori informazioni, consulta [Chiavi gestite dal cliente](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Scegli se utilizzare con attenzione le chiavi gestite dal cliente o le chiavi AWS di proprietà. Le aree di lavoro create con chiavi gestite dal cliente non possono essere convertite per utilizzare chiavi AWS di proprietà in un secondo momento (e viceversa).

#### Note

Amazon Managed Service for Prometheus abilita automaticamente la crittografia dei dati inattivi AWS utilizzando chiavi di proprietà per proteggere i dati senza costi aggiuntivi. Tuttavia, l'utilizzo di una chiave AWS KMS gestita dal cliente comporta dei costi. Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Key Management Service](#).

Per ulteriori informazioni su AWS KMS, consulta [Cos'è AWS Key Management Service?](#)

#### Note

Le aree di lavoro create con chiavi gestite dal cliente non possono utilizzare [raccoltori gestiti AWS](#) per l'importazione.

## In che modo Amazon Managed Service for Prometheus utilizza le sovvenzioni in AWS KMS

Amazon Managed Service for Prometheus richiede tre [concessioni](#) da usare per la chiave gestita dal cliente.

Quando crei un'area di lavoro Amazon Managed Service per Prometheus crittografata con una chiave gestita dal cliente, Amazon Managed Service for Prometheus crea le tre sovvenzioni per tuo conto inviando richieste a [CreateGrant](#) AWS KMS. Le sovvenzioni AWS KMS vengono utilizzate per consentire ad Amazon Managed Service for Prometheus di accedere alla chiave KMS del tuo account, anche quando non viene richiamata direttamente per tuo conto (ad esempio, quando memorizzi dati di metrica che sono stati estratti da un cluster Amazon EKS).

Amazon Managed Service for Prometheus richiede l'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia [DescribeKey](#) richieste per verificare che la chiave AWS KMS KMS simmetrica gestita dal cliente fornita durante la creazione di uno spazio di lavoro sia valida.

- Invia [GenerateDataKey](#) richieste per AWS KMS generare chiavi dati crittografate dalla tua chiave gestita dal cliente.
- Invia le richieste [Decrypt](#) a per AWS KMS decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati.

Amazon Managed Service for Prometheus crea tre concessioni alla AWS KMS chiave che consentono ad Amazon Managed Service for Prometheus di utilizzare la chiave per tuo conto. Puoi rimuovere l'accesso alla chiave modificando la policy della chiave, disabilitando la chiave o revocando la concessione. È necessario comprendere le conseguenze di queste azioni prima di eseguirle. Ciò può causare la perdita di dati nell'area di lavoro.

Se rimuovi l'accesso a una delle concessioni, Amazon Managed Service for Prometheus non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, né di archiviare nuovi dati inviati allo spazio di lavoro; ciò influisce su tutte le operazioni che dipendono da tali dati. I nuovi dati inviati all'area di lavoro non saranno accessibili e potrebbero andare persi definitivamente.

#### Warning

- Se disabiliti la chiave o rimuovi l'accesso ad Amazon Managed Service for Prometheus nella policy della chiave, i dati dell'area di lavoro non sono più accessibili. I nuovi dati inviati all'area di lavoro non saranno accessibili e potrebbero andare persi definitivamente.

Puoi accedere ai dati dell'area di lavoro e cominciare a ricevere nuovi dati ripristinando l'accesso di Amazon Managed Service for Prometheus alla chiave.

- Se revochi una concessione, questa non può essere ricreata e i dati nell'area di lavoro vengono persi definitivamente.

## Fase 1: creare una chiave gestita dal cliente

Puoi creare una chiave simmetrica gestita dal cliente utilizzando o le API. AWS Management Console AWS KMS Non è necessario che la chiave si trovi nello stesso account dell'area di lavoro di Amazon Managed Service for Prometheus, a condizione che tu fornisca l'accesso corretto tramite la policy, come descritto di seguito.

Per creare una chiave simmetrica gestita dal cliente

Segui la procedura riportata in [Creazione di una chiave simmetrica gestita dal cliente](#) nella Guida per gli sviluppatori di AWS Key Management Service .

## Policy della chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta [Gestione dell'accesso alle chiavi gestite dal cliente](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per utilizzare la chiave gestita dal cliente con le aree di lavoro di Amazon Managed Service for Prometheus, le seguenti operazioni API devono essere permesse nella policy della chiave:

- [kms:CreateGrant](#): aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso di controllo a una chiave KMS specificata, che consente l'accesso alle [operazioni di concessione](#) richieste da Amazon Managed Service for Prometheus. Per ulteriori informazioni sulle autorizzazioni, consulta [Utilizzo delle concessioni](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Ciò consente ad Amazon Managed Service for Prometheus di fare quanto segue:

- Chiama `GenerateDataKey` per generare una chiave dati crittografata e archivarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.
- Chiama `Decrypt` per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.
- [kms:DescribeKey](#): fornisce i dettagli della chiave gestiti dal cliente per consentire ad Amazon Managed Service for Prometheus di convalidare la chiave.

I seguenti sono esempi di dichiarazione di policy che puoi aggiungere per Amazon Managed Service for Prometheus:

```
"Statement" : [  
  {  
    "Sid" : "Allow access to Amazon Managed Service for Prometheus principal within  
your account",  
    "Effect" : "Allow",  
    "Principal" : {  
      "AWS" : "*"   
    },  
  },  
]
```

```

    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant",
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "aps.region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    },
    {
      "Sid": "Allow access for key administrators - not required for Amazon Managed
Service for Prometheus",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:*"
      ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    <other statements needed for other non-Amazon Managed Service for Prometheus
scenarios>
  ]

```

- Per ulteriori informazioni su come [specificare le autorizzazioni in una policy](#), consulta la Guida per gli sviluppatori di AWS Key Management Service .
- Per informazioni sulla [Risoluzione dei problemi delle chiavi di accesso](#) consulta la Guida per gli sviluppatori di AWS Key Management Service .

## Fase 2: Specificazione di una chiave gestita dal cliente per Amazon Managed Service for Prometheus

Quando crei un'area di lavoro, puoi specificare la chiave gestita dal cliente inserendo un ARN chiave KMS che Amazon Managed Service for Prometheus utilizza per crittografare i dati archiviati dall'area di lavoro.

## Fase 3: Accesso ai dati da altri servizi, come Amazon Managed Grafana

Questo passaggio è facoltativo: è necessario solo se devi accedere ai dati di Amazon Managed Service for Prometheus da un altro servizio.

I tuoi dati crittografati non sono accessibili da altri servizi, a meno che anche loro abbiano accesso per utilizzare la chiave. AWS KMS Ad esempio, se desideri utilizzare Amazon Managed Grafana per creare una dashboard o un avviso sui tuoi dati, devi consentire ad Amazon Managed Grafana l'accesso alla chiave.

Per consentire ad Amazon Managed Grafana di accedere alla tua chiave gestita dai clienti

1. Nell'[elenco delle aree di lavoro Amazon Managed Grafana](#), seleziona il nome dell'area di lavoro a cui desideri accedere ad Amazon Managed Service for Prometheus. Questo mostra informazioni di riepilogo sul tuo spazio di lavoro Amazon Managed Grafana.
2. Prendi nota del nome del ruolo IAM utilizzato dal tuo spazio di lavoro. Il nome è nel formato `AmazonGrafanaServiceRole-<unique-id>`. La console mostra l'ARN completo per il ruolo. Specificherai questo nome nella AWS KMS console in un passaggio successivo.
3. Nell'[elenco delle chiavi gestite dai AWS KMS clienti](#), scegli la chiave gestita dal cliente che hai utilizzato durante la creazione dell'area di lavoro Amazon Managed Service for Prometheus. Si apre la pagina dei dettagli della configurazione chiave.
4. Accanto a Utenti chiave, seleziona il pulsante Aggiungi.
5. Dall'elenco di nomi, scegli il ruolo IAM di Amazon Managed Grafana che hai indicato sopra. Per facilitarne la ricerca, puoi anche effettuare la ricerca in base al nome.
6. Scegli Aggiungi per aggiungere il ruolo IAM all'elenco degli utenti chiave.

Il tuo spazio di lavoro Amazon Managed Grafana può ora accedere ai dati nell'area di lavoro Amazon Managed Service for Prometheus. Puoi aggiungere altri utenti o ruoli agli utenti chiave per consentire ad altri servizi di accedere al tuo spazio di lavoro.

## Contesto di crittografia di Amazon Managed Service for Prometheus

Un [contesto di crittografia](#) è un set facoltativo di coppie chiave-valore che contengono ulteriori informazioni contestuali sui dati.

AWS KMS utilizza il contesto di crittografia come [dati autenticati aggiuntivi](#) per supportare la crittografia [autenticata](#). Quando includi un contesto di crittografia in una richiesta di crittografia dei

dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

## Contesto di crittografia di Amazon Managed Service per Prometheus

Amazon Managed Service for Prometheus utilizza lo stesso contesto di crittografia in AWS KMS tutte le operazioni crittografiche, in cui la chiave è `aws:aps:arn` e il valore è l'[Amazon Resource Name](#) (ARN) dell'area di lavoro.

### Example

```
"encryptionContext": {
  "aws:aps:arn": "arn:aws:aps:us-west-2:111122223333:workspace/ws-sample-1234-
abcd-56ef-7890abcd12ef"
}
```

## Utilizzo del contesto di crittografia per il monitoraggio

Quando si utilizza una chiave simmetrica gestita dal cliente per crittografare i dati dell'area di lavoro, è possibile utilizzare il contesto di crittografia anche nei record e nei log di controllo per identificare come viene utilizzata la chiave gestita dal cliente. Il contesto di crittografia appare anche nei [log generati da AWS CloudTrail o Amazon CloudWatch Logs](#).

## Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente

È possibile utilizzare il contesto di crittografia nelle policy delle chiavi e nelle policy IAM come `conditions` per controllare l'accesso alla chiave simmetrica gestita dal cliente. È possibile utilizzare i vincoli del contesto di crittografia in una concessione.

Amazon Managed Service for Prometheus utilizza un vincolo del contesto di crittografia nelle concessioni per controllare l'accesso alla chiave gestita dal cliente nel tuo account o Regione. Il vincolo della concessione richiede che le operazioni consentite dalla concessione utilizzino il contesto di crittografia specificato.

### Example

Di seguito sono riportati alcuni esempi di istruzioni delle policy delle chiavi per concedere l'accesso a una chiave gestita dal cliente per un contesto di crittografia specifico. Questa istruzione della policy impone come condizione che le concessioni abbiano un vincolo che specifica il contesto di crittografia.

```
{
  "Sid": "Enable DescribeKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
  },
  "Action": "kms:DescribeKey",
  "Resource": "*"
},
{
  "Sid": "Enable CreateGrant",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:aws:aps:arn": "arn:aws:aps:us-west-2:111122223333:workspace/ws-sample-1234-abcd-56ef-7890abcd12ef"
    }
  }
}
}
```

## Monitoraggio delle chiavi di crittografia per Amazon Managed Service for Prometheus

Quando utilizzi una chiave gestita AWS KMS dal cliente con le tue aree di lavoro Amazon Managed Service for Prometheus, puoi utilizzare [AWS CloudTrailAmazon CloudWatch Logs per tenere traccia delle richieste inviate da Amazon](#) Managed Service for Prometheus. AWS KMS

Gli esempi seguenti sono AWS CloudTrail eventi per CreateGrant GenerateDataKeyDecrypt, e per DescribeKey monitorare le operazioni KMS chiamate da Amazon Managed Service for Prometheus per accedere ai dati crittografati dalla chiave gestita dal cliente:

### CreateGrant

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare il tuo spazio di lavoro, Amazon Managed Service for Prometheus invia tre CreateGrant richieste per tuo conto per accedere alla chiave KMS che hai specificato. Le concessioni create da Amazon Managed Service for Prometheus sono specifiche per la risorsa associata alla chiave gestita dal cliente AWS KMS .

L'evento di esempio seguente registra l'operazione CreateGrant:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "TESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE-KEY-ID1",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "TESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-22T17:02:00Z"
      }
    },
    "invokedBy": "aps.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:07:02Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "ExampleDesktop/1.0 (V1; OS)",
  "requestParameters": {
    "retiringPrincipal": "aps.region.amazonaws.com",
    "operations": [
      "GenerateDataKey",
      "Decrypt",
      "DescribeKey"
    ],
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "granteePrincipal": "aps.region.amazonaws.com"
  },
  "responseElements": {
```

```

    "grantId":
      "0ab0ac0db000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
  }
}

```

## GenerateDataKey

Quando abiliti una chiave gestita AWS KMS dal cliente per il tuo spazio di lavoro, Amazon Managed Service for Prometheus crea una chiave unica. Invia una `GenerateDataKey` richiesta a AWS KMS cui specifica la chiave gestita dal AWS KMS cliente per la risorsa.

L'evento di esempio seguente registra l'operazione `GenerateDataKey`:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "aps.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:07:02Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "ExampleDesktop/1.0 (V1; OS)",
  "requestParameters": {
    "encryptionContext": {

```

```

      "aws:aps:arn": "arn:aws:aps:us-west-2:111122223333:workspace/ws-
sample-1234-abcd-56ef-7890abcd12ef"
    },
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "sharedEventID": "57f5dbec-16da-413e-979f-2c4c6663475e"
}

```

## Decrypt

Quando viene generata una query su un'area di lavoro crittografata, Amazon Managed Service for Prometheus richiama l'operazione Decrypt per utilizzare la chiave dati crittografata memorizzata e accedere ai dati crittografati.

L'evento di esempio seguente registra l'operazione Decrypt:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "aps.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:10:51Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",

```

```

"awsRegion": "us-west-2",
"sourceIPAddress": "172.12.34.56",
"userAgent": "ExampleDesktop/1.0 (V1; OS)",
"requestParameters": {
  "encryptionContext": {
    "aws:aps:arn": "arn:aws:aps:us-west-2:111122223333:workspace/ws-
sample-1234-abcd-56ef-7890abcd12ef"
  },
  "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
  "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
},
"responseElements": null,
"requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333",
"sharedEventID": "dc129381-1d94-49bd-b522-f56a3482d088"
}

```

## DescribeKey

Amazon Managed Service for Prometheus utilizza l'operazione `DescribeKey` per verificare se la chiave gestita dal cliente associata AWS KMS al tuo spazio di lavoro esiste nell'account e nella regione.

L'evento di esempio seguente registra l'operazione `DescribeKey`:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",

```

```
"principalId": "TESTANDEXAMPLE:Sampleuser01",
"arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
"accountId": "111122223333",
"accessKeyId": "EXAMPLE-KEY-ID1",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "TESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-22T17:02:00Z"
  }
},
"invokedBy": "aps.amazonaws.com"
},
"eventTime": "2021-04-22T17:07:02Z",
"eventSource": "kms.amazonaws.com",
"eventName": "DescribeKey",
"awsRegion": "us-west-2",
"sourceIPAddress": "172.12.34.56",
"userAgent": "ExampleDesktop/1.0 (V1; OS)",
"requestParameters": {
  "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
},
"responseElements": null,
"requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
```

```
"recipientAccountId": "111122223333"  
}
```

## Ulteriori informazioni

Le seguenti risorse forniscono ulteriori informazioni sulla crittografia dei dati a riposo.

- Per ulteriori informazioni su [Concetti base di AWS Key Management Service](#), consulta la Guida per gli sviluppatori di AWS Key Management Service .
- Per ulteriori informazioni sulle [migliori pratiche di sicurezza per AWS Key Management Service](#), consulta la Guida per gli AWS Key Management Service sviluppatori.

## Identity and Access Management per il servizio gestito da Amazon per Prometheus

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (accesso effettuato) e autorizzato (dotato di autorizzazioni) per utilizzare le risorse del servizio gestito da Amazon per Prometheus. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

### Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [In che modo il servizio gestito da Amazon per Prometheus funziona con IAM](#)
- [Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus](#)
- [AWS politiche gestite per Amazon Managed Service for Prometheus](#)
- [Identità e accesso di Amazon Managed Service per le risorse del servizio gestito da Amazon per Prometheus](#)

## Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon Managed Service for Prometheus.

**Utente del servizio:** se utilizzi il servizio gestito da Amazon per Prometheus per eseguire il tuo lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità del servizio gestito da Amazon per Prometheus utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità nel servizio gestito da Amazon per Prometheus, consulta [Identità e accesso di Amazon Managed Service per le risorse del servizio gestito da Amazon per Prometheus](#).

**Amministratore del servizio:** se si è responsabile delle risorse del servizio gestito da Amazon per Prometheus. presso la propria azienda, probabilmente si dispone dell'accesso completo al servizio gestito da Amazon per Prometheus. Il tuo compito è determinare le funzionalità e le risorse del servizio gestito da Amazon per Prometheus a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con il servizio gestito da Amazon per Prometheus, consulta [In che modo il servizio gestito da Amazon per Prometheus funziona con IAM](#).

**Amministratore IAM:** se sei un amministratore IAM, potresti essere interessato a ottenere informazioni su come scrivere policy per gestire l'accesso al servizio gestito da Amazon per Prometheus. Per visualizzare policy basate su identità del servizio gestito da Amazon per Prometheus. di esempio che possono essere utilizzate in IAM, consulta [Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus](#).

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle

identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Signing AWS API request](#) nella IAM User Guide.

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

## Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

## Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center .

## Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente IAM.

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

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

## Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console [cambiando ruolo](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente 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 IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta [Cross Account Resource Access in IAM nella IAM](#) User Guide.
- **Accesso tra servizi:** 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.
- **Sessioni di accesso diretto (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente IAM.

- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS CloudShell è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente IAM.

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

## Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

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

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

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione

`iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall' AWS CLI, dall' AWS API.

## Policy basate su identità

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

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente IAM.

## Policy basate su risorse

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

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

## Liste di controllo degli accessi (ACL)

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

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

## Altri tipi di policy

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

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente IAM.
- **Politiche di controllo dei servizi (SCP):** le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente IAM.

## Più tipi di policy

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

## In che modo il servizio gestito da Amazon per Prometheus funziona con IAM

Prima di utilizzare IAM per gestire l'accesso al servizio gestito da Amazon per Prometheus, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con il servizio gestito da Amazon per Prometheus.

### Funzionalità IAM utilizzabili con il servizio gestito da Amazon per Prometheus

Funzionalità IAM	Supporto Amazon Managed Service per Prometheus
<a href="#">Policy basate su identità</a>	Sì
<a href="#">Policy basate su risorse</a>	No
<a href="#">Azioni di policy</a>	Sì
<a href="#">Risorse relative alle policy</a>	Sì
<a href="#">Chiavi di condizione delle policy</a>	No
<a href="#">Liste di controllo degli accessi (ACL)</a>	No
<a href="#">ABAC (tag nelle policy)</a>	Sì
<a href="#">Credenziali temporanee</a>	Sì
<a href="#">Inoltro delle sessioni di accesso (FAS)</a>	No
<a href="#">Ruoli di servizio</a>	No
<a href="#">Ruoli collegati al servizio</a>	Sì

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

## Policy basate su identità per il servizio gestito da Amazon per Prometheus

Supporta le policy basate su identità

Sì

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

Per visualizzare esempi di policy basate su identità del servizio gestito da Amazon per Prometheus, consulta [Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus](#).

## Policy basate su risorse all'interno del servizio gestito da Amazon per Prometheus

Supporta le policy basate su risorse

No

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

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il

principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Cross Account Resource Access in IAM](#) nella IAM User Guide.

## Policy definite dal servizio gestito da Amazon per Prometheus

Supporta le operazioni di policy	Sì
----------------------------------	----

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

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

Per visualizzare un elenco completo delle operazioni del servizio gestito da Amazon per Prometheus, consulta [Operazioni, risorse e chiavi di condizione per il servizio gestito da Amazon per Prometheus](#) nella Guida di riferimento per l'autorizzazione del servizio.

Le operazioni delle policy in Managed Service for Prometheus utilizzano il seguente prefisso prima dell'operazione:

```
aps
```

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

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

Per visualizzare esempi di policy basate su identità del servizio gestito da Amazon per Prometheus, consulta [Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus](#).

## Risorse di policy Amazon Managed Service per Prometheus

Supporta le risorse di policy	Sì
-------------------------------	----

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

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'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 di tipi di risorse del servizio gestito da Amazon per Prometheus e le loro ARN, consulta [Risorse definite da Amazon Managed Service per Prometheus](#) in Guida di riferimento all'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta [Operazioni definite dal servizio gestito da Amazon per Prometheus](#).

Per visualizzare esempi di policy basate su identità del servizio gestito da Amazon per Prometheus, consulta [Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus](#).

## Policy sulle chiavi di condizione per il servizio gestito da Amazon per Prometheus

Supporta le chiavi di condizione delle policy specifiche del servizio	No
---	----

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

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

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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco completo delle chiavi di condizione del servizio gestito da Amazon per Prometheus, consulta [Chiavi di condizione per il servizio gestito da Amazon per Prometheus](#) nella Guida di riferimento per l'autorizzazione del servizio. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta [Operazioni definite dal servizio gestito da Amazon per Prometheus](#).

Per visualizzare esempi di policy basate su identità del servizio gestito da Amazon per Prometheus, consulta [Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus](#).

Liste di controllo degli accessi (ACL) nel servizio gestito da Amazon per Prometheus

Supporta le ACL

No

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

## Controllo degli accessi basato su attributi (ABAC) con Amazon Managed Service per Prometheus

Supporta ABAC (tag nelle policy)	Si
----------------------------------	----

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

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

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

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

Per ulteriori informazioni su ABAC, consulta [Che cos'è ABAC?](#) nella Guida per l'utente 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 il servizio gestito da Amazon per Prometheus

Supporta le credenziali temporanee	Si
------------------------------------	----

Alcuni Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla [Servizi AWS compatibilità con IAM nella IAM User Guide](#).

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le

credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Cambio di un ruolo \(console\)](#) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API o AWS CLI. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Inoltre le sessioni di accesso per Amazon Managed Service for Prometheus

Supports forward access sessions (FAS)	No
--	----

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli del servizio per il servizio gestito da Amazon per Prometheus

Supporta i ruoli di servizio	No
------------------------------	----

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

 Warning

La modifica delle autorizzazioni per un ruolo del servizio potrebbe compromettere la funzionalità del servizio gestito da Amazon per Prometheus. Modifica i ruoli del servizio solo quando il servizio gestito da Amazon per Prometheus fornisce le indicazioni per farlo.

## Ruoli collegati al servizio per il servizio gestito da Amazon per Prometheus

Supporta i ruoli collegati ai servizi Sì

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

Per maggiori dettagli su come creare e gestire i ruoli collegati al servizio gestito da Amazon per Prometheus, consulta [Utilizzo di ruoli collegati ai servizi per il servizio gestito da Amazon per Prometheus](#).

## Esempi di policy basate su identità per il servizio gestito da Amazon per Prometheus

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

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

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti dal servizio gestito da Amazon per Prometheus, incluso il formato degli ARN per ogni tipo di risorsa, consulta [Operazioni, risorse e chiavi di condizione per il servizio gestito da Amazon per Prometheus](#) nella Guida di riferimento per l'autorizzazione del servizio.

### Argomenti

- [Best practice per le policy](#)
- [Uso della console di Amazon Managed Service per Prometheus](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

## Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse del servizio gestito da Amazon per Prometheus all'interno dell'account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: 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 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 anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per IAM Access Analyzer](#) nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Configurazione dell'accesso alle API protetto con MFA](#) nella Guida per l'utente IAM.

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

## Uso della console di Amazon Managed Service per Prometheus

Per accedere alla console del servizio gestito da Amazon per Prometheus, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse del servizio gestito da Amazon per Prometheus nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l' AWS CLI API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console Amazon Managed Service for Prometheus, collega anche Amazon Managed Service for ConsoleAccess Prometheus o la policy gestita alle entità. ReadOnly AWS 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 collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o in modo programmatico. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
}
```

## AWS politiche gestite per Amazon Managed Service for Prometheus

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

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

### AmazonPrometheusFullAccess

È possibile allegare la policy AmazonPrometheusFullAccess alle identità IAM.

## Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `aps` – Consente l'accesso completo al servizio gestito da Amazon per Prometheus
- `eks` – Consente al servizio gestito da Amazon per Prometheus di leggere informazioni sui cluster Amazon EKS. Ciò è necessario per consentire la creazione di scraper gestiti e scoprire i parametri nel cluster.
- `ec2` – Consente al servizio gestito da Amazon per Prometheus di leggere informazioni sulle reti Amazon EC2. Ciò è necessario per consentire la creazione di scraper gestiti con accesso ai parametri di Amazon EKS.
- `iam` – Consente ai responsabili di creare un ruolo collegato ai servizi per gli scraper gestiti tramite parametri.

I contenuti di `AmazonPrometheusFullAccess` sono i seguenti:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllPrometheusActions",
      "Effect": "Allow",
      "Action": [
        "aps:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeCluster",
      "Effect": "Allow",
      "Action": [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "aps.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

    },
    "Resource": "*"
  },
  {
    "Sid": "CreateServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "scrapper.aps.amazonaws.com"
      }
    }
  }
]
}

```

## AmazonPrometheusConsoleFullAccess

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

### Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `aps` – Consente l'accesso completo al servizio gestito da Amazon per Prometheus
- `tag` – Consente ai responsabili di visualizzare i suggerimenti sui tag nella console del servizio gestito da Amazon per Prometheus.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TagSuggestions",
      "Effect": "Allow",
      "Action": [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource": "*"
    }
  ],
}

```

```
{
  "Sid": "PrometheusConsoleActions",
  "Effect": "Allow",
  "Action": [
    "aps:CreateWorkspace",
    "aps:DescribeWorkspace",
    "aps:UpdateWorkspaceAlias",
    "aps>DeleteWorkspace",
    "aps:ListWorkspaces",
    "aps:DescribeAlertManagerDefinition",
    "aps:DescribeRuleGroupsNamespace",
    "aps:CreateAlertManagerDefinition",
    "aps:CreateRuleGroupsNamespace",
    "aps>DeleteAlertManagerDefinition",
    "aps>DeleteRuleGroupsNamespace",
    "aps:ListRuleGroupsNamespaces",
    "aps:PutAlertManagerDefinition",
    "aps:PutRuleGroupsNamespace",
    "aps:TagResource",
    "aps:UntagResource",
    "aps:CreateLoggingConfiguration",
    "aps:UpdateLoggingConfiguration",
    "aps>DeleteLoggingConfiguration",
    "aps:DescribeLoggingConfiguration"
  ],
  "Resource": "*"
}
```

## AmazonPrometheusRemoteWriteAccess

I contenuti di AmazonPrometheusRemoteWriteAccess sono i seguenti:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aps:RemoteWrite"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
    }  
  ]  
}
```

## AmazonPrometheusQueryAccess

I contenuti di AmazonPrometheusQueryAccess sono i seguenti:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Action": [  
        "aps:GetLabels",  
        "aps:GetMetricMetadata",  
        "aps:GetSeries",  
        "aps:QueryMetrics"  
      ],  
      "Effect": "Allow",  
      "Resource": "*"   
    }  
  ]  
}
```

## AWS politica gestita: AmazonPrometheusScrapeServiceRolePolicy

Non puoi collegarti AmazonPrometheusScrapeServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente al servizio gestito da Amazon per Prometheus di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo dei ruoli per l'analisi dei parametri da EKS](#).

Questa policy concede le autorizzazioni per i contributori che consentono la lettura dal tuo cluster Amazon EKS e la scrittura nel tuo spazio di lavoro del servizio gestito da Amazon per Prometheus.

### Note

Questa guida per l'utente in precedenza chiamava erroneamente questa politica AmazonPrometheusScrapeServiceLinkedRolePolicy

## Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `aps` – Consente al responsabile del servizio di scrivere metriche nelle aree di lavoro del servizio gestito da Amazon per Prometheus.
- `ec2` – Consente al responsabile del servizio di leggere e modificare la configurazione di rete per connettersi alla rete che contiene i cluster Amazon EKS.
- `eks` – Consente al responsabile del servizio di accedere ai cluster Amazon EKS. Ciò è necessario per consentire di acquisire automaticamente i parametri. Consente inoltre al committente di ripulire le risorse Amazon EKS quando viene rimosso uno scraper.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DeleteSLR",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid": "NetworkDiscovery",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ENIManagement",
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterface",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMPAgentlessScraper"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
},
{
  "Sid": "TagManagement",
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2:*:*:network-interface/*",
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction": "CreateNetworkInterface"
    },
    "Null": {
      "aws:RequestTag/AMPAgentlessScrapper": "false"
    }
  }
},
{
  "Sid": "ENIUpdating",
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "ec2:ResourceTag/AMPAgentlessScrapper": "false"
    }
  }
},
{
  "Sid": "EKSAccess",
  "Effect": "Allow",
  "Action": "eks:DescribeCluster",
  "Resource": "arn:aws:eks:*:*:cluster/*"
},
{
  "Sid": "DeleteEKSAccessEntry",
  "Effect": "Allow",
  "Action": "eks:DeleteAccessEntry",
  "Resource": "arn:aws:eks:*:*:access-entry/*/role/*",
  "Condition": {
```

```

"StringEquals": {
  "aws:PrincipalAccount": "${aws:ResourceAccount}"
},
"ArnLike": {
  "eks:principalArn": "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
}
},
{
  "Sid": "APSWriting",
  "Effect": "Allow",
  "Action": "aps:RemoteWrite",
  "Resource": "arn:aws:aps:*:*:workspace/*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "${aws:ResourceAccount}"
    }
  }
}
]
}

```

## Amazon Managed Service for Prometheus aggiorna le policy gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon Managed Service for Prometheus da quando questo servizio ha iniziato a tracciare queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina di Cronologia dei documenti del servizio gestito da Amazon per Prometheus.

Modifica	Descrizione	Data
<a href="#">AmazonPrometheusScraperServiceRolePolicy</a> : aggiornamento a una policy esistente	Amazon Managed Service for Prometheus ha aggiunto nuove autorizzazioni per supportare l'utilizzo delle voci di accesso AmazonPrometheusScraperServiceRolePolicyin Amazon EKS.	2 maggio 2024

Modifica	Descrizione	Data
	<p>Include le autorizzazioni per la gestione delle voci di accesso di Amazon EKS per consentire la pulizia delle risorse quando gli scraper vengono eliminati.</p> <div data-bbox="591 478 1029 1035" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>In precedenza, la guida per l'utente indicava erroneamente questa politica AmazonPrometheusScraperServiceLinkedRolePolicy</p> </div>	
<p><a href="#">AmazonPrometheusFu</a>  <a href="#">IIAccess</a>: aggiornamento a una policy esistente</p>	<p>Il servizio gestito da Amazon per Prometheus ha aggiunto nuove autorizzazioni per AmazonPrometheusFuIIAccess per supportare la creazione di scraper gestiti per i parametri nei cluster Amazon EKS.</p> <p>Include le autorizzazioni per la connessione ai cluster Amazon EKS, la lettura delle reti Amazon EC2 e la creazione di un ruolo collegato ai servizi per gli scraper.</p>	<p>26 novembre 2023</p>

Modifica	Descrizione	Data
<a href="#">AmazonPrometheusScrapingServiceLinkedRolePolicy</a> : nuova policy	<p>Il servizio gestito da Amazon per Prometheus ha aggiunto una nuova policy relativa ai ruoli collegati ai servizi da leggere dai contenitori Amazon EKS, per consentire lo scraping automatico dei parametri.</p> <p>Include le autorizzazioni per la connessione ai cluster Amazon EKS, la lettura di reti Amazon EC2 e la creazione e l'eliminazione di reti contrassegnate <code>AMPAgentlessScrape</code>, nonché per la scrittura negli spazi di lavoro del servizio gestito da Amazon per Prometheus.</p>	26 novembre 2023

Modifica	Descrizione	Data
<a href="#">AmazonPrometheusConsoleFullAccess</a> : aggiornamento a una policy esistente	<p>Amazon Managed Service for Prometheus ha aggiunto nuove autorizzazioni AmazonPrometheusConsoleFullAccess per supportare la registrazione degli eventi di Alert Manager e Ruler in Logs. CloudWatch</p> <p>Le autorizzazioni <code>aps:CreateLoggingConfiguration</code>, <code>aps:UpdateLoggingConfiguration</code>, <code>aps&gt;DeleteLoggingConfiguration</code>, <code>aps:DescribeLoggingConfiguration</code> sono state aggiunte.</p>	24 ottobre 2022

Modifica	Descrizione	Data
<p><a href="#">AmazonPrometheusConsoleFullAccess</a>: aggiornamento a una policy esistente</p>	<p>Il servizio gestito da Amazon per Prometheus ha aggiunto nuove autorizzazioni AmazonPrometheusConsoleFullAccess per supportare le nuove funzionalità del servizio gestito da Amazon per Prometheus, in modo che gli utenti con questa policy possano visualizzare un elenco di suggerimenti di tag quando applicano tag alle risorse del servizio gestito da Amazon per Prometheus.</p> <p>Le autorizzazioni tag: GetTags , tag:GetTagsValues , aps:CreateAlertManagerDefinition , aps:CreateRuleGroupsNamespace , aps&gt;DeleteAlertManagerDefinition , aps&gt;DeleteRuleGroupsNamespace , aps:DescribeAlertManagerDefinition , aps:DescribeRuleGroupsNamespace , aps:ListRuleGroupsNamespaces , aps:PutAlertManagerDefinition , aps:PutRuleGroupsNamespace , aps:TagRe</p>	<p>29 settembre 2021</p>

Modifica	Descrizione	Data
	source e aps:Untag Resource sono state aggiunte.	
Il servizio gestito da Amazon per Prometheus ha iniziato a tenere traccia delle modifiche	Amazon Managed Service for Prometheus ha iniziato a tracciare le modifiche alle sue politiche gestite. AWS	15 settembre 2021

## Identità e accesso di Amazon Managed Service per le risorse del servizio gestito da Amazon per Prometheus

Utilizza le informazioni seguenti per eseguire la diagnosi e risolvere i problemi comuni che possono verificarsi durante l'utilizzo del servizio gestito da Amazon per Prometheus e IAM.

### Argomenti

- [Non sono autorizzato a eseguire un'operazione nel servizio gestito da Amazon per Prometheus](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Managed Service for Prometheus](#)

## Non sono autorizzato a eseguire un'operazione nel servizio gestito da Amazon per Prometheus

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 *aps:GetWidget* fittizie.

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

Se hai bisogno di assistenza, contatta il tuo 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 disponi dell'autorizzazione per eseguire l'operazione `iam:PassRole`, per poter passare un ruolo al servizio gestito da Amazon per Prometheus dovrai aggiornare le policy.

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

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

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

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

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

## Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Managed Service for Prometheus

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 degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per scoprire se un servizio supporta queste funzionalità del servizio gestito da Amazon per Prometheus, consulta [In che modo il servizio gestito da Amazon per Prometheus funziona con IAM](#).
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella Guida](#) per l'utente IAM.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta [Cross Account Resource Access in IAM nella IAM](#) User Guide.

## Autorizzazioni e policy IAM

L'accesso alle azioni e ai dati di Amazon Managed Service for Prometheus richiede delle credenziali. Queste credenziali devono disporre delle autorizzazioni per eseguire le azioni e accedere alle AWS risorse, come il recupero di dati di Amazon Managed Service for Prometheus relativi alle risorse cloud. Nelle sezioni seguenti vengono fornite informazioni su come utilizzare AWS Identity and Access Management (IAM) ed Amazon Managed Service for Prometheus per proteggere le risorse tramite il controllo degli accessi. Per ulteriori informazioni, consulta [Policy e autorizzazioni in IAM](#).

## Permessi di Amazon Managed Service per Prometheus

La tabella seguente mostra le possibili azioni di Amazon Managed Service for Prometheus e le relative autorizzazioni richieste. Le azioni possono richiedere anche le autorizzazioni di altri servizi, non descritte qui.

Azione	Autorizzazione richiesta
Avviso creato.	<code>aps:CreateAlertManagerAlerts</code>
Crea una definizione di alert manager in un'area di lavoro. Per ulteriori informazioni, consulta <a href="#">Alert Manager</a> .	<code>aps:CreateAlertManagerDefinition</code>

Azione	Autorizzazione richiesta
Crea uno spazio dei namespace di regole in un'area di lavoro. Per ulteriori informazioni, consulta <a href="#">Regole di registrazione e regole di avviso</a> .	<code>aps:CreateRuleGroupsNamespace</code>
Crea un'area di lavoro Amazon Managed Service per Prometheus. Un'area di lavoro è uno spazio logico dedicato all'archiviazione e all'interrogazione delle metriche di Prometheus.	<code>aps:CreateWorkspace</code>
Eliminare una definizione di alert manager da un'area di lavoro.	<code>aps&gt;DeleteAlertManagerDefinition</code>
Elimina gli avvisi silenziosi.	<code>aps&gt;DeleteAlertManagerSilence</code>
Cancella l'area di lavoro Amazon Managed Service for Prometheus.	<code>aps&gt;DeleteWorkspace</code>
Recupera informazioni dettagliate sulle definizioni di alert manager.	<code>aps:DescribeAlertManagerDefinition</code>
Recupera informazioni dettagliate sui namespace dei gruppi di regole.	<code>aps:DescribeRuleGroupsNamespace</code>
Recupera informazioni dettagliate su un'area di lavoro Amazon Managed Service for Prometheus.	<code>aps:DescribeWorkspace</code>
Recupera informazioni dettagliate sugli avvisi silenziosi.	<code>aps:GetAlertManagerSilence</code>
Recupera lo stato di alert manager in un'area di lavoro.	<code>aps:GetAlertManagerStatus</code>
Recupera le etichette.	<code>aps:GetLabels</code>

Azione	Autorizzazione richiesta
Recupera i metadati per i parametri Amazon Managed Service for Prometheus.	<code>aps:GetMetricMetadata</code>
Recupera i dati delle serie temporali.	<code>aps:GetSeries</code>
Recupera un elenco dei gruppi di avvisi definiti nella definizione di alert manager.	<code>aps:ListAlertManagerAlertGroups</code>
Recupera un elenco degli avvisi definiti in alert manager.	<code>aps:ListAlertManagerAlerts</code>
Recupera un elenco dei ricevitori definiti nella definizione di alert manager.	<code>aps:ListAlertManagerReceivers</code>
Recupera un elenco di avvisi silenziosi definiti.	<code>aps:ListAlertManagerSilences</code>
Recupera un elenco di avvisi attivi.	<code>aps:ListAlerts</code>
Recupera un elenco di regole nei namespace dei gruppi di regole nelle tue aree di lavoro.	<code>aps:ListRules</code>
Recupera un elenco dei namespace dei gruppi di regole nelle tue aree di lavoro.	<code>aps:ListRuleGroupsNamespaces</code>
Recupera i tag associati alle tue risorse Amazon Managed Service for Prometheus.	<code>aps:ListTagsForResource</code>
Recupera un elenco delle aree di lavoro di Amazon Managed Service for Prometheus presenti nell'account.	<code>aps:ListWorkspaces</code>
Aggiorna la definizione di un alert manager esistente in un'area di lavoro.	<code>aps:PutAlertManagerDefinition</code>

Azione	Autorizzazione richiesta
Crea avvisi silenziosi.	<code>aps:PutAlertManagerSilences</code>
Aggiornamento di un namespace dei gruppi di regole esistente.	<code>aps:PutRuleGroupsNamespace</code>
Poni una domanda sui parametri Amazon Managed Service for Prometheus.	<code>aps:QueryMetrics</code>
Esegui un'operazione di scrittura remota per avviare lo streaming di parametri da un server Prometheus ad Amazon Managed Service for Prometheus.	<code>aps:RemoteWrite</code>
Assegna tag alle risorse Amazon Managed Service for Prometheus.	<code>aps:TagResource</code>
Rimuovi tag dalle risorse Amazon Managed Service for Prometheus.	<code>aps:UntagResource</code>
Modifica gli alias delle aree di lavoro esistenti.	<code>aps:UpdateWorkspaceAlias</code>
Crea una configurazione di registrazione.	<code>aps:CreateLoggingConfiguration</code>
Elimina una configurazione di registrazione.	<code>aps&gt;DeleteLoggingConfiguration</code>
Descrivi la configurazione di registrazione dell'area di lavoro.	<code>aps:DescribeLoggingConfiguration</code>
Aggiorna una configurazione di registrazione.	<code>aps:UpdateLoggingConfiguration</code>

## Esempio di policy IAM

Questa sezione fornisce esempi di altre policy autogestite che puoi creare.

La seguente politica IAM garantisce l'accesso completo ad Amazon Managed Service for Prometheus e consente inoltre a un utente di scoprire i cluster Amazon EKS e visualizzarne i dettagli.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps:*",
        "eks:DescribeCluster",
        "eks:ListClusters"
      ],
      "Resource": "*"
    }
  ]
}
```

## Convalida di conformità per Amazon Managed Service per Prometheus

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

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

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- [Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

**Note**

Non tutti i Servizi AWS sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione [Riferimenti sui servizi conformi ai requisiti HIPAA](#).

- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- [Valutazione delle risorse con regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente l'AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

## La resilienza in Amazon Managed Service for Prometheus

L'infrastruttura globale di AWS è basata su Regioni e zone di disponibilità AWS. Le Regioni AWS Le Regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e 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 sulle zone di disponibilità, consulta [Infrastruttura globale di AWS](#).

Oltre all'AWSinfrastruttura globale, Amazon Managed Service for Prometheus offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup, incluso il supporto per dati ad [alta disponibilità](#).

## Sicurezza dell'infrastruttura in Amazon Managed Service for Prometheus

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

Utilizza le chiamate API pubblicate di AWS per accedere ad Amazon Managed Service tramite la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

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

## Utilizzo di ruoli collegati ai servizi per il servizio gestito da Amazon per Prometheus

[Amazon Managed Service for Prometheus AWS Identity and Access Management utilizza ruoli collegati ai servizi \(IAM\)](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente al servizio gestito da Amazon per Prometheus. I ruoli collegati ai servizi sono predefiniti dal servizio gestito da Amazon per Prometheus e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri AWS servizi per conto dell'utente.

Un ruolo collegato ai servizi semplifica la configurazione del servizio gestito da Amazon per Prometheus perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Il servizio gestito da Amazon per Prometheus definisce le autorizzazioni dei ruoli collegati ai servizi e, salvo diversamente definito, solo servizio gestito da Amazon per Prometheus può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

## Utilizzo dei ruoli per l'analisi dei parametri da EKS

Quando si esegue automaticamente lo scraping delle metriche utilizzando Amazon Managed Service for Prometheus managed collector, il ruolo `AWSServiceRoleForAmazonPrometheusScraper` collegato al servizio viene utilizzato per semplificare la configurazione di Managed Collector, poiché non è necessario aggiungere manualmente le autorizzazioni necessarie. Il servizio gestito da Amazon per Prometheus definisce le autorizzazioni e solo servizio gestito da Amazon per Prometheus può assumersi il ruolo.

Per informazioni sugli altri servizi che supportano i ruoli collegati al servizio, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizio. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

## Autorizzazioni del ruolo collegato ai servizi per il servizio gestito da Amazon per Prometheus

Amazon Managed Service for Prometheus utilizza un ruolo collegato al servizio denominato con il prefisso `AWSServiceRoleForAmazonPrometheusScraper` consentire ad Amazon Managed Service for Prometheus di acquisire automaticamente le metriche nei cluster Amazon EKS.

Il ruolo collegato ai servizi prevede che i seguenti servizi assumano il ruolo:

`AWSServiceRoleForAmazonPrometheusScraper`

- `scraper.aps.amazonaws.com`

La politica di autorizzazione dei ruoli denominata

[AmazonPrometheusScraperServiceRolePolicy](#) consente ad Amazon Managed Service for Prometheus di completare le seguenti azioni sulle risorse specificate:

- Prepara e modifica la configurazione di rete per connetterti alla rete che contiene il tuo cluster Amazon EKS.

- Leggi i parametri dai cluster Amazon EKS e scrivi i parametri nelle tue aree di lavoro del servizio gestito da Amazon per Prometheus.

Devi configurare le autorizzazioni per consentire a un'entità di creare o eliminare un ruolo collegato ai servizi. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Creazione di un ruolo collegato ai servizi per il servizio gestito da Amazon per Prometheus

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un'istanza di raccolta gestita utilizzando Amazon EKS o Amazon Managed Service for Prometheus nella, nella o nell' AWS Management Console AWS API AWS CLI, Amazon Managed Service for Prometheus crea il ruolo collegato al servizio per te.

### Important

Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo.

[Per ulteriori informazioni, consulta A new role appeared in my. Account AWS](#)

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un'istanza di Managed Collector utilizzando Amazon EKS o il servizio gestito da Amazon per Prometheus, il servizio gestito da Amazon per Prometheus crea di nuovo il ruolo collegato ai servizi per tuo conto.

## Modifica di un ruolo collegato ai servizi per il servizio gestito da Amazon per Prometheus

Amazon Managed Service for Prometheus non consente di modificare il ruolo collegato al servizio. `AWSServiceRoleForAmazonPrometheusScrapers` Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Eliminazione di un ruolo collegato ai servizi per il servizio gestito da Amazon per Prometheus

Non è necessario eliminare manualmente il ruolo. `AWSServiceRoleForAmazonPrometheusScraper`. Quando elimini tutte le istanze Managed Collector associate al ruolo nell' AWS Management Console, nella o nell' AWS API AWS CLI, Amazon Managed Service for Prometheus pulisce le risorse ed elimina il ruolo collegato al servizio per te.

## Regioni supportate per i ruoli collegati ai servizi del servizio gestito da Amazon per Prometheus

Il servizio gestito da Amazon per Prometheus supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni supportate](#).

## Registrazione delle chiamate API di Amazon Managed Service for Prometheus tramite AWS CloudTrail

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

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

## Informazioni su Amazon Managed Service per Prometheus in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon Managed Service for Prometheus, tale attività viene registrata in CloudTrail un evento insieme AWS ad altri eventi di servizio nella cronologia degli eventi. Puoi

visualizzare, cercare e scaricare eventi recenti nel tuo account. AWS Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon Managed Service for Prometheus, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi da tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

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

Amazon Managed Service for Prometheus supporta la registrazione delle seguenti operazioni di:

- [CreateAlertManagerAlerts](#)
- [CreateAlertManagerDefinition](#)
- [CreateRuleGroupsNamespace](#)
- [CreateWorkspace](#)
- [DeleteAlertManagerDefinition](#)
- [DeleteAlertManagerSilence](#)
- [DeleteWorkspace](#)
- [DeleteRuleGroupsNamespace](#)
- [DescribeAlertManagerDefinition](#)
- [DescribeRulesGroupsNamespace](#)
- [DescribeWorkspace](#)
- [ListRuleGroupsNamespaces](#)
- [ListWorkspaces](#)
- [PutAlertManagerDefinition](#)
- [PutAlertManagerSilences](#)

- [PutRuleGroupsNamespace](#)
- [UpdateWorkspaceAlias](#)

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

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

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

## Informazioni sulle voci dei file di log di Amazon Managed Service for Prometheus

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

Esempio: CreateWorkspace

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' CreateWorkspaceazione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLE123EXAMPLE123-1234567890616",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/admin",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
    },
    "webIdFederationData": {

    },
    "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-11-30T23:39:29Z"
    }
}
},
"eventTime": "2020-11-30T23:43:21Z",
"eventSource": "aps.amazonaws.com",
"eventName": "CreateWorkspace",
"awsRegion": "us-west-2",
"sourceIPAddress": "203.0.113.1",
"userAgent": "aws-cli/1.11.167 Python/2.7.10 Darwin/16.7.0 botocore/1.7.25",
"requestParameters": {
    "alias": "alias-example",
    "clientToken": "12345678-1234-abcd-1234-12345abcd1"
},
"responseElements": {
    "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-trace-id,x-amzn-errormessage,x-amz-apigw-id,date",
    "arn": "arn:aws:aps:us-west-2:123456789012:workspace/ws-abc123456-abcd-1234-5678-1234567890",
    "status": {
        "statusCode": "CREATING"
    },
    "workspaceId": "ws-12345678-1234-abcd-1234-1234567890"
},
"requestID": "890b8639-e51f-11e7-b038-EXAMPLE",
"eventID": "874f89fa-70fc-4798-bc00-EXAMPLE",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}
```

## Esempio: CreateAlertManagerDefinition

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

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLE123EXAMPLE123-1234567890616",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/admin",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {

      },
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-09-23T20:20:14Z"
      }
    }
  },
  "eventTime": "2021-09-23T20:22:43Z",
  "eventSource": "aps.amazonaws.com",
  "eventName": "CreateAlertManagerDefinition",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.1",
  "userAgent": "Boto3/1.17.46 Python/3.6.14 Linux/4.14.238-182.422.amzn2.x86_64 exec-env/AWS_ECS_FARGATE Botocore/1.20.46",
  "requestParameters": {
    "data":
    "YWxlcnRtYW5hZ2VyX2NvbWZpZzogfAogIGdsb2JhbDoKICAgIHNTdHBfc21hcnRob3N00iAnbG9jYWxob3N00jI1JwogI
    "clientToken": "12345678-1234-abcd-1234-12345abcd1",
    "workspaceId": "ws-12345678-1234-abcd-1234-1234567890"
  },
  "responseElements": {
```

```

    "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
trace-id,x-amzn-errormessage,x-amz-apigw-id,date",
    "status": {
      "statusCode": "CREATING"
    }
  },
  "requestID": "890b8639-e51f-11e7-b038-EXAMPLE",
  "eventID": "874f89fa-70fc-4798-bc00-EXAMPLE",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}

```

### Esempio: CreateRuleGroupsNamespace

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

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLE123EXAMPLE123-1234567890616",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/admin",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {

      },
      "attributes": {
        "creationDate": "2021-09-23T20:22:19Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}

```

```

    }
  },
  "eventTime": "2021-09-23T20:25:08Z",
  "eventSource": "aps.amazonaws.com",
  "eventName": "CreateRuleGroupsNamespace",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "34.212.33.165",
  "userAgent": "Boto3/1.17.63 Python/3.6.14 Linux/4.14.238-182.422.amzn2.x86_64 exec-
env/AWS_ECS_FARGATE Botocore/1.20.63",
  "requestParameters": {
    "data":
      "Z3JvdXBz0gogIC0gYmFtZTogdGVzZdFJ1bGVHcm91cHN0YW1lc3BhY2UKICAgIHJ1bGVz0gogICAgLSBhbGVydDogdGVzZ
      "clientToken": "12345678-1234-abcd-1234-12345abcd1",
      "name": "exampleRuleGroupsNamespace",
      "workspaceId": "ws-12345678-1234-abcd-1234-1234567890"
    },
  "responseElements": {
    "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
trace-id,x-amzn-errormessage,x-amz-apigw-id,date",
    "name": "exampleRuleGroupsNamespace",
    "arn": "arn:aws:aps:us-west-2:492980759322:rulegroupsnamespace/ws-
ae46a85c-1609-4c22-90a3-2148642c3b6c/exampleRuleGroupsNamespace",
    "status": {
      "statusCode": "CREATING"
    },
  },
  "tags": {}
},
"requestID": "890b8639-e51f-11e7-b038-EXAMPLE",
"eventID": "874f89fa-70fc-4798-bc00-EXAMPLE",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}

```

## Imposta ruoli IAM per gli account di servizio.

Grazie ai ruoli IAM per gli account di servizio, è possibile associare un ruolo IAM a un account di servizio Kubernetes. Questo account di servizio può quindi fornire le autorizzazioni AWS ai container in qualsiasi pod che utilizza tale account. Per ulteriori informazioni, consulta [Ruoli IAM per gli account di servizio](#).

I ruoli IAM per gli account di servizio sono noti anche come ruoli di servizio.

In Amazon Managed Service for Prometheus, l'utilizzo dei ruoli di servizio può aiutarti a ottenere i ruoli necessari per l'autorizzazione e l'autenticazione tra Amazon Managed Service for Prometheus, i server Prometheus e i server Grafana.

## Prerequisiti

Le procedure in questa pagina richiedono che sia installata l'interfaccia a riga di comando EKSCTL e AWS CLI.

## Configura i ruoli di servizio per l'acquisizione di metriche dai cluster Amazon EKS.

Per configurare i ruoli di servizio per consentire ad Amazon Managed Service for Prometheus di importare le metriche dai server Prometheus nei cluster Amazon EKS, devi accedere a un account con le seguenti autorizzazioni:

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:GetRole`
- `iam:AttachRolePolicy`
- `iam:GetOpenIDConnectProvider`

Per configurare il ruolo di servizio per l'acquisizione in Amazon Managed Service for Prometheus

1. Creare un archivio denominato `createIRSA-AMPIngest.sh` con i seguenti contenuti. Sostituire `<my_amazon_eks_clustername>` con il nome del cluster e sostituirlo `<my_prometheus_namespace>` con il namespace Prometheus.

```
#!/bin/bash -e
CLUSTER_NAME=<my_amazon_eks_clustername>
SERVICE_ACCOUNT_NAMESPACE=<my_prometheus_namespace>
AWS_ACCOUNT_ID=$(aws sts get-caller-identity --query "Account" --output text)
OIDC_PROVIDER=$(aws eks describe-cluster --name $CLUSTER_NAME --query
  "cluster.identity.oidc.issuer" --output text | sed -e "s/^https://\//")
SERVICE_ACCOUNT_AMP_INGEST_NAME=amp-iamproxy-ingest-service-account
SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE=amp-iamproxy-ingest-role
SERVICE_ACCOUNT_IAM_AMP_INGEST_POLICY=AMPIngestPolicy
```

```
#
# Set up a trust policy designed for a specific combination of K8s service account
# and namespace to sign in from a Kubernetes cluster which hosts the OIDC Idp.
#
cat <<EOF > TrustPolicy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::${AWS_ACCOUNT_ID}:oidc-provider/
${OIDC_PROVIDER}"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "${OIDC_PROVIDER}:sub": "system:serviceaccount:
${SERVICE_ACCOUNT_NAMESPACE}:${SERVICE_ACCOUNT_AMP_INGEST_NAME}"
        }
      }
    }
  ]
}
EOF
#
# Set up the permission policy that grants ingest (remote write) permissions for
# all AMP workspaces
#
cat <<EOF > PermissionPolicyIngest.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps:RemoteWrite",
        "aps:GetSeries",
        "aps:GetLabels",
        "aps:GetMetricMetadata"
      ],
      "Resource": "*"
    }
  ]
}
```

```
EOF

function getRoleArn() {
    OUTPUT=$(aws iam get-role --role-name $1 --query 'Role.Arn' --output text 2>&1)

    # Check for an expected exception
    if [[ $? -eq 0 ]]; then
        echo $OUTPUT
    elif [[ -n $(grep "NoSuchEntity" <<< $OUTPUT) ]]; then
        echo ""
    else
        >&2 echo $OUTPUT
        return 1
    fi
}

#
# Create the IAM Role for ingest with the above trust policy
#
SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE_ARN=$(getRoleArn
    $SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE)
if [ "$SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE_ARN" = "" ];
then
    #
    # Create the IAM role for service account
    #
    SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE_ARN=$(aws iam create-role \
        --role-name $SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE \
        --assume-role-policy-document file://TrustPolicy.json \
        --query "Role.Arn" --output text)
    #
    # Create an IAM permission policy
    #
    SERVICE_ACCOUNT_IAM_AMP_INGEST_ARN=$(aws iam create-policy --policy-name
    $SERVICE_ACCOUNT_IAM_AMP_INGEST_POLICY \
        --policy-document file://PermissionPolicyIngest.json \
        --query 'Policy.Arn' --output text)
    #
    # Attach the required IAM policies to the IAM role created above
    #
    aws iam attach-role-policy \
        --role-name $SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE \
        --policy-arn $SERVICE_ACCOUNT_IAM_AMP_INGEST_ARN
else
```

```
    echo "$SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE_ARN IAM role for ingest already
exists"
fi
echo $SERVICE_ACCOUNT_IAM_AMP_INGEST_ROLE_ARN
#
# EKS cluster hosts an OIDC provider with a public discovery endpoint.
# Associate this IdP with AWS IAM so that the latter can validate and accept the
OIDC tokens issued by Kubernetes to service accounts.
# Doing this with eksctl is the easier and best approach.
#
eksctl utils associate-iam-oidc-provider --cluster $CLUSTER_NAME --approve
```

2. Immetti il seguente comando per assegnare allo script i privilegi necessari.

```
chmod +x createIRSA-AMPIngest.sh
```

3. Eseguire lo script.

## Imposta ruoli IAM per gli account di servizio per le domande delle metriche

Per configurare il ruolo IAM per l'account di servizio (service role) per abilitare l'interrogazione delle metriche dagli spazi di lavoro di Amazon Managed Service for Prometheus, devi accedere a un account con le seguenti autorizzazioni:

- iam:CreateRole
- iam:CreatePolicy
- iam:GetRole
- iam:AttachRolePolicy
- iam:GetOpenIDConnectProvider

Configurare ruoli di servizio per l'interrogazione delle metriche di Amazon Managed Service for Prometheus;

1. Creare un archivio denominato `createIRSA-AMPQuery.sh` con i seguenti contenuti.  
<my\_amazon\_eks\_clustername>Sostituiscilo con il nome del tuo cluster e sostituiscilo <my\_prometheus\_namespace>con il tuo namespace Prometheus.

```
#!/bin/bash -e
CLUSTER_NAME=<my_amazon_eks_clustername>
```

```

SERVICE_ACCOUNT_NAMESPACE=<my_prometheus_namespace>
AWS_ACCOUNT_ID=$(aws sts get-caller-identity --query "Account" --output text)
OIDC_PROVIDER=$(aws eks describe-cluster --name $CLUSTER_NAME --query
  "cluster.identity.oidc.issuer" --output text | sed -e "s/^https://\//")
SERVICE_ACCOUNT_AMP_QUERY_NAME=amp-iamproxy-query-service-account
SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE=amp-iamproxy-query-role
SERVICE_ACCOUNT_IAM_AMP_QUERY_POLICY=AMPQueryPolicy
#
# Setup a trust policy designed for a specific combination of K8s service account
  and namespace to sign in from a Kubernetes cluster which hosts the OIDC Idp.
#
cat <<EOF > TrustPolicy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::${AWS_ACCOUNT_ID}:oidc-provider/
${OIDC_PROVIDER}"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "${OIDC_PROVIDER}:sub": "system:serviceaccount:
${SERVICE_ACCOUNT_NAMESPACE}:${SERVICE_ACCOUNT_AMP_QUERY_NAME}"
        }
      }
    }
  ]
}
EOF
#
# Set up the permission policy that grants query permissions for all AMP workspaces
#
cat <<EOF > PermissionPolicyQuery.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aps:QueryMetrics",
        "aps:GetSeries",
        "aps:GetLabels",

```

```

        "aps:GetMetricMetadata"
    ],
    "Resource": "*"
}
]
}
EOF

function getRoleArn() {
    OUTPUT=$(aws iam get-role --role-name $1 --query 'Role.Arn' --output text 2>&1)

    # Check for an expected exception
    if [[ $? -eq 0 ]]; then
        echo $OUTPUT
    elif [[ -n $(grep "NoSuchEntity" <<< $OUTPUT) ]]; then
        echo ""
    else
        >&2 echo $OUTPUT
        return 1
    fi
}

#
# Create the IAM Role for query with the above trust policy
#
SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE_ARN=$(getRoleArn
$SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE)
if [ "$SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE_ARN" = "" ];
then
    #
    # Create the IAM role for service account
    #
    SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE_ARN=$(aws iam create-role \
--role-name $SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE \
--assume-role-policy-document file://TrustPolicy.json \
--query "Role.Arn" --output text)
    #
    # Create an IAM permission policy
    #
    SERVICE_ACCOUNT_IAM_AMP_QUERY_ARN=$(aws iam create-policy --policy-name
$SERVICE_ACCOUNT_IAM_AMP_QUERY_POLICY \
--policy-document file://PermissionPolicyQuery.json \
--query 'Policy.Arn' --output text)
    #

```

```
# Attach the required IAM policies to the IAM role create above
#
aws iam attach-role-policy \
  --role-name $SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE \
  --policy-arn $SERVICE_ACCOUNT_IAM_AMP_QUERY_ARN
else
  echo "$SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE_ARN IAM role for query already
exists"
fi
echo $SERVICE_ACCOUNT_IAM_AMP_QUERY_ROLE_ARN
#
# EKS cluster hosts an OIDC provider with a public discovery endpoint.
# Associate this IdP with AWS IAM so that the latter can validate and accept the
OIDC tokens issued by Kubernetes to service accounts.
# Doing this with eksctl is the easier and best approach.
#
eksctl utils associate-iam-oidc-provider --cluster $CLUSTER_NAME --approve
```

2. Immetti il seguente comando per assegnare allo script i privilegi necessari.

```
chmod +x createIRSA-AMPQuery.sh
```

3. Eseguire lo script.

## Utilizzo di Amazon Managed Service for Prometheus con endpoint VPC di interfaccia

Se usi Amazon Virtual Private Cloud (Amazon VPC) per l'hosting delle risorse AWS, puoi stabilire delle connessioni private tra il VPC e Amazon Managed Service for Prometheus. È possibile utilizzare queste connessioni per abilitare Amazon Managed Service for Prometheus. in modo da comunicare con le risorse nel VPC senza accedere all'Internet pubblico.

Amazon VPC è un servizio AWS che puoi utilizzare per avviare risorse AWS in una rete virtuale da te definita. Con un VPC, detieni il controllo delle impostazioni della rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per connettere il VPC a Amazon Managed Service for Prometheus, è necessario definire un endpoint VPC di interfaccia per connettere il VPC ai servizi AWS. L'endpoint offre una connettività scalabile e affidabile a Amazon Managed Service for Prometheus senza richiedere un Internet gateway, un'istanza NAT (Network Address Translation) o una connessione VPN. Per ulteriori informazioni, consulta [Che cos'è Amazon VPC?](#) nella Guida per l'utente Amazon VPC.

Gli endpoint VPC di interfaccia si basano su AWS PrivateLink, una tecnologia AWS che permette la comunicazione privata tra AWS servizi che utilizzano un'interfaccia di rete elastica con indirizzi IP privati. Per ulteriori informazioni, consulta il post del blog [New – AWS PrivateLink for AWS Services](#).

Le informazioni seguenti sono per gli utenti di Amazon VPC. Per informazioni su come iniziare con Amazon VPC, consulta [Come iniziare](#) con Amazon VPC nella Guida per l'utente di Amazon VPC.

## Creazione di un endpoint VPC di interfaccia per Amazon Managed Service per Prometheus

Creazione di un endpoint VPC di interfaccia per iniziare a usare Amazon Managed Service per Prometheus. Scegli tra i seguenti endpoint con nomi di servizio:

- `com.amazonaws.region.aps-workspaces`

Scegli questo nome di servizio per utilizzare le API compatibili con Prometheus. Per ulteriori informazioni, consulta le [API compatibili con Prometheus](#) nella Guida per l'utente di Amazon Managed Service for Prometheus.

- `com.amazonaws.region.aps`

Scegli questo nome di servizio per eseguire attività di gestione dell'area di lavoro. Per ulteriori informazioni, consulta [Le API di Amazon Managed Service for Prometheus](#) nella Guida per l'utente Amazon Managed Service for Prometheus User Guide.

### Note

Se utilizzi `remote_write` in un VPC senza accesso diretto a Internet, devi anche creare un'interfaccia VPC endpoint per AWS Security Token Service, per consentire a sigv4 di funzionare attraverso l'endpoint. Per informazioni sulla creazione di endpoint VPC AWS STS, consulta [Utilizzo degli AWS STS endpoint VPC di interfaccia](#) nella AWS Identity and Access Management Guida per l'utente. Devi impostare AWS STS per l'utilizzo degli [endpoint regionalizzati](#).

Per ulteriori informazioni, incluse istruzioni dettagliate per creare un endpoint VPC di interfaccia, consulta [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di Amazon VPC.

**Note**

Puoi utilizzare le policy degli endpoint VPC per controllare l'accesso al tuo endpoint VPC con interfaccia Amazon Managed Service for Prometheus. Per maggiori informazioni, consulta la prossima sezione.

Se hai creato un endpoint VPC di interfaccia per Amazon Managed Service per Prometheus e hai già dati che vengono trasmessi alle aree di lavoro che si trovano nel VPC, i parametri verranno trasmessi attraverso l'endpoint VPC di interfaccia per impostazione predefinita. Amazon Managed Service for Prometheus utilizza endpoint pubblici o endpoint di interfaccia privati (a seconda di quale siano in uso) per eseguire questa attività.

## Controllo dell'accesso all'endpoint VPC di Amazon Managed Service per Prometheus

Puoi utilizzare le policy degli endpoint VPC per controllare l'accesso al tuo endpoint VPC con interfaccia Amazon Managed Service for Prometheus. Una policy endpoint VPC è una policy della risorsa IAM che viene collegata a un endpoint durante la creazione o la modifica dell'endpoint. Se non colleghi una policy durante la creazione di un endpoint, Amazon VPC collega una policy predefinita che consente l'accesso completo al servizio. Una policy endpoint non esclude né sostituisce policy IAM basate sull'identità o policy specifiche del servizio. Si tratta di una policy separata per controllare l'accesso dall'endpoint al servizio specificato.

Per ulteriori informazioni, consultare [Controllo degli accessi ai servizi con endpoint VPC](#) nella Guida per l'utente di Amazon VPC.

Di seguito è riportato un esempio di una policy endpoint per l'API di Amazon Managed Service for Prometheus. Questa policy consente agli utenti con ruolo che si `PromUser` connettono ad Amazon Managed Service for Prometheus tramite VPC di visualizzare aree di lavoro e gruppi di regole, ma non, ad esempio, di creare o eliminare aree di lavoro.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonManagedPrometheusPermissions",
      "Effect": "Allow",
      "Action": [
        "aps:DescribeWorkspace",
        "aps:DescribeRuleGroupsNamespace",
```

```

        "aps:ListRuleGroupsNamespace",
        "aps:ListWorkspaces"
    ],
    "Resource": "arn:aws:aps:*:*:/workspaces*",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:role/PromUser"
        ]
    }
}
]
}

```

L'esempio seguente mostra una policy che consente l'esito positivo solo delle richieste provenienti da un indirizzo IP specificato nel VPC specificato. Le richieste provenienti da altri indirizzi IP avranno esito negativo.

```

{
  "Statement": [
    {
      "Action": "aps:*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:VpcSourceIp": "192.0.2.123"
        },
        "StringEquals": {
          "aws:SourceVpc": "vpc-555555555555"
        }
      }
    }
  ]
}

```

# Risoluzione dei problemi

Utilizza le sezioni seguenti per risolvere i problemi con il servizio gestito da Amazon per Prometheus.

## Argomenti

- [429 o limita gli errori superati](#)
- [Vedo esempi duplicati](#)
- [Vedo errori sui timestamp dei campioni](#)
- [Viene visualizzato un messaggio di errore relativo a un limite](#)
- [L'output del server Prometheus locale supera il limite.](#)
- [Alcuni dei miei dati non vengono visualizzati](#)

## 429 o limita gli errori superati

Se visualizzi un errore 429 simile al seguente esempio, le tue richieste hanno superato le quote di acquisizione del servizio gestito da Amazon per Prometheus.

```
ts=2020-10-29T15:34:41.845Z caller=dedupe.go:112 component=remote level=error
  remote_name=e13b0c
url=http://iamproxy-external.prometheus.uswest2-prod.eks:9090/workspaces/workspace_id/
api/v1/remote_write
msg="non-recoverable error" count=500 err="server returned HTTP status 429
Too Many Requests: ingestion rate limit (6666.666666666667) exceeded while adding 499
samples and 0 metadata"
```

Se visualizzi un errore 429 simile al seguente esempio, le tue richieste hanno superato la quota del servizio gestito da Amazon per Prometheus per il numero di parametri attivi in un'area di lavoro.

```
ts=2020-11-05T12:40:33.375Z caller=dedupe.go:112 component=remote level=error
  remote_name=aps
url=http://iamproxy-external.prometheus.uswest2-prod.eks:9090/workspaces/workspace_id/
api/v1/remote_write
msg="non-recoverable error" count=500 err="server returned HTTP status 429 Too Many
Requests: user=accountid_workspace_id:
per-user series limit (local limit: 0 global limit: 3000000 actual local limit: 500000)
exceeded"
```

Se visualizzi un errore 400 simile al seguente esempio, le tue richieste hanno superato la quota di Amazon Managed Service for Prometheus per le serie temporali attive. Per informazioni dettagliate su come vengono gestite le quote delle serie temporali attive, consulta [Serie attive \(impostazione predefinita\)](#)

```
ts=2024-03-26T16:50:21.780708811Z caller=push.go:53 level=warn
url=https://aps-workspaces.us-east-1.amazonaws.com/workspaces/workspace_id/api/v1/
remote_write
msg="non-recoverable error" count=500 exemplarCount=0
err="server returned HTTP status 400 Bad Request: maxFailure (quorum) on a given error
family, rpc error: code = Code(400)
desc = addr=10.1.41.23:9095 state=ACTIVE zone=us-east-1a, rpc error: code = Code(400)
desc = user=accountid_workspace_id: per-user series limit of 10000000 exceeded,
Capacity from 2,000,000 to 10,000,000 is automatically adjusted based on the last 30
min of usage.
If throttled above 10,000,000 or in case of incoming surges, please contact
administrator to raise it.
(local limit: 0 global limit: 10000000 actual local limit: 92879)"
```

Per ulteriori informazioni sulle quote del servizio gestito da Amazon per Prometheus e su come richiedere aumenti, consulta [Quote del servizio Amazon Managed Service per Prometheus](#)

## Vedo esempi duplicati

Se utilizzi un gruppo Prometheus ad alta disponibilità, devi utilizzare etichette esterne sulle istanze Prometheus per configurare la deduplicazione. Per ulteriori informazioni, consulta [Deduplicazione dei parametri di disponibilità elevata inviati al servizio gestito da Amazon per Prometheus](#).

Altre questioni relative ai dati duplicati vengono discusse nella sezione successiva.

## Vedo errori sui timestamp dei campioni

Amazon Managed Service for Prometheus inserisce i dati in ordine e prevede che ogni campione abbia un timestamp successivo al campione precedente.

Se i dati non arrivano in ordine, puoi visualizzare errori relativi a, o. `out-of-order samples duplicate sample for timestamp samples with different value but same timestamp` Questi problemi sono in genere causati da una configurazione errata del client che invia dati ad Amazon Managed Service for Prometheus. Se utilizzi un client Prometheus in esecuzione

in modalità agente, controlla la configurazione per le regole con nomi di serie duplicati o obiettivi duplicati. Se le tue metriche forniscono direttamente il timestamp, verifica che non siano errate.

Per maggiori dettagli su come funziona o su come verificare la configurazione, consulta il post del blog [Understanding Duplicate Samples and Out-of-order Timestamp Errors in Prometheus di Prometheus Labs](#).

## Viene visualizzato un messaggio di errore relativo a un limite

### Note

Amazon Managed Service for Prometheus fornisce [metriche di utilizzo per monitorare l'CloudWatch utilizzo](#) delle risorse di Prometheus. Utilizzando la funzione di allarme delle metriche di CloudWatch utilizzo, è possibile monitorare le risorse e l'utilizzo di Prometheus per evitare errori limite.

Se visualizzi uno dei seguenti messaggi di errore, puoi richiedere un aumento di una delle quote del servizio gestito da Amazon per Prometheus per risolvere il problema. Per ulteriori informazioni, consulta [Quote del servizio Amazon Managed Service per Prometheus](#).

- limite di serie per utente di `<value>` superato, contatta l'amministratore per aumentarlo
- limite di serie per utente di `<value>` superato, contatta l'amministratore per aumentarlo
- limite della frequenza di acquisizione (...) superato
- la serie ha troppe etichette (...) serie: '%s'
- l'intervallo di tempo della domanda supera il limite (lunghezza della domanda: xxx, limite: yyy)
- la domanda ha raggiunto il limite massimo di blocchi durante il recupero di blocchi dalle acquisizioni
- Limite superato. Numero massimo di workspace per account.

## L'output del server Prometheus locale supera il limite.

Il servizio gestito da Amazon per Prometheus prevede quote del servizio per la quantità di dati che un'area di lavoro può ricevere dai server Prometheus. Per trovare la quantità di dati che il tuo server Prometheus sta inviando al servizio gestito da Amazon per Prometheus, puoi porre le seguenti domande sul tuo server Prometheus. Se scopri che la tua produzione Prometheus supera il limite

del servizio gestito da Amazon per Prometheus, puoi richiedere un aumento della quota del servizio corrispondente. Per ulteriori informazioni, consulta [Quote del servizio Amazon Managed Service per Prometheus](#).

Interroga il server Prometheus locale a esecuzione automatica per trovare i limiti di output.

Tipo di dato	Domanda da utilizzare
Serie attiva attuale	<code>prometheus_tsdb_head_series</code>
Frequenza di acquisizione attuale	<code>rate(prometheus_tsdb_head_samples_appended_total[5m])</code>
ost-to-least Elenco M di serie attive per nome metrico	<code>sort_desc(count by(__name__){__name__!=""})</code>
Numero di etichette per serie di parametri	<code>group by(mylabelname){__name__!=""})</code>

## Alcuni dei miei dati non vengono visualizzati

I dati inviati ad Amazon Managed Service for Prometheus possono essere scartati per vari motivi. La tabella seguente mostra i motivi per cui i dati potrebbero essere eliminati anziché essere ingeriti.

Puoi tenere traccia della quantità e dei motivi per cui i dati vengono scartati utilizzando Amazon CloudWatch. Per ulteriori informazioni, consulta [CloudWatch metriche](#).

Motivo	Significato
greater_than_max_sample_age	Eliminare le righe di registro più vecchie dell'ora corrente
new-value-for-timestamp	I campioni duplicati vengono inviati con un timestamp diverso da quello registrato in precedenza
per_metric_series_limit	L'utente ha raggiunto il limite delle serie attive per parametro
per_user_series_limit	L'utente ha raggiunto il limite totale di serie attive
rate_limited	Frequenza di acquisizione limitata
sample-out-of-order	I campioni sono stati inviati fuori servizio e non possono essere elaborati
label_value_too_long	Il valore dell'etichetta è più lungo del limite di caratteri consentito
max_label_names_per_series	L'utente ha raggiunto i nomi delle etichette per parametro
missing_metric_name	Il nome del parametro non è stato fornito
metric_name_invalid	Nome parametro non valido
label_invalid	Etichetta non valida
duplicate_label_names	Forniti nomi di etichette duplicati

# Assegnazione di tag

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

- Una chiave di tag (ad esempio, `CostCenter`, `Environment`, `Project` o `Secret`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un campo facoltativo noto come valore del tag (ad esempio, `111122223333`, `Production` o un nome di team). 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.

Tutti questi sono noti come coppie chiave-valore. Puoi assegnare fino a 50 tag a ogni area di lavoro.

I tag aiutano a identificare e a organizzare le risorse AWS. Molti servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono correlate. Ad esempio, puoi assegnare a un workspace Amazon Managed Service for Prometheus lo stesso tag che assegni a un bucket Amazon S3. Per ulteriori informazioni sulle strategie di tag, consulta [Tag delle AWS risorse](#).

In Amazon Managed Service for Prometheus, è possibile contrassegnare sia nelle aree di lavoro che i namespace dei gruppi di regole. È possibile utilizzare la console, AWS CLI, le API o gli SDK per aggiungere, gestire o rimuovere i tag per queste risorse. Oltre a identificare, organizzare e tracciare i tuoi spazi di lavoro e i gruppi di regole con i tag, puoi usare i tag nelle policy IAM per controllare chi può visualizzare e interagire con le tue risorse Amazon Managed Service for Prometheus.

## Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- 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.
- Se lo schema di assegnazione dei tag viene utilizzato in più servizi e risorse AWS, tieni presente che altri servizi potrebbero prevedere limitazioni sui caratteri consentiti. I caratteri solitamente

consentiti sono lettere, numeri, spazi rappresentabili in formato UTF-8, oltre ai seguenti caratteri: . : + = @ \_ / - (trattino).

- 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.
- Non utilizzare `aws :`, `AWS :` o qualsiasi combinazione di maiuscole o minuscole di un tale prefisso per chiavi o valori. Questi sono riservati solo all'utilizzo di 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 il limite del numero di tag per risorsa.

## Argomenti

- [Taggare le aree di lavoro](#)
- [Tag dei namespace dei gruppi di regole.](#)

## Taggare le aree di lavoro

Utilizza le procedure descritte in questa sezione per utilizzare i tag per le aree di lavoro di Amazon Managed Service for Prometheus.

## Argomenti

- [Aggiunta di tag a un'area di lavoro](#)
- [Visualizzazione dei tag per un'area di lavoro](#)
- [Come modificare i tag per un'area di lavoro](#)
- [Rimuovi un tag da un'area di lavoro](#)

## Aggiunta di tag a un'area di lavoro

L'aggiunta di tag ad Amazon Managed Service for Prometheus un progetto può aiutarti a identificare e organizzare le risorse AWS e gestirne l'accesso. In primo luogo, è possibile aggiungere uno o più tag (coppie chiave-valore) a un'area di lavoro. Dopo aver ottenuto i tag, puoi creare policy IAM per gestire l'accesso all'area di lavoro in base a questi tag. Puoi utilizzare la console o AWS CLI aggiungere i tag a un'area di lavoro Amazon Managed Service for Prometheus.

**⚠ Important**

L'aggiunta di tag a un'area di lavoro può influire sull'accesso a quell'area di lavoro. Prima di aggiungere un tag a un gruppo di report, assicurati di rivedere le policy IAM che potrebbero usare i tag per controllare l'accesso alle risorse.

Per ulteriori informazioni sull'aggiunta di tag a un'area di lavoro Amazon Managed Service for Prometheus al momento della creazione, consulta [Creare un'area di lavoro](#).

**Argomenti**

- [Aggiunta di tag a un'area di lavoro \(console\)](#)
- [Aggiunta di un tag a un'area di lavoro \(AWS CLI\)](#)

**Aggiunta di tag a un'area di lavoro (console)**

Puoi utilizzare la console per aggiungere uno o più tag a un'area di lavoro Amazon Managed Service for Prometheus.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Seleziona la scheda Tags (Tag).
6. Se non sono stati aggiunti tag all'area di lavoro di Amazon Managed Service for Prometheus, scegli Crea tag. Altrimenti, scegli Gestisci tag.
7. Per Key (Chiave), inserire un nome per il tag. È possibile aggiungere un valore facoltativo al tag in Value (Valore).
8. (Facoltativo) Per aggiungere un altro tag, scegliere Add tag (Aggiungi tag) .
9. Una volta completata l'aggiunta di tag, scegli Salva modifiche.

## Aggiunta di un tag a un'area di lavoro (AWS CLI)

Segui questi passaggi per aggiungere un tag AWS CLI a un'area di lavoro Amazon Managed Service for Prometheus. Per aggiungere un tag a un'area di lavoro al momento della creazione, consulta [Creare un'area di lavoro](#).

In queste fasi, si assume che sia già installata una versione recente della AWS CLI o che sia aggiornata alla versione corrente. Per ulteriori informazioni, consulta l'argomento relativo all'[installazione di AWS Command Line Interface](#).

Al terminale o alla riga di comando, eseguir il comando `tag-resource`, specificando l'Amazon Resource Name (ARN) dell'area di lavoro in cui aggiungere i tag e la chiave e il valore del tag che desideri aggiungere. Puoi aggiungere più di un tag a un'area di lavoro. Ad esempio, per etichettare un'area di lavoro Amazon Managed Service for Prometheus denominata My-Workspace con due tag, una chiave di tag denominata *Status* con il valore del tag *Secret* e una chiave di tag denominata *Team* con il valore del tag *My-Team*:

```
aws amp tag-resource --resource-arn arn:aws:aps:us-  
west-2:123456789012:workspace/IDstring  
--tags Status=Secret,Team=My-Team
```

In caso di successo, questo comando non restituisce alcun risultato.

## Visualizzazione dei tag per un'area di lavoro

I tag possono aiutarti a identificare e organizzare le risorse AWS e gestirne l'accesso. Per ulteriori informazioni sulle strategie di tag, consulta [Tag delle AWS risorse](#).

### Visualizzazione dei tag per un'area di lavoro Amazon Managed Service for Prometheus (console)

Puoi utilizzare la console per visualizzare i tag associati a un'area di lavoro Amazon Managed Service for Prometheus.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.

4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Seleziona la scheda Tags (Tag).

## Visualizza i tag di un'area di lavoro Amazon Managed Service for Prometheus (AWS CLI)

Segui questa procedura per utilizzare la AWS CLI per visualizzare i AWS tag per un'area di lavoro. Se non sono stati aggiunti tag, l'elenco restituito è vuoto.

Dal terminale o dalla riga di comando, esegui il comando `list-tags-for-resource`. Ad esempio, per visualizzare un elenco di valori di chiavi e di tag per un'area di lavoro:

```
aws amp list-tags-for-resource --resource-arn arn:aws:aps:us-  
west-2:123456789012:workspace/IDstring
```

Se il comando viene eseguito correttamente, restituisce informazioni simili alle seguenti:

```
{  
  "tags": {  
    "Status": "Secret",  
    "Team": "My-Team"  
  }  
}
```

## Come modificare i tag per un'area di lavoro

È possibile modificare il valore di un tag associato a un'area di lavoro. È anche possibile modificare il nome della chiave. Questa operazione equivale alla sostituzione del tag esistente con un tag differente che ha un nuovo nome ma lo stesso valore dell'altra chiave.

### Important

Come modificare i tag per un'area di lavoro Amazon Managed Service for Prometheus. Prima di modificare il nome (chiave) o il valore di un tag per un'area di lavoro, assicurati di rivedere le policy IAM che potrebbero utilizzare la chiave o il valore di un tag per controllare l'accesso alle risorse, ad esempio i repository.

## Come modificare un tag per un'area di lavoro Amazon Managed Service for Prometheus (console)

Puoi utilizzare la console per modificare i tag associati a un'area di lavoro Amazon Managed Service for Prometheus.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Seleziona la scheda Tags (Tag).
6. Se non sono stati aggiunti tag all'area di lavoro, scegliere Crea tag. Altrimenti, scegli Gestisci tag.
7. Per Key (Chiave), inserire un nome per il tag. È possibile aggiungere un valore facoltativo al tag in Value (Valore).
8. (Facoltativo) Per aggiungere un altro tag, scegliere Add tag (Aggiungi tag) .
9. Una volta completata l'aggiunta di tag, scegli Salva modifiche.

## Modificare i tag di un'area di lavoro Amazon Managed Service for Prometheus (AWS CLI)

Segui questa procedura per utilizzare AWS CLI per aggiornare un tag per un'area di lavoro. È possibile modificare il valore di una chiave esistente o aggiungere un'altra chiave.

Al terminale o nella riga di comando, esegui il comando `tag-resource` specificando l'Amazon Resource Name (ARN) dell'area di lavoro Amazon Managed Service for Prometheus in cui desideri aggiornare un tag e specificare la chiave e il valore di tag:

```
aws amp tag-resource --resource-arn arn:aws:aps:us-west-2:123456789012:workspace/IDstring --tags Team=New-Team
```

## Rimuovi un tag da un'area di lavoro

Puoi rimuovere uno o più tag associati a un'area di lavoro. La rimozione di un tag non elimina il tag da altre risorse AWS associate a tale tag.

**⚠ Important**

La rimozione dei tag per un'area di lavoro di Amazon Managed Service for Prometheus può influire sull'accesso a tale area di lavoro. Prima di rimuovere un tag da un repository, assicurati di rivedere tutte le policy IAM che potrebbero utilizzare la chiave o il valore di un tag per controllare l'accesso alle risorse, ad esempio ai repository.

## Rimuovere un tag da un'area di lavoro Amazon Managed Service for Prometheus (console)

Puoi utilizzare la console per rimuovere l'associazione tra un tag e un'area di lavoro.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Seleziona la scheda Tags (Tag).
6. Scegliere Gestisci tag.
7. Trova il tag che desideri eliminare e scegli Rimuovi.

## Rimuovere un'area di lavoro Amazon Managed Service for Prometheus (AWS CLI)

Segui queste fasi per utilizzare AWS CLI per rimuovere un tag da un'area di lavoro. La rimozione di un tag non lo elimina completamente, ma rimuove semplicemente l'associazione tra il tag e l'area di lavoro.

**ℹ Note**

Se elimini un'area di lavoro Amazon Managed Service for Prometheus, tutte le associazioni di tag vengono rimosse dall'area di lavoro eliminata. Non è necessario rimuovere i tag prima di eliminare un'area di lavoro.

Al terminale o nella riga di comando, eseguire il comando `untag-resource` specificando l'Amazon Resource Name (ARN) del repository da cui desideri rimuovere i tag e la relativa chiave. Ad esempio, per rimuovere un tag da un'area di lavoro denominata `My-Workspace` con la chiave tag `Status`:

```
aws amp untag-resource --resource-arn arn:aws:aps:us-  
west-2:123456789012:workspace/IDstring --tag-keys Status
```

In caso di successo, questo comando non restituisce alcun risultato. Per verificare i tag associati all'area di lavoro, esegui il comando `list-tags-for-resource`.

## Tag dei namespace dei gruppi di regole.

Utilizza le procedure in questa sezione per lavorare con i tag per i namespace dei gruppi di regole di Amazon Managed Service for Prometheus.

### Argomenti

- [Aggiungi un tag a un namespace dei gruppi di regole](#)
- [Visualizzazione dei tag per un namespace dei gruppi di regole](#)
- [Modifica i tag per un namespace dei gruppi di regole](#)
- [Rimuovere un tag da un namespace dei gruppi di regole](#)

## Aggiungi un tag a un namespace dei gruppi di regole

L'aggiunta di tag a un namespace dei gruppi di lavoro Amazon Managed Service for Prometheus può aiutarti a identificare e organizzare le risorse AWS e gestirne l'accesso. In primo luogo, puoi aggiungere uno o più tag (coppie chiave-valore) a un namespace dei gruppi di regole. Dopo aver ottenuto i tag, è possibile creare policy IAM per gestire l'accesso al namespace in base a questi tag. Puoi utilizzare la console o aggiungere tag AWS CLI a un namespace dei gruppi di regole Amazon Managed Service for Prometheus.

### Important

L'aggiunta di tag a un namespace dei gruppo di regole può influire sull'accesso a tale namespace dei gruppi di regole. Prima di aggiungere un tag, assicurati di rivedere le policy IAM che potrebbero usare i tag per controllare l'accesso alle risorse.

Per ulteriori informazioni sull'aggiunta di tag a un namespace dei gruppi di regole al momento della creazione, consulta [Creazione di un file di regole](#).

## Argomenti

- [Aggiungi un tag a un namespace dei gruppi di regole \(console\)](#)
- [Aggiungi un tag a un namespace dei gruppi di regole \(AWS CLI\)](#)

## Aggiungi un tag a un namespace dei gruppi di regole (console)

Puoi utilizzare la console per aggiungere uno o più tag a un namespace dei gruppi di regole di Amazon Managed Service for Prometheus.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Scegli la scheda Gestione delle regole.
6. Scegli il pulsante accanto al nome del namespace e scegli Modifica.
7. Seleziona Crea tag, Aggiungi un nuovo tag.
8. Per Key (Chiave), inserire un nome per il tag. È possibile aggiungere un valore facoltativo al tag in Value (Valore).
9. (Facoltativo) Per aggiungere un altro tag, scegli di nuovo Aggiungi nuovo tag.
10. Una volta completata l'aggiunta di tag, scegli Salva modifiche.

## Aggiungi un tag a un namespace dei gruppi di regole (AWS CLI)

Segui questi passaggi AWS CLI per aggiungere un tag a un namespace dei gruppi di regole Amazon Managed Service for Prometheus. Per aggiungere un tag a un namespace dei gruppi di regole durante la creazione, consulta [Caricamento di un file di configurazione delle regole nel servizio gestito da Amazon per Prometheus](#).

In queste fasi, si assume che sia già installata una versione recente della AWS CLI o che sia aggiornata alla versione corrente. Per ulteriori informazioni, consulta l'argomento relativo all'[installazione di AWS Command Line Interface](#).

Al terminale o alla riga di comando, esegui il comando `tag-resource`, specificando l'Amazon Resource Name (ARN) del namespace dei gruppi di regole in cui aggiungere i tag e la chiave e il valore del tag che desideri aggiungere. È possibile aggiungere più di un tag al namespace dei gruppi di regole. Ad esempio, per taggare un namespace Amazon Managed Service for Prometheus denominato `My-Workspace` con due tag, una chiave di tag denominata `Status` con il valore del tag `Secret` e una chiave di tag denominata `Team` con il valore del tag `My-Team`:

```
aws amp tag-resource \  
  --resource-arn arn:aws:aps:us-  
west-2:123456789012:rulegroupsnamespace/IDstring/namespace_name \  
  --tags Status=Secret,Team=My-Team
```

In caso di successo, questo comando non restituisce alcun risultato.

## Visualizzazione dei tag per un namespace dei gruppi di regole

I tag possono aiutarti a identificare e organizzare le risorse AWS e gestirne l'accesso. Per ulteriori informazioni sulle strategie di tag, consulta [Tag delle AWS risorse](#).

### Visualizza i tag per un namespace dei gruppi di regole di Amazon Managed Service for Prometheus (console)

Puoi utilizzare la console per visualizzare i tag associati a un namespace dei gruppi di regole di Amazon Managed Service for Prometheus.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Scegli la scheda Gestione delle regole.
6. Scegli il nome del namespace.

### Visualizza i tag di un'area di lavoro Amazon Managed Service for Prometheus (AWS CLI)

Segui questa procedura per utilizzare AWS CLI per visualizzare i tag AWS per un namespace dei gruppi di regole. Se non sono stati aggiunti tag, l'elenco restituito è vuoto.

Dal terminale o dalla riga di comando, esegui il comando `list-tags-for-resource`. Ad esempio, per visualizzare un elenco di chiavi di tag e valori di tag per un namespace dei gruppi di regole:

```
aws amp list-tags-for-resource --resource-arn rn:aws:aps:us-  
west-2:123456789012:rulegroupsnamespace/IDstring/namespace_name
```

Se il comando viene eseguito correttamente, restituisce informazioni simili alle seguenti:

```
{  
  "tags": {  
    "Status": "Secret",  
    "Team": "My-Team"  
  }  
}
```

## Modifica i tag per un namespace dei gruppi di regole

È possibile modificare il valore di un tag associato a un namespace dei gruppi di regole. È anche possibile modificare il nome della chiave. Questa operazione equivale alla sostituzione del tag esistente con un tag differente che ha un nuovo nome ma lo stesso valore dell'altra chiave.

### Important

La modifica dei tag per un namespace dei gruppi di regole può influire sull'accesso a tale spazio. Prima di modificare il nome (chiave) o il valore di un tag per una risorsa, assicurati di rivedere tutte le policy IAM che potrebbero utilizzare la chiave o il valore di un tag per controllare l'accesso alle risorse.

## Modifica un tag per un namespace dei gruppi di regole Amazon Managed Service for Prometheus (console)

Puoi utilizzare la console per modificare i tag associati a un namespace dei gruppi di regole di Amazon Managed Service for Prometheus.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.

3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Scegli la scheda Gestione delle regole.
6. Scegli il nome dello spazio dei nomi.
7. Scegli Gestisci tag, Aggiungi nuovo tag.
8. Per modificare il valore di un tag esistente, inserisci il nuovo valore in Valore.
9. o aggiungi un altro tag, scegli Aggiungi nuovo tag.
10. Una volta completata l'aggiunta di tag, scegli Salva modifiche.

## Modifica i tag per un namespace dei gruppi di regole Amazon Managed Service for Prometheus (AWS CLI)

Segui questa procedura per utilizzare la AWS CLI per aggiornare un tag per un namespace dei gruppi di regole. È possibile modificare il valore di una chiave esistente o aggiungere un'altra chiave.

Al terminale o nella riga di comando, esegui il comando `tag-resource` specificando l'Amazon Resource Name (ARN) della risorsa in cui desideri aggiornare un tag e specificare la chiave e il valore di tag:

```
aws amp tag-resource --resource-arn rn:aws:aps:us-west-2:123456789012:rulegroupsnamespace/IDstring/namespace_name --tags Team=New-Team
```

## Rimuovere un tag da un namespace dei gruppi di regole

È possibile rimuovere uno o più tag associati a un namespace dei gruppi di regole. La rimozione di un tag non elimina il tag da altre risorse AWS associate a tale tag.

### Important

La rimozione dei tag per una risorsa può influire sull'accesso a tale risorsa. Prima di rimuovere un tag da una risorsa, assicurati di rivedere tutte le policy IAM che potrebbero utilizzare la chiave o il valore di un tag per controllare l'accesso alle risorse, ad esempio ai repository.

## Rimuovere un tag da un namespace dei gruppi di regole di Amazon Managed Service for Prometheus (console)

È possibile utilizzare la console per rimuovere l'associazione tra un tag e un namespace dei gruppi di lavoro.

1. Apri la console Amazon Managed Service for Prometheus all'indirizzo <https://console.aws.amazon.com/prometheus/>.
2. Nel riquadro di navigazione, seleziona l'icona del menu.
3. Seleziona Tutte le aree di lavoro.
4. Scegli l'ID dell'area di lavoro che desideri gestire.
5. Scegli la scheda Gestione delle regole.
6. Scegli il nome dello spazio dei nomi.
7. Scegliere Gestisci tag.
8. Scegli Rimuovi accanto al tag che desideri eliminare.
9. Al termine, scegli Salva le modifiche.

## Rimuovere un tag da un namespace dei gruppi di regole di Amazon Managed Service for Prometheus (AWS CLI)

Segui questa procedura per utilizzare AWS CLI per rimuovere un tag da un namespace di un gruppo di regole. La rimozione di un tag non lo elimina completamente, ma rimuove semplicemente l'associazione tra il tag e il namespace dei gruppi di regole.

### Note

Se elimini un namespace dei gruppi di regole Amazon Managed Service for Prometheus, tutte le associazioni di tag vengono rimosse dal namespace eliminato. Non è necessario rimuovere i tag prima di eliminare un namespace.

Al terminale o nella riga di comando, eseguire il comando `untag-resource` specificando l'Amazon Resource Name (ARN) del namespace dei gruppi di lavoro da cui desideri rimuovere i tag e la relativa chiave. Ad esempio, per rimuovere un tag da un'area di lavoro denominata My-Workspace con la chiave tag *Status*:

```
aws amp untag-resource --resource-arn arn:aws:aps:us-west-2:123456789012:rulegroupsnamespace/IDstring/namespace_name --tag-keys Status
```

In caso di successo, questo comando non restituisce alcun risultato. Per verificare i tag associati alla risorsa, eseguire il comando `list-tags-for-resource`.

# Quote del servizio Amazon Managed Service per Prometheus

Le due sezioni seguenti descrivono le quote e i limiti associati ad Amazon Managed Service for Prometheus.

## Quote del servizio

Amazon Managed Service for Prometheus prevede le seguenti quote. Amazon Managed Service for Prometheus fornisce metriche di utilizzo per monitorare l'[utilizzo](#) delle risorse di PrometheusCloudWatch . Utilizzando la funzione di allarme delle metriche di CloudWatch utilizzo, è possibile monitorare le risorse e l'utilizzo di Prometheus per evitare errori limite.

Man mano che i tuoi progetti e le tue aree di lavoro crescono, le quote più comuni che potresti dover monitorare o richiedere un aumento sono: Serie attiva per area di lavoro, tasso di importazione per area di lavoro e Dimensione del burst di importazione per area di lavoro.

Per tutte le quote regolabili, puoi richiedere un aumento della quota selezionando il link nella colonna Regolabile o [richiedendo un aumento della quota](#).

Il limite della serie attiva per area di lavoro viene applicato dinamicamente. Per ulteriori informazioni, consulta [Serie attive \(impostazione predefinita\)](#). La velocità di ingestione per area di lavoro e la dimensione di ingestione burst per area di lavoro controllano insieme la velocità con cui è possibile importare i dati nell'area di lavoro. Per ulteriori informazioni, consulta [Limitazione dell'ingestione](#).

### Note

Salvo diversa indicazione, queste quote si intendono per area di lavoro.

Nome	Predefinita	Adattabile	Descrizione
Parametri attivi con metadati per area di lavoro	Ogni regione supportata: 20.000	No	Numero di parametri attivi univoci con metadati per area di lavoro: 20.000

Nome	Predefinita	Adattate	Descrizione
Serie attive per area di lavoro	Ogni regione supportata: 10.000.000 per 2 ore	<a href="#">Sì</a>	Il numero di serie attive univoche per area di lavoro. Una serie è attiva se un campione è stato segnalato nelle ultime 2 ore. La capacità da 2 M a 10 M viene regolata automaticamente in base agli ultimi 30 minuti di utilizzo.
Dimensione del gruppo di aggregazione avvisi nel file di definizione di alert manager	Ogni regione supportata: 1.000	<a href="#">Sì</a>	La dimensione massima di un gruppo di aggregazione degli avvisi nel file di definizione di alert manager. Ogni combinazione di valori di etichetta di group_by creerebbe un gruppo di aggregazione.
Dimensione del file di definizione del gestore avvisi	Ogni regione supportata: 1 MB	No	Dimensione massima di un file di definizione di alert manager.
Avvisa la dimensione del payload in Alert Manager	Ogni regione supportata: 20 MB	No	La dimensione massima del payload degli avvisi di Alert Manager per area di lavoro. La dimensione e degli avvisi dipende dalle etichette e dalle annotazioni.

Nome	Predefinita	Adatta	Descrizione
Avvisi in Alert Manager	Ogni regione supportata: 1.000	<a href="#">Sì</a>	Il numero massimo di avvisi simultanei di Alert Manager per area di lavoro.
Cluster di tracker HA	Ogni regione supportata: 500	No	Il numero massimo di cluster di cui il tracker HA terrà traccia per i campioni ingeriti per area di lavoro.
Dimensione burst delle importazioni per area di lavoro	Ogni regione supportata: 1.000.000	<a href="#">Sì</a>	Il numero massimo di campioni che possono essere importati per area di lavoro in un'unica sequenza al secondo.
Tasso di importazione per area di lavoro	Ogni regione supportata: 170.000	<a href="#">Sì</a>	Frequenza dei parametri di importazione dei campioni per area di lavoro al secondo.
Regole di inibizione nel file di definizione di alert manager	Ogni regione supportata: 100	<a href="#">Sì</a>	Il numero massimo di regole di inibizione nel file di definizione di alert manager.
Dimensione etichetta	Ogni regione supportata: 7 KB	No	La dimensione massima combinata di tutte le etichette e i valori di etichetta accettati per una serie.
Etichette per serie di parametri	Ogni regione supportata: 70	<a href="#">Sì</a>	Numero di etichette per serie dei parametri.

Nome	Predefinita	Adatta e	Descrizione
Lunghezza dei metadati	Ogni regione supportata: 1 KB	No	La lunghezza massima accettata per i parametri dei metadati I metadati si riferiscono a Metric Name, HELP e UNIT.
Metadati per parametro	Ogni regione supportata: 10	No	Numero di metadati per parametro.
Nodi nell'albero di instradamento di alert manager	Ogni regione supportata: 100	<a href="#">Sì</a>	Il numero massimo di nodi nell'albero di instradamento di alert manager.
Numero di operazioni API nelle transazioni al secondo	Ogni regione supportata: 10	<a href="#">Sì</a>	Il numero massimo di richieste di operazioni API che è possibile effettuare e al secondo per regione. Ciò include le API CRUD dell'area di lavoro, le API di tag, le API CRUD del namespace dei gruppi di regole e le API CRUD per la definizione di alert manager.
Byte di query per query istantanee	Ogni regione supportata: 5 GB	No	I byte massimi che possono essere scansionati da una singola query istantanea

Nome	Predefinita	Adattate	Descrizione
Byte di query per query di intervallo	Ogni regione supportata: 5 GB	No	I byte massimi che possono essere scansionati per intervallo di 24 ore in una query a intervallo singolo.
Blocchi di query recuperati	Ogni regione supportata: 20.000.000	No	Il numero massimo di blocchi che possono essere scansionati durante una singola query.
Esempi di query	Ogni regione supportata: 50.000.000	No	Il numero massimo di campioni che possono essere scansionati durante una singola query.
Serie di query recuperata	Ogni regione supportata: 12.000.000	No	Il numero massimo di serie che possono essere scansionati durante una singola query.
Intervallo di tempo delle query in giorni	Ogni regione supportata: 32	No	L'intervallo di tempo massimo di qualsiasi query PromQL.
Dimensione richiesta	Ogni regione supportata: 1 MB	No	La dimensione massima dell'importazione o della richiesta di query.

Nome	Predefinita	Adattate	Descrizione
Tempo di conservazione per i dati importati in giorni	Ogni regione supportata: 150	<a href="#">Sì</a>	Il numero di giorni per cui vengono conservati i dati in un'area di lavoro. I dati più vecchi vengono eliminati. È possibile richiedere modifiche alle quote per aumentare o diminuire questo valore.
Intervallo di valutazione delle regole	Ogni regione supportata: 30 secondi	<a href="#">Sì</a>	L'intervallo minimo di valutazione delle regole di un gruppo di regole per area di lavoro.
Dimensione del file di definizione del namespace del gruppo di regole	Ogni regione supportata: 1 MB	No	La dimensione massima di un file di definizione del namespace di un gruppo di regole.
Regole per area di lavoro	Ogni regione supportata: 2.000	<a href="#">Sì</a>	Il numero massimo di regole per area di lavoro.
Modelli nel file di definizione di alert manager	Ogni regione supportata: 100	<a href="#">Sì</a>	Il numero massimo di modelli nel file di definizione di alert manager.
Area di lavoro per regione per account	Ogni regione supportata: 25	<a href="#">Sì</a>	Il numero massimo di aree di lavoro per regione.

## Serie attive (impostazione predefinita)

Amazon Managed Service for Prometheus ti consente di utilizzare per impostazione predefinita fino alla tua quota di serie temporali attive.

Le aree di lavoro di Amazon Managed Service for Prometheus si adattano automaticamente al tuo volume di importazione. All'aumentare dell'utilizzo, Amazon Managed Service for Prometheus aumenterà automaticamente la capacità delle serie temporali per raddoppiare l'utilizzo di base, fino alla quota predefinita. Ad esempio, se la tua serie temporale attiva media degli ultimi 30 minuti è 3,5 milioni, puoi utilizzare fino a 7 milioni di serie storiche senza limitazioni.

Se hai bisogno di più del doppio della linea di base precedente, Amazon Managed Service for Prometheus alloca automaticamente più capacità all'aumentare del volume di importazione, per garantire che il carico di lavoro non subisca una limitazione sostenuta, fino a raggiungere la tua quota. Tuttavia, il throttling può verificarsi se si eccede del doppio la precedente linea di base calcolata negli ultimi 30 minuti. Per evitare limitazioni, Amazon Managed Service for Prometheus consiglia di aumentare gradualmente l'importazione quando si arriva a più del doppio delle precedenti serie temporali attive.

#### Note

La capacità minima per le serie temporali attive è di 2 milioni, non è prevista alcuna limitazione quando si hanno meno di 2 milioni di serie.

Per superare la quota predefinita, puoi richiedere un aumento della quota.

## Limitazione dell'ingestione

Amazon Managed Service for Prometheus limita l'ingestione per ogni area di lavoro, in base ai tuoi limiti attuali. Questo aiuta a mantenere le prestazioni dell'area di lavoro. Se superi il limite, lo vedrai `DiscardedSamples` nelle CloudWatch metriche (con il `rate_limited` motivo). Puoi usare Amazon CloudWatch per monitorare l'ingestione e creare un allarme per avvisarti quando stai per raggiungere i limiti di limitazione. Per ulteriori informazioni, consulta [CloudWatch metriche](#).

Amazon Managed Service for Prometheus utilizza l'algoritmo [token bucket per implementare il throttling dell'ingestione](#). Con questo algoritmo, il tuo account dispone di un bucket che contiene un numero specifico di token. Il numero di token nel bucket rappresenta il limite di ingestione in un dato secondo.

Ogni campione di dati ingerito rimuove un token dal bucket. Se la dimensione del bucket (dimensione del burst di Ingestion per workspace) è 1.000.000, lo spazio di lavoro può importare un milione di campioni di dati in un secondo. Se supera il milione di campioni da importare, verrà limitato e non inserirà più record. I campioni di dati aggiuntivi verranno eliminati.

Il secchio si ricarica automaticamente a una velocità prestabilita. Se il bucket è al di sotto della sua capacità massima, gli viene aggiunto un determinato numero di token ogni secondo fino a raggiungere la capacità massima. Se il secchio è pieno quando arrivano i gettoni di ricarica, questi vengono scartati. Il bucket non può contenere più del numero massimo di token. La frequenza di ricarica per l'ingestione del campione è impostata dal limite della frequenza di ingestione per area di lavoro. Se la frequenza di ingestione per area di lavoro è impostata su 170.000, la frequenza di ricarica per il bucket è di 170.000 token al secondo.

Se il tuo spazio di lavoro acquisisce 1.000.000 di campioni di dati in un secondo, il tuo bucket viene immediatamente ridotto a zero token. Il bucket viene quindi ricaricato con 170.000 token ogni secondo, fino a raggiungere la capacità massima di 1.000.000 di token. Se non viene più effettuata alcuna operazione di ingestione, il bucket precedentemente vuoto tornerà alla sua capacità massima in 6 secondi.

### Note

L'ingestione avviene in richieste in batch. Se hai 100 token disponibili e invii una richiesta con 101 campioni, l'intera richiesta viene rifiutata. Amazon Managed Service for Prometheus non accetta richieste parzialmente. Se stai scrivendo un raccogliitore, puoi gestire i nuovi tentativi (con batch più piccoli o dopo un certo periodo di tempo).

Non è necessario attendere che il bucket sia pieno prima che l'area di lavoro possa importare altri campioni di dati. È possibile utilizzare i token man mano che vengono aggiunti al bucket. Se si utilizzano immediatamente i gettoni di ricarica, il secchio non raggiunge la sua capacità massima. Ad esempio, se esaurisci il bucket, puoi continuare a importare 170.000 campioni di dati al secondo. Il bucket può essere ricaricato fino alla capacità massima solo se si inseriscono meno di 170.000 campioni di dati al secondo.

## Limiti aggiuntivi per i dati importati

Amazon Managed Service for Prometheus prevede quote aggiuntive per i dati che vengono importati nell'area di lavoro. Queste non sono regolabili.

- I campioni dei parametri più vecchi di 1 ora non possono essere acquisiti.
- Ogni campione e i metadati devono avere un nome per il parametro.

# Documentazione di riferimento delle API

Questa sezione elenca le operazioni API e le strutture di dati supportate da Amazon Managed Service for Prometheus.

Per informazioni su queste operazioni API e sulle relative quote per serie, etichette e richieste API, consulta le quote del servizio [Amazon Managed Service for Prometheus nella Guida per l'utente di Amazon Managed Service for Prometheus](#).

## Argomenti

- [Amazon Managed Service for Prometheus](#)
- [API compatibili con Prometheus](#)

## Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus fornisce operazioni API per la creazione e la manutenzione delle aree di lavoro Amazon Managed Service for Prometheus. Ciò include API per aree di lavoro, scraper, definizioni di alert manager, gruppi di regole, namespace e registrazione.

Per informazioni dettagliate sulle API Amazon Managed Service for Prometheus, consulta l'[Amazon Managed Service for Prometheus API Reference](#).

## Utilizzo di Amazon Managed Service per Prometheus con un SDK AWS

AWS i kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice e documentazione che facilita agli sviluppatori la creazione di AWS applicazioni nel linguaggio preferito. Per un elenco di SDK e strumenti suddivisi per lingua, consulta [Tools to Building on AWS](#) nel AWS Developer Center.

### Versioni SDK

Ti consigliamo di utilizzare la build più recente dell' AWS SDK e qualsiasi altro SDK che utilizzi nei tuoi progetti e di mantenere gli SDK aggiornati. L' AWS SDK offre le caratteristiche e le funzionalità più recenti e anche aggiornamenti di sicurezza.

# API compatibili con Prometheus

Amazon Managed Service for Prometheus supporta le seguenti API compatibili con Prometheus.

Per ulteriori informazioni sull'utilizzo delle API compatibili con Prometheus, vedere [Interrogazione tramite API compatibili con Prometheus](#)

## Argomenti

- [CreateAlertManagerAlerts](#)
- [DeleteAlertManagerSilence](#)
- [GetAlertManagerStatus](#)
- [GetAlertManagerSilence](#)
- [GetLabels](#)
- [GetMetricMetadata](#)
- [GetSeries](#)
- [ListAlerts](#)
- [ListAlertManagerAlerts](#)
- [ListAlertManagerAlertGroups](#)
- [ListAlertManagerReceivers](#)
- [ListAlertManagerSilences](#)
- [ListRules](#)
- [PutAlertManagerSilences](#)
- [QueryMetrics](#)
- [RemoteWrite](#)

## CreateAlertManagerAlerts

L'CreateAlertManagerAlertsoperazione crea un avviso nell'area di lavoro.

Verbi HTTP validi:

POST

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/alerts`

## URL dei parametri delle domande:

`alerts` Una matrice di oggetti, in cui ogni oggetto rappresenta un avviso. Di seguito è illustrato un esempio del percorso di un oggetto:

```
[
  {
    "startsAt": "2021-09-24T17:14:04.995Z",
    "endsAt": "2021-09-24T17:14:04.995Z",
    "annotations": {
      "additionalProp1": "string",
      "additionalProp2": "string",
      "additionalProp3": "string"
    },
    "labels": {
      "additionalProp1": "string",
      "additionalProp2": "string",
      "additionalProp3": "string"
    },
    "generatorURL": "string"
  }
]
```

## Richiesta di esempio

```
POST /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/alerts
HTTP/1.1
Content-Length: 203,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

```
[
  {
    "labels": {
      "alertname": "test-alert"
    },
    "annotations": {
      "summary": "this is a test alert used for demo purposes"
    },
    "generatorURL": "https://www.amazon.com/"
  }
]
```

```
] ]
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 0
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin
```

## DeleteAlertManagerSilence

DeleteSilence elimina un avviso silenzioso.

Verbi HTTP validi:

DELETE

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/silence/silenceID`

URL dei parametri delle domande: nessuno

## Richiesta di esempio

```
DELETE /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/silence/
d29d9df3-9125-4441-912c-70b05f86f973 HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
```

```
Content-Length: 0
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin
```

## GetAlertManagerStatus

GetAlertManagerStatus recupera informazioni sullo stato di alert manager.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/status`

URL dei parametri delle domande: nessuno

Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/status
HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 941
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin
```

```
{
  "cluster": null,
  "config": {
    "original": "global:\n  resolve_timeout: 5m\n  http_config:\n
follow_redirects: true\n  smtp_hello: localhost\n  smtp_require_tls: true\nroute:
\n  receiver: sns-0\n  group_by:\n    - label\n  continue: false\nreceivers:\n-
name: sns-0\n  sns_configs:\n    - send_resolved: false\n    http_config:\n
      follow_redirects: true\n    sigv4: {}\n    topic_arn: arn:aws:sns:us-
west-2:123456789012:test\n    subject: '{{ template \"sns.default.subject\" . }}'\n
    message: '{{ template \"sns.default.message\" . }}'\n    workspace_arn:
arn:aws:aps:us-west-2:123456789012:workspace/ws-58a6a446-5ec4-415b-9052-a449073bbd0a
\n  templates: []\n"
  },
  "uptime": null,
  "versionInfo": null
}
```

## GetAlertManagerSilence

GetAlertManagerSilence recupera informazioni su un avviso di silenzio.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/silence/silenceID`

URL dei parametri delle domande: nessuno

Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/silence/
d29d9df3-9125-4441-912c-70b05f86f973 HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 310
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

{
  "id": "d29d9df3-9125-4441-912c-70b05f86f973",
  "status": {
    "state": "active"
  },
  "updatedAt": "2021-10-22T19:32:11.763Z",
  "comment": "hello-world",
  "createdBy": "test-person",
  "endsAt": "2023-07-24T01:05:36.000Z",
  "matchers": [
    {
      "isEqual": true,
      "isRegex": true,
      "name": "job",
      "value": "hello"
    }
  ],
  "startsAt": "2021-10-22T19:32:11.763Z"
}
```

## GetLabels

L'GetLabel operazione recupera le etichette associate a una serie temporale.

Verbi HTTP validi:

GET, POST

URI validi:

`/workspaces/workspaceId/api/v1/labels`

`/workspaces/workspaceId/api/v1/label/label-name/values` Questo URI supporta solo le richieste GET.

## URL dei parametri delle domande:

`match[]=<series_selector>` Argomento del selettore di serie ripetute che seleziona la serie da cui leggere i nomi delle etichette. Facoltativo.

`start=<rfc3339 | unix_timestamp>` Timestamp di inizio. Facoltativo.

`end=<rfc3339 | unix_timestamp>` Timestamp di fine. Facoltativo.

## Esempio di richiesta per `/workspaces/workspaceId/api/v1/labels`

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/labels HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Esempio di risposta per `/workspaces/workspaceId/api/v1/labels`

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 1435
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

{
  "status": "success",
  "data": [
    "__name__",
    "access_mode",
    "address",
    "alertname",
    "alertstate",
    "apiservice",
    "app",
    "app_kubernetes_io_instance",
    "app_kubernetes_io_managed_by",
    "app_kubernetes_io_name",
    "area",
```

```
    "beta_kubernetes_io_arch",
    "beta_kubernetes_io_instance_type",
    "beta_kubernetes_io_os",
    "boot_id",
    "branch",
    "broadcast",
    "buildDate",
    ...
  ]
}
```

### Richiesta di esempio per `/workspaces/workspaceId/api/v1/label/label-name/values`

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/label/access_mode/values
HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

### Esempio di risposta per `/workspaces/workspaceId/api/v1/label/label-name/values`

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 74
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

{
  "status": "success",
  "data": [
    "ReadWriteOnce"
  ]
}
```

## GetMetricMetadata

L'operazione `GetMetricMetadata` recupera i metadati relativi dei parametri attualmente eliminati dalle destinazioni. Non fornisce alcuna informazione sull'obiettivo.

La sezione dati del risultato della domanda è costituita da un oggetto in cui ogni chiave è un nome di metrica e ogni valore è un elenco di oggetti di metadati univoci, come esposto per quel nome di metrica in tutte le destinazioni.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/api/v1/metadata`

URL dei parametri delle domande:

`limit=<number>` Il numero massimo di righe da restituire.

`metric=<string>` Un nome di metrica per cui filtrare i metadati. Se lo lasci vuoto, vengono recuperati tutti i metadati dei parametri.

Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/metadata HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
Transfer-Encoding: chunked

{
  "status": "success",
  "data": {
    "aggregator_openapi_v2_regeneration_count": [
      {
```

```
        "type": "counter",
        "help": "[ALPHA] Counter of OpenAPI v2 spec regeneration count broken
down by causing APIService name and reason.",
        "unit": ""
    }
],
...
}
}
```

## GetSeries

L'GetSeriesoperazione recupera l'elenco delle serie temporali che corrispondono a un determinato set di etichette.

Verbi HTTP validi:

GET, POST

URI validi:

`/workspaces/workspaceId/api/v1/series`

URL dei parametri delle domande:

`match[]=<series_selector>` Argomento del selettore di serie ripetute che seleziona la serie da restituire. Devi specificarne almeno `match[]` uno.

`start=<rfc3339 | unix_timestamp>` Timestamp di inizio. Facoltativo

`end=<rfc3339 | unix_timestamp>` Timestamp di fine. Facoltativo

Richiesta di esempio

```
POST /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/series --data-urlencode
'match[]=node_cpu_seconds_total{app="prometheus"}' --data-urlencode 'start=1634936400'
--data-urlencode 'end=1634939100' HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
content-encoding: gzip

{
  "status": "success",
  "data": [
    {
      "__name__": "node_cpu_seconds_total",
      "app": "prometheus",
      "app_kubernetes_io_managed_by": "Helm",
      "chart": "prometheus-11.12.1",
      "cluster": "cluster-1",
      "component": "node-exporter",
      "cpu": "0",
      "heritage": "Helm",
      "instance": "10.0.100.36:9100",
      "job": "kubernetes-service-endpoints",
      "kubernetes_name": "servicesstackprometheuscf14a6d7-node-exporter",
      "kubernetes_namespace": "default",
      "kubernetes_node": "ip-10-0-100-36.us-west-2.compute.internal",
      "mode": "idle",
      "release": "servicesstackprometheuscf14a6d7"
    },
    {
      "__name__": "node_cpu_seconds_total",
      "app": "prometheus",
      "app_kubernetes_io_managed_by": "Helm",
      "chart": "prometheus-11.12.1",
      "cluster": "cluster-1",
      "component": "node-exporter",
      "cpu": "0",
      "heritage": "Helm",
      "instance": "10.0.100.36:9100",
      "job": "kubernetes-service-endpoints",
      "kubernetes_name": "servicesstackprometheuscf14a6d7-node-exporter",
      "kubernetes_namespace": "default",
      "kubernetes_node": "ip-10-0-100-36.us-west-2.compute.internal",
```

```
        "mode": "iowait",
        "release": "servicesstackprometheuscf14a6d7"
    },
    ...
]
}
```

## ListAlerts

L'ListAlertsoperazione recupera gli avvisi attualmente attivi nell'area di lavoro.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/api/v1/alerts`

Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/alerts HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 386
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

{
  "status": "success",
  "data": {
    "alerts": [
      {
```

```
    "labels": {
      "alertname": "test-1.alert",
      "severity": "none"
    },
    "annotations": {
      "message": "message"
    },
    "state": "firing",
    "activeAt": "2020-12-01T19:37:25.429565909Z",
    "value": "1e+00"
  }
]
},
"errorType": "",
"error": ""
}
```

## ListAlertManagerAlerts

`ListAlertManagerAlerts` Recupera le informazioni sugli avvisi attualmente attivati in alert manager nell'area di lavoro.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/alerts`

Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/alerts
HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
```

```
Content-Length: 354
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

[
  {
    "annotations": {
      "summary": "this is a test alert used for demo purposes"
    },
    "endsAt": "2021-10-21T22:07:31.501Z",
    "fingerprint": "375eab7b59892505",
    "receivers": [
      {
        "name": "sns-0"
      }
    ],
    "startsAt": "2021-10-21T22:02:31.501Z",
    "status": {
      "inhibitedBy": [],
      "silencedBy": [],
      "state": "active"
    },
    "updatedAt": "2021-10-21T22:02:31.501Z",
    "labels": {
      "alertname": "test-alert"
    }
  }
]
```

## ListAlertManagerAlertGroups

L'operazione `ListAlertManagerAlertGroups` recupera un elenco di gruppi di avvisi configurati in alert manager nell'area di lavoro.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/alerts/groups`

## URL dei parametri delle domande:

`active` Booleano. Se vero, l'elenco restituito include gli avvisi attivi. Il valore predefinito è `true`.

Facoltativo

`silenced` Booleano. Se vero, l'elenco restituito include avvisi silenziati. Il valore predefinito è `true`. Facoltativo

`inhibited` Booleano. Se vero, l'elenco restituito include avvisi inibiti. Il valore predefinito è `true`.

Facoltativo

`filter` Una matrice di stringhe. Un elenco di abbinatori in base ai quali filtrare gli avvisi.

Facoltativo

`receiver` Stringa. Un'espressione regolare che abbina i ricevitori in base ai quali filtrare gli avvisi. Facoltativo

## Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/alerts/
groups HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 443
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

[
  {
    "alerts": [
      {
        "annotations": {
```

```
        "summary": "this is a test alert used for demo purposes"
      },
      "endsAt": "2021-10-21T22:07:31.501Z",
      "fingerprint": "375eab7b59892505",
      "receivers": [
        {
          "name": "sns-0"
        }
      ],
      "startsAt": "2021-10-21T22:02:31.501Z",
      "status": {
        "inhibitedBy": [],
        "silencedBy": [],
        "state": "unprocessed"
      },
      "updatedAt": "2021-10-21T22:02:31.501Z",
      "generatorURL": "https://www.amazon.com/",
      "labels": {
        "alertname": "test-alert"
      }
    }
  ],
  "labels": {},
  "receiver": {
    "name": "sns-0"
  }
}
]
```

## ListAlertManagerReceivers

L'operazione `ListAlertManagerReceivers` recupera informazioni sui ricevitori configurati in alert manager.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/receivers`

URL dei parametri delle domande: nessuno

## Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/receivers
HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 19
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

[
  {
    "name": "sns-0"
  }
]
```

## ListAlertManagerSilences

L'operazione `ListAlertManagerSilences` recupera informazioni sui silenzi di avviso configurati nell'area di lavoro.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/silences`

## Richiesta di esempio

```
GET /workspaces/ws-58a6a446-5ec4-415b-9052-a449073bbd0a/alertmanager/api/v2/silences
HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 312
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

[
  {
    "id": "d29d9df3-9125-4441-912c-70b05f86f973",
    "status": {
      "state": "active"
    },
    "updatedAt": "2021-10-22T19:32:11.763Z",
    "comment": "hello-world",
    "createdBy": "test-person",
    "endsAt": "2023-07-24T01:05:36.000Z",
    "matchers": [
      {
        "isEqual": true,
        "isRegex": true,
        "name": "job",
        "value": "hello"
      }
    ],
    "startsAt": "2021-10-22T19:32:11.763Z"
  }
]
```

## ListRules

ListRules recupera informazioni sulle regole configurate nell'area di lavoro.

Verbi HTTP validi:

GET

URI validi:

`/workspaces/workspaceId/api/v1/rules`

Richiesta di esempio

```
GET /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/rules HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 423
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin

{
  "status": "success",
  "data": {
    "groups": [
      {
        "name": "test-1.rules",
        "file": "test-rules",
        "rules": [
          {
            "name": "record:1",
            "query": "sum(rate(node_cpu_seconds_total[10m:1m]))",
```

```
        "labels": {},
        "health": "ok",
        "lastError": "",
        "type": "recording",
        "lastEvaluation": "2021-10-21T21:22:34.429565909Z",
        "evaluationTime": 0.001005399
      }
    ],
    "interval": 60,
    "lastEvaluation": "2021-10-21T21:22:34.429563992Z",
    "evaluationTime": 0.001010504
  }
],
},
"errorType": "",
"error": ""
}
```

## PutAlertManagerSilences

L'PutAlertManagerSilencesoperazione crea un nuovo avviso silenzioso o ne aggiorna uno esistente.

Verbi HTTP validi:

POST

URI validi:

`/workspaces/workspaceId/alertmanager/api/v2/silences`

URL dei parametri delle domande:

`silence` Un oggetto che rappresenta il silenzio. Di seguito è riportato il formato:

```
{
  "id": "string",
  "matchers": [
    {
      "name": "string",
      "value": "string",
      "isRegex": Boolean,
      "isEqual": Boolean
    }
  ]
}
```

```
],  
  "startsAt": "timestamp",  
  "endsAt": "timestamp",  
  "createdBy": "string",  
  "comment": "string"  
}
```

## Richiesta di esempio

```
POST /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/alertmanager/api/v2/silences  
HTTP/1.1  
Content-Length: 281,  
Authorization: AUTHPARAMS  
X-Amz-Date: 20201201T193725Z  
User-Agent: Grafana/8.1.0  
  
{  
  "matchers": [  
    {  
      "name": "job",  
      "value": "up",  
      "isRegex": false,  
      "isEqual": true  
    }  
  ],  
  "startsAt": "2020-07-23T01:05:36+00:00",  
  "endsAt": "2023-07-24T01:05:36+00:00",  
  "createdBy": "test-person",  
  "comment": "test silence"  
}
```

## Risposta di esempio

```
HTTP/1.1 200 OK  
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535  
Content-Length: 53  
Connection: keep-alive  
Date: Tue, 01 Dec 2020 19:37:25 GMT  
Content-Type: application/json  
Server: amazon  
vary: Origin
```

```
{
  "silenceID": "512860da-74f3-43c9-8833-cec026542b32"
}
```

## QueryMetrics

L'QueryMetrics operazione valuta un'interrogazione istantanea in un singolo momento o in un intervallo di tempo.

Verbi HTTP validi:

GET, POST

URI validi:

`/workspaces/workspaceId/api/v1/query` Questo URI valuta una domanda istantanea in un singolo momento.

`/workspaces/workspaceId/api/v1/query_range` Questo URI valuta una domanda istantanea in un intervallo di tempo.

URL dei parametri delle domande:

`query=<string>` Una stringa di domanda con espressioni Prometheus. Utilizzato in entrambi `query` e `query_range`.

`time=<rfc3339 | unix_timestamp>` (Facoltativo) Timestamp di valutazione se si utilizza il `query` per una domanda istantanea in un singolo momento.

`timeout=<duration>` (Facoltativo) Timeout di valutazione. L'impostazione predefinita è ed è limitato dal valore di `-query.timeout` flag. Utilizzato in entrambi `query` e `query_range`.

`start=<rfc3339 | unix_timestamp>` Inizia il timestamp se lo utilizzi `query_range` per porre una domanda in un intervallo di tempo.

`end=<rfc3339 | unix_timestamp>` Termina il timestamp se lo utilizzi `query_range` per porre una domanda in un intervallo di tempo.

`step=<duration | float>` Larghezza del passo di risoluzione della domanda in `duration` formato o in `float` numero di secondi. Utilizza questa opzione solo se utilizza `query_range` per porre una domanda in un intervallo di tempo e, se necessario, per tale domanda.

## Duration (Durata)

`duration` In un'API compatibile con Prometheus, `A` è un numero, seguito immediatamente da una delle seguenti unità:

- ms millisecondi
- s secondi
- m minuti
- h ore
- d giorni, supponendo che un giorno abbia sempre 24 ore
- w settimane, supponendo che una settimana abbia sempre 7 giorni
- y anni, supponendo che un anno abbia sempre 365 giorni

## Richiesta di esempio

```
POST /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/query?
query=sum(node_cpu_seconds_total) HTTP/1.1
Content-Length: 0,
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Grafana/8.1.0
```

## Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length: 132
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
content-encoding: gzip

{
  "status": "success",
  "data": {
    "resultType": "vector",
    "result": [
      {
```

```
        "metric": {},
        "value": [
            1634937046.322,
            "252590622.81000024"
        ]
    }
]
```

## RemoteWrite

L'RemoteWriteoperazione scrive i parametri da un server Prometheus a un URL remoto in un formato standardizzato. In genere, si utilizza un client esistente come un server Prometheus per richiamare questa operazione.

Verbi HTTP validi:

POST

URI validi:

`/workspaces/workspaceId/api/v1/remote_write`

URL dei parametri delle domande:

Nessuno

RemoteWrite ha una velocità di ingestione di 70.000 campioni al secondo e una dimensione del burst di ingestione di 1.000.000 di campioni.

Richiesta di esempio

```
POST /workspaces/ws-b226cc2a-a446-46a9-933a-ac50479a5568/api/v1/remote_write --data-binary "@real-dataset.sz" HTTP/1.1
Authorization: AUTHPARAMS
X-Amz-Date: 20201201T193725Z
User-Agent: Prometheus/2.20.1
Content-Type: application/x-protobuf
Content-Encoding: snappy
X-Prometheus-Remote-Write-Version: 0.1.0
```

*body*

**Note**

Per la sintassi del corpo della richiesta, vedere la definizione del buffer di protocollo all'indirizzo <https://github.com/prometheus/prometheus/blob/1c624c58ca934f618be737b4995e22051f5724c1/prompb/remote.pb.go#L64>.

**Risposta di esempio**

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-abcd-4442-b8c5-262b45e9b535
Content-Length:0
Connection: keep-alive
Date: Tue, 01 Dec 2020 19:37:25 GMT
Content-Type: application/json
Server: amazon
vary: Origin
```

# Guida per l'utente del servizio gestito da Amazon per Prometheus

Nella tabella seguente sono descritti importanti aggiornamenti della documentazione nella Guida per l'utente del servizio gestito da Amazon per Prometheus. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
<a href="#">È stata aggiunta la modifica dei file di definizione delle regole e dei file di configurazione di Alert Manager nella console</a>	Amazon Managed Service for Prometheus aggiunge il supporto per la <a href="#">modifica dei file di configurazione di Alert Manager e dei file di definizione delle regole</a> dall'interno della console Amazon Managed Service for Prometheus.	16 maggio 2024
<a href="#">Aggiunta una configurazione del raccoglitore AWS gestito più semplice con voci di accesso per Amazon EKS</a>	<a href="#">Amazon Managed Service for Prometheus aggiunge il supporto per le voci di accesso Amazon EKS per semplificare la configurazione dei raccoglitori gestiti.</a> AWS La politica <a href="#">AmazonPrometheusScraperServiceRolePolicy</a> gestita per i raccoglitori AWS gestiti viene aggiornata per consentire l'eliminazione delle voci di accesso che non vengono più utilizzate.	2 maggio 2024
<a href="#">Sposta AWS l'API in una guida di riferimento API separata</a>	Le API Amazon Managed Service for AWS Prometheus sono ora disponibili nel loro	7 febbraio 2024

riferimento, [Amazon Managed Service for Prometheus API Reference](#). Le API compatibili con Prometheus continuano a essere documentate nella Guida per l'utente di Amazon [Managed Service for Prometheus](#).

[Aggiunte chiavi gestite dal cliente per la crittografia dell'area di lavoro](#)

Amazon Managed Service for Prometheus aggiunge il supporto per le chiavi gestite dai clienti per la crittografia dell'area di lavoro. Per ulteriori informazioni, consultare [Crittografia dei dati inattivi](#).

21 dicembre 2023

[Sono state aggiunte nuove autorizzazioni a AmazonPrometheusFullAccess](#)

Sono state aggiunte nuove autorizzazioni alla policy [AmazonPrometheusFullAccess](#) gestita per supportare la creazione di raccoglitori AWS gestiti per i cluster Amazon EKS.

26 novembre 2023

[Aggiunta una nuova politica gestita, AmazonPrometheusScraperServiceLinkedRolePolicy](#)

È stata aggiunta una nuova policy gestita, [AmazonPrometheusScraperServiceLinkedRolePolicy](#) per consentire ai raccoglitori AWS gestiti di raccogliere metriche dai cluster Amazon EKS.

26 novembre 2023

[Sono stati aggiunti i AWS raccoglitori gestiti come metodo di inserimento](#)

Il servizio gestito da Amazon per Prometheus aggiunge il supporto per i [AWS raccoglitori gestiti](#).

26 novembre 2023

---

<a href="#">Aggiunto supporto per l'integrazione con Grafana gestito da Amazon</a>	Il servizio gestito da Amazon per Prometheus aggiunge il supporto per l' <a href="#">integrazione con gli avvisi Grafana gestito da Amazon</a> .	23 novembre 2022
<a href="#">Sono state aggiunte nuove autorizzazioni a AmazonPrometheusConsoleFullAccess</a>	Sono state aggiunte nuove autorizzazioni alla politica <a href="#">AmazonPrometheusConsoleFullAccess</a> gestita per supportare la registrazione degli eventi del gestore degli avvisi e dei righelli nei registri. CloudWatch	24 ottobre 2022
<a href="#">È stata aggiunta la soluzione di osservabilità Amazon EKS.</a>	Amazon Managed Service for Prometheus aggiunge una nuova soluzione utilizzando Observability Accelerator. AWS Per maggiori informazioni, consulta <a href="#">Utilizzo di AWS Observability Accelerator</a> .	14 ottobre 2022
<a href="#">È stato aggiunto il supporto per l'integrazione nel monitoraggio dei costi di Amazon EKS.</a>	Il servizio gestito da Amazon per Prometheus aggiunge il supporto per l'integrazione nel monitoraggio dei costi di Amazon EKS. Per ulteriori informazioni, consulta <a href="#">Integrazione con il monitoraggio dei costi di Amazon EKS</a> .	22 settembre 2022

<a href="#">È stato lanciato il supporto per i log di Alert Manager e Ruler in Amazon CloudWatch Logs.</a>	Amazon Managed Service for Prometheus lancia il supporto per i log di errore di Alert Manager e Ruler in Amazon CloudWatch. Per ulteriori informazioni, consulta <a href="#">Amazon CloudWatch Logs</a> .	1 settembre 2022
<a href="#">È stato aggiunto il supporto personalizzato per la conservazione degli archivi.</a>	Il servizio gestito da Amazon per Prometheus aggiunge un supporto personalizzato per la conservazione degli archivi, per area di lavoro, modificando la quota per quell'area di lavoro. <a href="#">Per ulteriori informazioni sulle quote nel servizio gestito da Amazon per Prometheus, consulta Quote del servizio.</a>	12 agosto 2022
<a href="#">Aggiunte metriche di utilizzo ad Amazon CloudWatch.</a>	Amazon Managed Service for Prometheus aggiunge il supporto per l'invio di metriche di utilizzo ad Amazon CloudWatch. Per ulteriori informazioni, consulta i <a href="#">CloudWatchparametri di Amazon</a> .	6 maggio 2022
<a href="#">Aggiunta del supporto per la regione Europa (Londra).</a>	Aggiunto il supporto del servizio gestito da Amazon per Prometheus per la regione Europa (Londra).	4 maggio 2022

---

<a href="#"><u>Il servizio gestito da Amazon per Prometheus è disponibile a livello generale e aggiunge il supporto per le regole e alert manager.</u></a>	Il servizio gestito da Amazon per Prometheus è disponibile a livello generale. Supporta anche regole e alert manager. Per ulteriori informazioni, consulta <a href="#"><u>Regole di registrazione e regole di avviso</u></a> e <a href="#"><u>Alert manager e templating</u></a> .	29 settembre 2021
<a href="#"><u>Aggiunto il supporto di tag.</u></a>	Il servizio gestito da Amazon per Prometheus supporta il tag delle aree di lavoro del servizio gestito da Amazon per Prometheus.	7 settembre 2021
<a href="#"><u>Le quote delle serie attive e del tasso di importazione sono aumentate.</u></a>	La quota delle serie attive è aumentata a 1.000.000 e la quota del tasso di importazione è aumentata a 70.000 campioni al secondo.	22 febbraio 2021
<a href="#"><u>Rilascio anteprima del servizio gestito da Amazon per Prometheus.</u></a>	Viene rilasciata l'anteprima del servizio gestito da Amazon per Prometheus.	15 dicembre 2020

# Glossario per AWS

Per la terminologia AWS più recente, consultare il [glossario AWS](#) nella documentazione di riferimento per Glossario AWS.

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