



Guida per l'utente

Amazon Managed Service per Prometheus



Amazon Managed Service per Prometheus: Guida per l'utente

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

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

Table of Contents

Cos'è il servizio gestito da Amazon per Prometheus?	1
Regioni supportate	1
Prezzi	8
Supporto premium	8
Inizia a usare	9
Configurare AWS	9
Registrati per un Account AWS	10
Crea un utente con accesso amministrativo	10
Creare un'area di lavoro	12
Parametri di acquisizione	13
Fase 1: aggiunta di nuovi repository del grafico Helm	14
Fase 2: creazione di un namespace Prometheus.	14
Fase 3: configurazione dei ruoli IAM per gli account del servizio.	14
Fase 4: configurazione del nuovo server e avvio dell'importazione dei parametri	15
Metriche di interrogazione	16
Gestisci gli spazi di lavoro	18
Creare un'area di lavoro	18
Configura il tuo spazio di lavoro	21
Modifica un alias dell'area di lavoro	23
Trova i dettagli del tuo spazio di lavoro	23
Eliminazione di un'area di lavoro.	25
Parametri di acquisizione	27
AWS collezionisti gestiti	28
Utilizzo di un raccoglitore gestito	29
Parametri compatibili con Prometheus	49
Raccoglitori gestiti dal cliente	49
Proteggi l'importazione dei tuoi parametri	50
ADOT Collectors	51
Raccoglitori Prometheus	68
Dati di disponibilità elevata	77
Interroga i tuoi parametri	86
Proteggi le tue interrogazioni metriche	86
Utilizzo AWS PrivateLink con Amazon Managed Service for Prometheus	50
Autenticazione e autorizzazione	50

Usa Amazon Managed Grafana	87
Connessione ad Grafana gestito da Amazon in un VPC privato	88
Usa Grafana open source	88
Prerequisiti	88
Passaggio 1: configurare AWS SigV4	89
Passaggio 2: aggiungi l'origine dati Prometheus a Grafana	90
Passaggio 3: (opzionale) Risoluzione dei problemi se Save & Test non funziona	93
Usa Grafana in Amazon EKS	94
AWS Configura SigV4	94
Imposta ruoli IAM per gli account del servizio	95
Aggiorna il server Grafana utilizzando Helm	96
Aggiungi l'origine dati Prometheus a Grafana	96
Usa interrogazioni dirette	97
Interrogazione con awscurl	98
Statistiche di interrogazione	100
Regole di registrazione e avviso	104
Autorizzazioni IAM necessarie	105
Crea un file di regole	107
Carica un file di regole	108
Modificare un file di regole	110
Risolvi i problemi relativi alla valutazione delle regole	112
Convalida lo stato di attivazione degli avvisi	112
Risolvi le notifiche di avviso mancanti	113
Controlla lo stato di integrità della regola	113
Utilizzate l'offset nelle query per gestire i ritardi di inserimento	115
Problemi e soluzioni comuni	116
Le migliori pratiche per la valutazione delle regole	117
Risoluzione dei problemi per ruler	117
Gestore degli avvisi	119
Autorizzazioni IAM necessarie	120
Crea un file di configurazione	121
Configura un ricevitore di avvisi	124
Crea argomento Amazon SNS	124
Sono necessarie le autorizzazioni Amazon SNS	125
Invia avvisi al tuo argomento Amazon SNS	128
Invia messaggi come JSON	129

Invia avvisi ad altre destinazioni	131
Regole di convalida di Amazon SNS	132
Carica un file di configurazione	134
Integra gli avvisi con Grafana	136
Prerequisiti	137
Configurazione di Grafana gestito da Amazon	138
Risolvi i problemi relativi al gestore degli avvisi	139
Avvisi attivi (avviso)	140
Aggregazione degli avvisi (avviso sulla dimensione del gruppo)	140
Le dimensioni degli avvisi sono troppo grandi (avviso).	141
Avviso di contenuto vuoto	141
Avviso non valido key/value	142
Avviso di limite dei messaggi	142
Nessun errore di policy basata su risorse	143
Avviso non ASCII	143
Non autorizzato a chiamare KMS	144
Errore nel modello	144
Monitoraggio degli spazi di lavoro	146
CloudWatch metriche	146
Impostazione di una CloudWatch sveglia	156
CloudWatch Registri	156
Configurazione dei registri CloudWatch	157
Informazioni e controllo delle interrogazioni	159
Configurazione della registrazione delle interrogazioni	160
Configurazione delle soglie di limitazione delle query	161
Contenuto del registro	162
Limitazioni	163
Comprendi e ottimizza i costi	164
Cosa contribuisce ai miei costi?	164
Qual è il modo migliore per ridurre i miei costi? Come posso ridurre i costi di acquisizione?	164
Qual è il modo migliore per ridurre i costi delle mie richieste?	164
Se riduco il periodo di conservazione dei miei parametri, ciò contribuirà a ridurre la mia fattura totale?	165
Come posso mantenere bassi i costi delle mie richieste di avviso?	165
Quali parametri posso utilizzare per monitorare i miei costi?	166
Posso controllare la mia fattura in qualsiasi momento?	166

Perché la mia fattura è più alta all'inizio del mese rispetto alla fine del mese?	167
Ho eliminato tutte le mie aree di lavoro Amazon Managed Service for Prometheus, ma sembra che continuino a ricevere degli addebiti. Cosa potrebbe succedere?	167
Integrazioni	168
Monitoraggio dei costi di Amazon EKS	168
AWS Acceleratore di osservabilità	169
Prerequisiti	169
Utilizzo dell'esempio di monitoraggio dell'infrastruttura	170
AWS Controller per Kubernetes	172
Prerequisiti	172
Implementazione di un'area di lavoro	173
Configurare il cluster per la scrittura remota	177
CloudWatch Metriche Amazon con Firehose	179
Infrastruttura	179
Creazione di uno CloudWatch stream Amazon	182
Rimozione	183
Sicurezza	184
Protezione dei dati	185
Dati raccolti da Amazon Managed Service per Prometheus	186
Crittografia a riposo	187
Identity and Access Management	200
Destinatari	201
Autenticazione con identità	201
Gestione dell'accesso con policy	205
In che modo il servizio gestito da Amazon per Prometheus funziona con IAM	208
Esempi di policy basate su identità	215
Risoluzione dei problemi	218
Autorizzazioni e policy IAM	220
Permessi di Amazon Managed Service per Prometheus	220
Esempio di policy IAM	220
Convalida della conformità	221
Resilienza	222
Sicurezza dell'infrastruttura	222
Uso di ruoli collegati ai servizi	223
Il ruolo dello scraping dei parametri	223
CloudTrail tronchi	226

Amazon Managed Service per gli eventi di gestione di Prometheus in CloudTrail	227
Esempi di eventi Amazon Managed Service per Prometheus	228
Imposta ruoli IAM per gli account del servizio.	232
Configura i ruoli di servizio per l'acquisizione di parametri dai cluster Amazon EKS.	233
Imposta ruoli IAM per gli account del servizio per le domande dei parametri	236
Endpoint VPC di interfaccia	239
Creazione di un endpoint VPC di interfaccia per Amazon Managed Service per Prometheus	240
Risoluzione dei problemi	243
429 o limita gli errori superati	243
Vedo esempi duplicati	244
Vedo errori sui timestamp dei campioni	245
Viene visualizzato un messaggio di errore relativo a un limite	245
L'output del server Prometheus locale supera il limite.	246
Alcuni dei miei dati non vengono visualizzati	247
Assegnazione di tag	248
Taggare le aree di lavoro	249
Aggiunta di un tag a un'area di lavoro	250
Visualizzazione dei tag per un'area di lavoro	251
Come modificare i tag per un'area di lavoro	253
Rimuovi un tag da un'area di lavoro	254
Tag dei namespace dei gruppi di regole.	255
Aggiungi un tag a un namespace dei gruppi di regole	256
Visualizzazione dei tag per un namespace dei gruppi di regole	258
Modifica i tag per un namespace dei gruppi di regole	259
Rimuovere un tag da un namespace dei gruppi di regole	260
Quote del servizio	262
Quote del servizio	262
Quote predefinite della serie attiva	269
Scalare al di sopra della quota predefinita	270
Limitazione dell'ingestione	270
Limiti aggiuntivi per i dati importati	271
Documentazione di riferimento delle API	272
Servizio gestito Amazon per Prometheus APIs	272
Utilizzo di Amazon Managed Service per Prometheus con un SDK AWS	273
Compatibile con Prometheus APIs	273

CreateAlertManagerAlerts	274
DeleteAlertManagerSilence	275
GetAlertManagerStatus	276
GetAlertManagerSilence	277
GetLabels	279
GetMetricMetadata	281
GetSeries	282
ListAlerts	284
ListAlertManagerAlerts	285
ListAlertManagerAlertGroups	287
ListAlertManagerReceivers	289
ListAlertManagerSilences	290
ListRules	291
PutAlertManagerSilences	292
QueryMetrics	294
RemoteWrite	296
Cronologia dei documenti	298
.....	ccxiv

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. Puoi modificare il periodo di conservazione configurando l'area di lavoro fino a un massimo di 1095 giorni (tre anni). Per ulteriori informazioni, consulta [Configurare](#) l'area di lavoro.

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	
		aps-workspaces-fips.us-east-2.amazonaws.com	HTTPS	
		aps-workspaces-fips.us-east-2.api.aws	HTTPS	
		aps-workspaces.us-east-2.api.aws	HTTPS	
		aps-fips.us-east-2.amazonaws.com	HTTPS	
		aps.us-east-2.api.aws	HTTPS	
		aps-fips.us-east-2.api.aws	HTTPS	
US East (N. Virginia)	us-east-1	aps.us-east-1.amazonaws.com	HTTPS	
		aps-workspaces.us-east-1.amazonaws.com	HTTPS	
		aps-workspaces-fips.us-east-1.amazonaws.com	HTTPS	
		aps-workspaces-fips.us-east-1.api.aws	HTTPS	
		aps-workspaces.us-east-1.api.aws	HTTPS	
		aps-fips.us-east-1.amazonaws.com	HTTPS	
		aps.us-east-1.api.aws	HTTPS	
		aps-fips.us-east-1.api.aws	HTTPS	
US West (Oregon)	us-west-2	aps.us-west-2.amazonaws.com	HTTPS	
		aps-workspaces.us-west-2.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
		aps-workspaces-fips.us-west-2.amazonaws.com	HTTPS	
			HTTPS	
		aps-workspaces-fips.us-west-2.api.aws	HTTPS	
		aps-workspaces.us-west-2.api.aws	HTTPS	
		aps-fips.us-west-2.amazonaws.com	HTTPS	
		aps.us-west-2.api.aws	HTTPS	
		aps-fips.us-west-2.api.aws	HTTPS	
Africa (Cape Town)	af-south-1	aps.af-south-1.amazonaws.com	HTTPS	
		aps-workspaces.af-south-1.amazonaws.com	HTTPS	
		aps-workspaces.af-south-1.api.aws	HTTPS	
		aps.af-south-1.api.aws	HTTPS	
Asia Pacifico (Hong Kong)	ap-east-1	aps.ap-east-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-east-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-east-1.api.aws	HTTPS	
		aps.ap-east-1.api.aws	HTTPS	
Asia Pacifico (Malesia)	ap-southeast-5	aps.ap-southeast-5.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-5.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-5.api.aws	HTTPS	
		aps.ap-southeast-5.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Asia Pacifico (Mumbai)	ap-south-1	aps.ap-south-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-south-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-south-1.api.aws	HTTPS	
		aps.ap-south-1.api.aws	HTTPS	
Asia Pacifico (Seoul)	ap-northeast-2	aps.ap-northeast-2.amazonaws.com	HTTPS	
		aps-workspaces.ap-northeast-2.amazonaws.com	HTTPS	
		aps-workspaces.ap-northeast-2.api.aws	HTTPS	
		aps.ap-northeast-2.api.aws	HTTPS	
Asia Pacifico (Singapore)	ap-southeast-1	aps.ap-southeast-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-1.api.aws	HTTPS	
		aps.ap-southeast-1.api.aws	HTTPS	
Asia Pacifico (Sydney)	ap-southeast-2	aps.ap-southeast-2.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-2.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-2.api.aws	HTTPS	
		aps.ap-southeast-2.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Asia Pacifico (Tailandia)	ap-southeast-7	aps.ap-southeast-7.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-7.amazonaws.com	HTTPS	
		aps-workspaces.ap-southeast-7.api.aws	HTTPS	
		aps.ap-southeast-7.api.aws	HTTPS	
Asia Pacifico (Tokyo)	ap-northeast-1	aps.ap-northeast-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-northeast-1.amazonaws.com	HTTPS	
		aps-workspaces.ap-northeast-1.api.aws	HTTPS	
		aps.ap-northeast-1.api.aws	HTTPS	
Canada (Centrale)	ca-central-1	aps.ca-central-1.amazonaws.com	HTTPS	
		aps-workspaces.ca-central-1.amazonaws.com	HTTPS	
		aps-workspaces-fips.ca-central-1.amazonaws.com	HTTPS	
		aps-workspaces-fips.ca-central-1.api.aws	HTTPS	
		aps-workspaces.ca-central-1.api.aws	HTTPS	
		aps-fips.ca-central-1.amazonaws.com	HTTPS	
		aps.ca-central-1.api.aws	HTTPS	
		aps-fips.ca-central-1.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Europa (Francoforte)	eu-central-1	aps.eu-central-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-central-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-central-1.api.aws	HTTPS	
		aps.eu-central-1.api.aws	HTTPS	
Europa (Irlanda)	eu-west-1	aps.eu-west-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-west-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-west-1.api.aws	HTTPS	
		aps.eu-west-1.api.aws	HTTPS	
Europa (Londra)	eu-west-2	aps.eu-west-2.amazonaws.com	HTTPS	
		aps-workspaces.eu-west-2.amazonaws.com	HTTPS	
		aps-workspaces.eu-west-2.api.aws	HTTPS	
		aps.eu-west-2.api.aws	HTTPS	
Europa (Milano)	eu-south-1	aps.eu-south-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-south-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-south-1.api.aws	HTTPS	
		aps.eu-south-1.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Europa (Parigi)	eu-west-3	aps.eu-west-3.amazonaws.com	HTTPS	
		aps-workspaces.eu-west-3.amazonaws.com	HTTPS	
		aps-workspaces.eu-west-3.api.aws	HTTPS	
		aps.eu-west-3.api.aws	HTTPS	
Europa (Stoccolma)	eu-north-1	aps.eu-north-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-north-1.amazonaws.com	HTTPS	
		aps-workspaces.eu-north-1.api.aws	HTTPS	
		aps.eu-north-1.api.aws	HTTPS	
Europa (Zurigo)	eu-central-2	aps.eu-central-2.amazonaws.com	HTTPS	
		aps-workspaces.eu-central-2.amazonaws.com	HTTPS	
		aps-workspaces.eu-central-2.api.aws	HTTPS	
		aps.eu-central-2.api.aws	HTTPS	
Medio Oriente (Emirati Arabi Uniti)	me-central-1	aps.me-central-1.amazonaws.com	HTTPS	
		aps-workspaces.me-central-1.amazonaws.com	HTTPS	
		aps-workspaces.me-central-1.api.aws	HTTPS	
		aps.me-central-1.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Sud America (São Paulo)	sa-east-1	aps.sa-east-1.amazonaws.com	HTTPS	
		aps-workspaces.sa-east-1.amazonaws.com	HTTPS	
		aps-workspaces.sa-east-1.api.aws	HTTPS	
		aps.sa-east-1.api.aws	HTTPS	

Amazon Managed Service for Prometheus include endpoint del piano di controllo (per eseguire attività di gestione dell'area di lavoro) ed endpoint del piano dati (per lavorare con dati compatibili con Prometheus in un'istanza di workspace). Gli endpoint del piano di controllo iniziano con, mentre gli endpoint del piano di controllo iniziano con. `aps.*` `aps-workspaces.*` Gli endpoint che terminano con il `.amazonaws.com` supporto IPv4 e gli endpoint che terminano con il supporto sia E. `.api.aws` IPv4 IPv6

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 i report AWS sui costi AWS Cost Explorer e sull'utilizzo 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.

Inizia a usare Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus è un servizio serverless compatibile con Prometheus per il monitoraggio delle metriche dei container che semplifica il monitoraggio sicuro degli ambienti container su larga scala. Questa sezione illustra tre aree chiave dell'utilizzo di Amazon Managed Service for Prometheus:

- [Crea uno spazio di lavoro: crea uno spazio](#) di lavoro Amazon Managed Service for Prometheus per archiviare e monitorare le tue metriche.
- [Inserisci metriche](#): l'area di lavoro è vuota finché non inserisci le metriche nell'area di lavoro. Puoi inviare i parametri ad Amazon Managed Service for Prometheus o fare in modo che Amazon Managed Service for Prometheus li raccolga automaticamente.
- [Esegui query sui parametri](#): una volta che hai le metriche come dati nel tuo spazio di lavoro, sei pronto per interrogare i dati per esplorare o monitorare tali metriche.

Se non lo conosci AWS, questa sezione include anche [dettagli sulla](#) configurazione di un Account AWS

Argomenti

- [Configurare AWS](#)
- [Creazione di un'area di lavoro del servizio gestito da Amazon per Prometheus.](#)
- [Inserisci i parametri di Prometheus nell'area di lavoro](#)
- [Esegui una ricerca sui parametri Prometheus](#)

Configurare AWS

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

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 <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di 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 best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a <https://aws.amazon.com/> e scegliendo 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, assegna 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 l'impostazione predefinita IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

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

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

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

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

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

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 sulla creazione di uno spazio di lavoro e sulle opzioni disponibili, consulta. [Crea un'area di lavoro Amazon Managed Service per Prometheus](https://console.aws.amazon.com/prometheus/)

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

1. Apri la console Amazon Managed Service for 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 uno spazio di lavoro unico IDs, generato da Amazon Managed Service for 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 l'endpoint URLs per questa area di lavoro sia per la scrittura remota che per le query.

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

Prendi nota di quanto URLs visualizzato 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 generare metriche in Amazon EKS, come Kubernetes o metriche a livello di nodo, puoi utilizzare i componenti aggiuntivi della community di Amazon EKS. Per ulteriori informazioni, consulta la sezione [Componenti aggiuntivi disponibili per la community](#) nella Guida per l'utente di Amazon EKS.

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 i parametri nel tuo spazio di lavoro Amazon Managed Service for Prometheus](#).

Note

Le metriche inserite in un'area di lavoro vengono archiviate per 150 giorni per impostazione predefinita e vengono quindi eliminate automaticamente. Puoi modificare il periodo di conservazione configurando l'area di lavoro fino a un massimo di 1095 giorni (tre anni). Per ulteriori informazioni, consulta [Configurare](#) l'area di lavoro.

Le istruzioni in questa sezione ti consentono di iniziare rapidamente a utilizzare il servizio gestito da Amazon per Prometheus. Si presuppone che tu abbia già [creato uno](#) spazio di lavoro. In questa sezione, configuri un nuovo server Prometheus in un cluster Amazon EKS e il nuovo server utilizza una configurazione predefinita per fungere da agente per inviare metriche ad Amazon Managed Service for Prometheus. Questo metodo ha i seguenti prerequisiti:

- È necessario disporre di un cluster Amazon EKS da cui il nuovo server Prometheus raccoglierà i parametri.
- Nel cluster Amazon EKS deve essere installato un [driver Amazon EBS CSI](#) (richiesto da Helm).
- È necessario utilizzare Helm CLI 3.0 o versione successiva.
- È necessario utilizzare un computer Linux o macOS per eseguire i passaggi descritti nelle sezioni seguenti.

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. Sostituiscilo *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 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 parametri 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 sei su 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 del file in `amp-iamproxy-ingest-rol` cui hai creato. [Configura i ruoli di servizio per l'acquisizione di parametri dai cluster Amazon EKS](#).
 - `WORKSPACE_ID` Sostituiscilo con l'ID del tuo spazio di lavoro Amazon Managed Service for Prometheus.
 - Sostituisci `REGION` con la regione del tuo spazio di lavoro Amazon Managed Service for 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.
- *prometheus-agent-namespace* Sostituiscilo 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 di Amazon Managed Service for Prometheus o utilizzare Amazon Managed Service for Prometheus, consulta. APIs [Esegui una ricerca sui parametri Prometheus](#)

[Questa sezione presuppone che tu abbia già creato uno spazio di lavoro e che tu stia inserendo delle metriche in esso.](#)

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 [Integra gli 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](#).

Gestisci Amazon Managed Service per le aree di lavoro Prometheus

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

- [Crea un'area di lavoro Amazon Managed Service per Prometheus](#)
- [Configura il tuo spazio di lavoro](#)
- [Modifica un alias dell'area di lavoro](#)
- [Trova i dettagli del tuo spazio di lavoro Amazon Managed Service for Prometheus, incluso l'ARN](#)
- [Eliminare un'area di lavoro Amazon Managed Service per Prometheus](#)

Crea un'area di lavoro Amazon Managed Service per Prometheus

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 uno spazio di lavoro unico IDs, generato da Amazon Managed Service for Prometheus.

(Facoltativo) Per utilizzare la tua chiave KMS per crittografare i dati archiviati nel tuo spazio di lavoro, puoi includere il parametro con la chiave da utilizzare. `kmsKeyArn` 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 Amazon Managed Service for Prometheus all'indirizzo. <https://console.aws.amazon.com/prometheus/>
2. Scegli Create (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 uno spazio di lavoro unico IDs, generato da Amazon Managed Service for Prometheus.

4. (Facoltativo) Per utilizzare la tua chiave KMS per crittografare i dati archiviati nel tuo spazio di lavoro, puoi 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 [raccoltori 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 l'endpoint URLs per questa area di lavoro sia per la scrittura remota che per le query.

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 di quelle visualizzate per **Endpoint - remote write URL** e **Endpoint - query URL**. URLs 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](#).

Configura il tuo spazio di lavoro

Puoi configurare il tuo spazio di lavoro per quanto segue:

- Definisci i set di etichette e definisci i limiti sulle serie temporali attive che corrispondono ai set di etichette definiti. Un set di etichette è un insieme di una o più etichette, che sono name/value coppie che aiutano a contestualizzare le metriche delle serie temporali.

Definendo i set di etichette e impostando i limiti attivi delle serie temporali, è possibile limitare i picchi in un tenant o in una fonte in modo che influiscano solo su quel tenant o sulla fonte. Ad esempio, se si imposta un limite di 1.000.000 di serie temporali attive sul set di etichette `team=A env=prod`, se il numero di serie temporali importate che corrispondono a quel set di etichette

supera il limite, vengono limitate solo le serie temporali che corrispondono al set di etichette. In questo modo, gli altri inquilini o le fonti metriche non vengono influenzati.

[Per ulteriori informazioni sulle etichette in Prometheus, vedere Data Model.](#)

- Imposta un periodo di conservazione per definire il numero di giorni in cui i dati devono essere conservati nell'area di lavoro.

Per configurare il tuo spazio di lavoro

1. Apri la console Amazon Managed Service for 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.
4. Scegli la scheda Configurazioni dell'area di lavoro.
5. Per impostare il periodo di conservazione per l'area di lavoro, scegli Modifica nella sezione Periodo di conservazione. Quindi specifica il nuovo periodo di conservazione in giorni. Il massimo è 1095 giorni (tre anni).
6. Per aggiungere o modificare i set di etichette e i relativi limiti di serie attivi, scegli Modifica nella sezione Set di etichette. Quindi, esegui queste operazioni:
 - a. (Facoltativo) Inserite un valore in Limite predefinito del bucket per impostare un limite al numero massimo di serie temporali attive che possono essere inserite nell'area di lavoro, contando solo le serie temporali che non corrispondono a nessun set di etichette definito.
 - b. Per definire un set di etichette, inserite un limite di serie temporali attive per il nuovo set di etichette in Limite di serie attivo.

Quindi, inserisci un'etichetta e un valore per un'etichetta che verrà utilizzata nel set di etichette e scegli Aggiungi etichetta.
 - c. (Facoltativo) Per definire un altro set di etichette, scegliete Aggiungi un altro set di etichette e ripetete i passaggi precedenti.
7. Al termine, scegliere Save changes (Salva le modifiche).

Modifica un alias dell'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 Amazon Managed Service for 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 i dettagli del tuo spazio di lavoro Amazon Managed Service for Prometheus, incluso l'ARN

Puoi trovare i dettagli del tuo spazio di lavoro Amazon Managed Service for Prometheus utilizzando la console o il. AWS AWS CLI

Console

Per trovare i dettagli del tuo spazio di lavoro utilizzando la console Amazon Managed Service for Prometheus

1. Apri la console Amazon Managed Service for 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. Verranno visualizzati i dettagli sul tuo spazio di lavoro, tra cui:
 - Stato attuale: lo stato dell'area di lavoro, ad esempio Attivo, viene visualizzato in Stato.
 - ARN — L'ARN dell'area di lavoro viene visualizzato in ARN.

- ID — L'ID dell'area di lavoro viene visualizzato in ID dell'area di lavoro.
- URLs— La console ne visualizza più di uno URLs per l'area di lavoro, inclusa quella URLs per scrivere o interrogare dati dall'area di lavoro.

Note

Per impostazione predefinita, i URLs dati sono i. IPv4 URLs Puoi anche usare dualstack (IPv4 e IPv6 supportato). URLs Sono uguali, ma si trovano nel dominio `api.aws` anziché in quello predefinito. `amazonaws.com` Ad esempio, se dovessi vedere quanto segue (un IPv4 URL):

```
https://aps-workspaces.us-east-1.amazonaws.com/workspaces/ws-abcd1234-ef56-7890-ab12-example/api/v1/remote_write
```

Puoi creare un URL dualstack (incluso il supporto per IPv6) come segue:

```
https://aps-workspaces.us-east-1.api.aws/workspaces/ws-abcd1234-ef56-7890-ab12-example/api/v1/remote_write
```

Sotto questa sezione sono riportate le schede con informazioni su regole, gestore degli avvisi, registri, configurazione e tag.

AWS CLI

Per trovare i dettagli del tuo spazio di lavoro, utilizza il AWS CLI

Il comando seguente restituisce i dettagli dell'area di lavoro. È necessario sostituirlo *my-workspace-id* con l'ID dell'area di lavoro di cui si desidera ottenere i dettagli.

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

Ciò restituisce i dettagli sull'area di lavoro, tra cui:

- Stato attuale: lo stato dell'area di lavoro, ad esempio `ACTIVE`, viene restituito nella `statusCode` proprietà.
- ARN — L'ARN dell'area di lavoro viene restituito nella proprietà. `arn`

- URLs— AWS CLI restituisce l'URL di base per l'area di lavoro nella proprietà `prometheusEndpoint`

 Note

Per impostazione predefinita, l'URL restituito è l' IPv4 URL. Puoi anche utilizzare un URL dualstack (IPv4 e IPv6 supportato) nel dominio `api.aws` anziché quello predefinito. `amazonaws.com` Ad esempio, se dovessi vedere quanto segue (un IPv4 URL):

```
https://aps-workspaces.us-east-1.amazonaws.com/workspaces/ws-abcd1234-ef56-7890-ab12-example/
```

Puoi creare un URL dualstack (incluso il supporto per IPv6) come segue:

```
https://aps-workspaces.us-east-1.api.aws/workspaces/ws-abcd1234-ef56-7890-ab12-example/
```

Puoi anche creare la scrittura e l'interrogazione remote URLs per l'area di lavoro, aggiungendo `/api/v1/remote_write` o, rispettivamente. `/api/v1/query`

Eliminare un'area di lavoro Amazon Managed Service per Prometheus

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 Amazon Managed Service for 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 i parametri nel tuo spazio di lavoro Amazon Managed Service for Prometheus

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 quindi eliminate automaticamente. Puoi modificare il periodo di conservazione configurando l'area di lavoro fino a un massimo di 1095 giorni (tre anni). Per ulteriori informazioni, consulta [Configurare](#) l'area di lavoro.

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

- [Inserisci metriche con AWS raccoglitori gestiti](#)

- [Raccoglitori gestiti dal cliente](#)

Inserisci metriche con AWS raccoglitori 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

Amazon EKS espone parametri, metriche e kube-controller-manager kube-scheduler metriche del server API in un cluster. Molte altre tecnologie e applicazioni eseguite in ambienti Kubernetes forniscono metriche compatibili con Prometheus. Per un elenco completo degli esportatori disponibili, consulta [Esportatori e integrazioni](#) nella documentazione Prometheus.

Amazon Managed Service for Prometheus fornisce uno scraper o raccoglitore 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 raccoglitore 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 Fargate. EC2

Un collettore Amazon Managed Service for Prometheus crea un'interfaccia di rete elastica (ENI) per sottorete specificata durante la creazione dello scraper. Il raccoglitore analizza le metriche e le ENIs 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 raccoglitore del servizio gestito da Amazon per Prometheus nel cluster Amazon EKS e sui parametri raccolti.

Argomenti

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

Utilizzo di un raccogliatore AWS 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'API o utilizzando il. AWS CLI

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 cluster Amazon EKS espongono i parametri per il server API. I cluster Amazon EKS con versione Kubernetes 1.28 o superiore espongono anche i parametri relativi alla `e.kube-scheduler` `kube-controller-manager`. Per ulteriori informazioni, consulta [Fetch control plane raw metrics in formato Prometheus nella Amazon EKS User Guide](#).

Note

L'estrazione dei parametri da un cluster può comportare costi per l'utilizzo della rete. Un modo per ottimizzare questi costi consiste nel configurare l'/metricsendpoint in modo da comprimere le metriche fornite (ad esempio, con gzip), riducendo i dati che devono essere spostati attraverso la rete. Il modo in cui eseguire questa operazione dipende dall'applicazione o dalla libreria che fornisce le metriche. Alcune librerie sono gzip di default.

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.

Esistono tre modi per creare uno scraper:

- Uno scraper viene creato automaticamente per te quando [crei un cluster Amazon EKS tramite la console Amazon EKS](#) e scegli di attivare le metriche di Prometheus.
- Puoi creare uno scraper dalla console Amazon EKS per un cluster esistente. Apri il cluster nella [console Amazon EKS](#), quindi, nella scheda Osservabilità, scegli Aggiungi scraper.

Per ulteriori dettagli sulle impostazioni disponibili, consulta [Attiva i parametri di Prometheus nella Amazon EKS User Guide](#).

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

Queste opzioni sono descritte nella procedura seguente.

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.
- [L'Amazon VPC in cui risiede il cluster Amazon EKS deve avere DNS abilitato.](#)

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

Come creare uno scraper utilizzando l' AWS API

Utilizzate l'operazione `CreateScraper` API per creare uno scraper con l'API. AWS Nell'esempio seguente viene creato uno scraper nella us-west-2 regione. È necessario sostituire le informazioni relative all'area di lavoro Account AWS, alla sicurezza e al cluster Amazon EKS con le proprie IDs e fornire la configurazione da utilizzare per lo scraper.

Note

Il gruppo di sicurezza e le sottoreti devono essere impostati sul gruppo di sicurezza e sulle sottoreti del cluster a cui ti stai connettendo.

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 di, vedere. `scrapeConfiguration` [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

Come creare uno scraper utilizzando 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. È necessario sostituire le informazioni relative all'area di lavoro Account AWS, alla sicurezza e al cluster Amazon EKS con le proprie IDs e fornire la configurazione da utilizzare per lo scraper.

Note

Il gruppo di sicurezza e le sottoreti devono essere impostati sul gruppo di sicurezza e sulle sottoreti del cluster a cui ti stai connettendo.

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 comando `get-default-scraper-configuration`. Per ulteriori informazioni sul formato di `scrape-configuration`, vedere [Configurazione dello scraper](#).

```

aws amp create-scraper \
  --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:

- Creare uno scraper con l'operazione [CreateScraper](#) API.

- Elenca i tuoi scraper esistenti con l'operazione [ListScrapers](#) API.
- Aggiorna l'alias, la configurazione o la destinazione di uno scraper con l'operazione [UpdateScraper](#) API.
- Elimina uno scraper con l'operazione [DeleteScraper](#) API.
- Ottieni maggiori dettagli su uno scraper con l'operazione [DescribeScraper](#) API.
- Ottieni una configurazione generica per gli scraper con l'operazione [GetDefaultScraperConfiguration](#) API.

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.

Configurazione tra più account

Per creare uno scraper in una configurazione tra più account quando il cluster Amazon EKS da cui desideri raccogliere le metriche si trova in un account diverso dal raccoglitore Amazon Managed Service for Prometheus, utilizza la procedura seguente.

Ad esempio, se disponi di due account, il primo account di origine `account_id_source` in cui si trova Amazon EKS e un secondo account di destinazione `account_id_target` in cui risiede l'area di lavoro Amazon Managed Service for Prometheus.

Per creare uno scraper in una configurazione con più account

1. Nell'account di origine, crea un ruolo `arn:aws:iam::account_id_source:role/Source` e aggiungi la seguente politica di fiducia.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "scraper.aps.amazonaws.com"
    ]
  },
  "Action": "sts:AssumeRole",
  "Condition": {
```

```

    "ArnEquals": {
      "aws:SourceArn": "scraper_ARN"
    },
    "StringEquals": {
      "AWS:SourceAccount": "account_id"
    }
  }
}

```

2. In ogni combinazione di origine (cluster Amazon EKS) e destinazione (Amazon Managed Service for Prometheus workspace), devi creare un `arn:aws:iam::account_id_target:role/Target` ruolo e aggiungere la seguente politica di fiducia con autorizzazioni per.

[AmazonPrometheusRemoteWriteAccess](#)

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account_id_source:role/Source"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "StringEquals": {
      "sts:ExternalId": "scraper_ARN"
    }
  }
}

```

3. Crea uno scraper con l'opzione. `--role-configuration`

```

aws amp create-scraper \
  --source eksConfiguration="{clusterArn='arn:aws:eks:us-west-2:account-id_source:cluster/xarw,subnetIds=[subnet-subnet-id]}" \
  --scrape-configuration configurationBlob=<base64-encoded-blob> \
  --destination ampConfiguration="{workspaceArn='arn:aws:aps:us-west-2:account-id_target:workspace/ws-workspace-id'}" \
  --role-configuration '{"sourceRoleArn":"arn:aws:iam::account-id_source:role/Source", "targetRoleArn":"arn:aws:iam::account-id_target:role/Target"}'

```

4. Convalida la creazione dello scraper.

```

aws amp list-scrappers
{
  "scrapers": [
    {
      "scraperId": "scraper-id",
      "arn": "arn:aws:aps:us-west-2:account_id_source:scraper/scraper-id",
      "roleArn": "arn:aws:iam::account_id_source:role/aws-service-role/
scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraperInternal_cc319052-41a3-4",
      "status": {
        "statusCode": "ACTIVE"
      },
      "createdAt": "2024-10-29T16:37:58.789000+00:00",
      "lastModifiedAt": "2024-10-29T16:55:17.085000+00:00",
      "tags": {},
      "source": {
        "eksConfiguration": {
          "clusterArn": "arn:aws:eks:us-west-2:account_id_source:cluster/
cluster-arn",
          "securityGroupIds": [
            "sg-security-group-id",
            "sg-security-group-id"
          ],
          "subnetIds": [
            "subnet-subnet-id"
          ]
        },
        "destination": {
          "ampConfiguration": {
            "workspaceArn": "arn:aws:aps:us-
west-2:account_id_target:workspace/ws-workspace-id"
          }
        }
      }
    }
  ]
}

```

Passaggio da un ruolo collegato al servizio RoleConfiguration e viceversa

Se desideri tornare a un ruolo collegato al servizio anziché scrivere su un'area di lavoro Amazon Managed Service for Prometheus, devi aggiornare UpdateScraper e fornire un'area di lavoro nello stesso account dello scraper senza il RoleConfiguration. RoleConfiguration verrà rimosso dallo scraper e verrà utilizzato il ruolo collegato al servizio.

Quando si modificano le aree di lavoro nello stesso account dello scraper e si desidera continuare a utilizzare il RoleConfiguration, è necessario fornire nuovamente l'attivazione. RoleConfiguration UpdateScraper

Creazione di scraper per aree di lavoro abilitate con chiavi gestite dal cliente

Per creare uno scraper per l'inserimento di metriche in un'area di lavoro di Amazon Managed Service for Prometheus con [chiavi gestite dal cliente](#), usa il con l'origine e la --role-configuration destinazione impostate sullo stesso account.

```
aws amp create-scraper \
  --source eksConfiguration="{clusterArn='arn:aws:eks:us-west-2:account-id:cluster/
xarw,subnetIds=[subnet-subnet-id]}" \
  --scrape-configuration configurationBlob=<base64-encoded-blob> \
  --destination ampConfiguration="{workspaceArn='arn:aws:aps:us-west-2:account-
id:workspace/ws-workspace-id'}" \
  --role-configuration '{"sourceRoleArn":"arn:aws:iam::account-id:role/Source",
"targetRoleArn":"arn:aws:iam::account-id:role/Target"}'
```

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, le sottoreti 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>CreateScraperAPI.

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:

- Durante la creazione di 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 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 Amazon Managed Service for Prometheus o la CLI](#) o tramite la console Amazon EKS 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",
  "apiGroups": [
    "metrics.eks.amazonaws.com"
  ],
  "resources": [
    "kcm/metrics",
    "ksh/metrics"
  ],
  "verbs": [
    "get"
  ]
},
{
  "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"]
  - apiGroups: ["metrics.eks.amazonaws.com"]
    resources: ["kcm/metrics", "ksh/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/scraper.aps.amazonaws.com/  
AWSServiceRoleForAmazonPrometheusScraper_1234abcd-56ef-7
```

Deve essere riscritto come:

```
arn:aws:iam::111122223333:role/  
AWSServiceRoleForAmazonPrometheusScraper_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, usa l'operazione API [ListScrapers](#).

In alternativa, con AWS CLI, chiama:

```
aws amp list-scrapers
```

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

```
{
  "scrapers": [
    {
      "scraperId": "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 uno scraper, trova `scraperId` relativo allo scraper che desideri eliminare, utilizzando l'operazione `ListScrapers`, quindi usa l'operazione [DeleteScraper](#) per eliminarlo.

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'operazione `GetDefaultScraperConfiguration` nell'API del servizio gestito da Amazon per Prometheus.

Per modificare la configurazione di uno scraper, è possibile utilizzare l'operazione `UpdateScraper`. Se devi aggiornare l'origine delle metriche (ad esempio, su un cluster Amazon EKS diverso), devi eliminare lo scraper e ricrearlo con la nuova fonte.

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 globale 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. Questo esempio include il supporto per le metriche del server dell'API kube kube-controller-manager e per le metriche kube-scheduler. Per ulteriori informazioni, consulta [Fetch control plane raw metrics in formato Prometheus nella Amazon EKS User Guide](#).

```
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
# Scheduler metrics
- job_name: 'ksh-metrics'
  kubernetes_sd_configs:
  - role: endpoints
  metrics_path: /apis/metrics.eks.amazonaws.com/v1/ksh/container/metrics
  scheme: https

```

```
bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
relabel_configs:
- source_labels:
  - __meta_kubernetes_namespace
  - __meta_kubernetes_service_name
  - __meta_kubernetes_endpoint_port_name
  action: keep
  regex: default;kubernetes;https
# Controller Manager metrics
- job_name: 'kcm-metrics'
  kubernetes_sd_configs:
  - role: endpoints
  metrics_path: /apis/metrics.eks.amazonaws.com/v1/kcm/container/metrics
  scheme: https
  bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
  relabel_configs:
  - source_labels:
    - __meta_kubernetes_namespace
    - __meta_kubernetes_service_name
    - __meta_kubernetes_endpoint_port_name
    action: keep
    regex: default;kubernetes;https
```

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

- 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.
- Risoluzione DNS: in relazione al nome di destinazione, l'unico nome di server riconosciuto in questa configurazione è il server API Kubernetes, `kubernetes.default.svc`. Tutti i nomi delle altre macchine devono essere specificati in base all'indirizzo 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?

 Important

Verifica che l'accesso privato per il tuo cluster Amazon EKS sia abilitato. Per ulteriori informazioni, consulta [Cluster private Endpoint](#) nella Amazon EKS User Guide.

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, ci sono diversi motivi per cui il raccoglitore potrebbe non riuscire a trovarlo.

- Potrebbe essere necessario modificare la configurazione dello scrape.
`relabel_config` Potrebbe essere necessario modificare la scoperta.
- Potrebbe esserci un problema con `role` Used for Discovery.
- L'Amazon VPC utilizzato dal cluster Amazon EKS potrebbe non avere il [DNS abilitato](#), il che impedirebbe al raccoglitore di trovare l'endpoint.
- `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. Puoi verificare che i dettagli siano corretti, ad esempio il protocollo (`http`/`https`), l'endpoint o la

porta che stai 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.
- 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 [Utilizzo di un raccoglitore AWS 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 che consente agli agenti di raccogliere i parametri. OpenTelemetry 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 raccoglitore](#)
- [Configura Amazon Managed Service per Prometheus per dati ad alta disponibilità](#)

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 dall'utente sia protetto all'interno della rete senza passare attraverso VPCs la rete Internet pubblica. AWS Per creare un endpoint AWS PrivateLink VPC per Amazon Managed Service for Prometheus, consulta. [Utilizzo del servizio gestito da Amazon per 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

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.

I seguenti argomenti descrivono tre modi diversi per configurare ADOT come raccoglitore per le tue metriche, a seconda che le metriche provengano da Amazon EKS, Amazon ECS o da un'istanza Amazon. EC2

Argomenti

- [Configura l'inserimento dei parametri utilizzando AWS Distro for OpenTelemetry 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 metriche da un' EC2 istanza Amazon utilizzando la scrittura remota](#)

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

Puoi utilizzare il collettore AWS Distor for OpenTelemetry (ADOT) per acquisire metriche da un'applicazione basata su Prometheus e inviarle ad Amazon Managed Service for Prometheus.

Note

Per ulteriori informazioni sul [AWS collettore](#) ADOT, consulta Distro for. OpenTelemetry

Per ulteriori informazioni sulle applicazioni con strumentazione Prometheus, vedere. [Quali sono i parametri compatibili con Prometheus?](#)

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 raccogliatore 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 parametri 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-role` quello 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.us-east-1.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "oidc.eks.us-east-1.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:adot-col:amp-iamproxy-ingest-service-account",
          "oidc.eks.us-east-1.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
        }
      }
    }
  ]
}
```

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

JSON

```
{
  "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 `awscli`. [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 `awscli`.](#)

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.

```
awscli --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 per 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 per 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.

Fase 1: definire un'immagine personalizzata del contenitore 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. 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 `sigv4auth`, consulta [Authenticator - Sigv4 on. 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]

```

Fase 2: invia l'immagine del contenitore 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 con il tuo valore *my-region*. 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
```

Passaggio 3: creare una definizione di attività Amazon ECS per eseguire lo scraping di Amazon Managed Service for 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"
```

```
}
```

Passaggio 4: autorizza la tua attività ad accedere ad Amazon Managed Service for Prometheus

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.

Fase 5: visualizza le tue metriche in Amazon Managed Grafana

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 metriche da un' EC2 istanza Amazon 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 e EC2 Amazon Managed Service for Prometheus. Per informazioni su come installare Prometheus, vedi [Guida introduttiva](#) sul sito web di Prometheus.

Se non conosci Amazon EC2 o Amazon Managed Service for Prometheus, ti consigliamo di iniziare leggendo le seguenti sezioni:

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

Crea un ruolo IAM per Amazon EC2

Per eseguire lo streaming delle metriche, devi prima creare un ruolo IAM con la policy AWS AmazonPrometheusRemoteWriteAccess gestita. 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. Scegliere Create Policy (Crea policy).

Avvia un' EC2 istanza Amazon

Per avviare un' EC2 istanza Amazon, segui le istruzioni in [Launch an instance](#) nella Amazon Elastic Compute Cloud User Guide for Linux Instances.

Esegui l'applicazione demo

Dopo aver creato il tuo ruolo IAM e avviato un' EC2 istanza 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, sostituisilo `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`, sostituisilo `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 raccoglitore

Puoi usare un'istanza Prometheus, in esecuzione in modalità agente (nota come agente Prometheus), per acquisire metriche e inviarle al tuo spazio di lavoro Amazon Managed Service for Prometheus.

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

Warning

Quando crei un agente Prometheus, sei responsabile della sua configurazione e manutenzione. [Evita di esporre gli endpoint scrape Prometheus 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 unico 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'acquisizione 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.
- Nel cluster Amazon EKS deve essere installato un [driver Amazon EBS CSI](#) (richiesto da Helm).
- È necessario utilizzare Helm CLI 3.0 o 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 spazio dei nomi.

```
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 parametri 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 `amp-iamproxy-ingest-role` cui hai creato. [Configura i ruoli di servizio per l'acquisizione di parametri dai cluster Amazon EKS](#).

- *WORKSPACE_ID* Sostituiscilo con l'ID del tuo spazio di lavoro Amazon Managed Service for Prometheus.
- Sostituisci *REGION* con la regione del tuo spazio di lavoro Amazon Managed Service for 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.
- *prometheus-namespace* Sostituiscilo 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'acquisizione da un server Prometheus esistente in Kubernetes su EC2

Amazon Managed Service for Prometheus supporta l'acquisizione di metriche dai server Prometheus in cluster che eseguono 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 di 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 le AWS 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 parametri 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 `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/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. Sostituiscilo *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
```

Configura Amazon Managed Service per Prometheus per dati ad alta disponibilità

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 [Usa aree di lavoro interregionali per aggiungere un'elevata disponibilità in Amazon Managed Service for Prometheus](#).

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](#)
- [Configura dati ad alta disponibilità su Amazon Managed Service for Prometheus utilizzando la tabella Prometheus Operator Helm](#)
- [Invia dati ad alta disponibilità ad Amazon Managed Service for Prometheus con Distro for AWS OpenTelemetry](#)
- [Invia dati di elevata disponibilità al servizio gestito da Amazon per Prometheus con il grafico Helm della community Prometheus](#)
- [Risposte alle domande più comuni sulla configurazione ad alta disponibilità in Amazon Managed Service for Prometheus](#)
- [Usa aree di lavoro interregionali per aggiungere un'elevata disponibilità in Amazon Managed Service for Prometheus](#)

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, `clusteretichetta` identifica l'agente dell'istanza Prometheus `prom-team1` e `__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'`clusteretichetta` 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](#).

Configura dati ad alta disponibilità su Amazon Managed Service for Prometheus utilizzando la tabella Prometheus Operator Helm

Per configurare una configurazione ad alta disponibilità con Prometheus Operator in Helm, devi applicare etichette esterne su tutte le istanze di un gruppo ad alta disponibilità, in modo che Amazon Managed Service for 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 Prometheus con Distro for AWS OpenTelemetry

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

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](#).

Risposte alle domande più comuni sulla configurazione ad alta disponibilità in Amazon Managed Service for Prometheus

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 `cluster` 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](#)

Usa aree di lavoro interregionali per aggiungere un'elevata disponibilità in Amazon Managed Service for Prometheus

Per aggiungere la disponibilità interregionale ai tuoi dati, puoi inviare metriche a più aree di lavoro in diverse regioni. AWS 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.

Per creare dashboard con rappresentazioni visive delle tue metriche, puoi utilizzare un servizio come Amazon Managed Grafana. Amazon Managed Grafana (o un'istanza autonoma di Grafana) può creare un'interfaccia grafica che mostra le tue metriche in un'ampia varietà di stili di presentazione del display. Per ulteriori informazioni su Amazon Managed Grafana, consulta la [Amazon Managed Grafana](#) User Guide.

Puoi anche creare query singole, esplorare i tuoi dati o scrivere applicazioni personalizzate che utilizzano i tuoi parametri utilizzando le tue query utilizzando le query dirette. Le query dirette utilizzano l'API Amazon Managed Service for Prometheus e il linguaggio di query Prometheus standard, PromQL, per ottenere dati dal tuo spazio di lavoro Prometheus. Per ulteriori informazioni su PromQL e sulla sua sintassi, consulta [Interrogazione a Prometheus](#) nella documentazione di Prometheus.

Argomenti

- [Proteggi le tue interrogazioni metriche](#)
- [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 Prometheus compatibile APIs](#)
- [Ottieni statistiche sull'utilizzo delle query per ogni query](#)

Proteggi le tue interrogazioni metriche

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 usi AWS PrivateLink, il traffico di rete proveniente dal tuo VPCs 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 del servizio gestito da Amazon per 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 [Integra gli 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

Puoi usare un'istanza di Grafana per interrogare le tue metriche in Amazon Managed Service for Prometheus. Questo argomento spiega come interrogare i parametri di Amazon Managed Service for Prometheus utilizzando un'istanza autonoma di Grafana.

Prerequisiti

Istanza Grafana: devi disporre di un'istanza Grafana in grado di autenticarsi con Amazon Managed Service for 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 AWS l'autenticazione Signature Version 4 (SigV4).

Per verificare la tua versione di Grafana, inserisci il seguente comando, sostituendolo *grafana_install_directory* con il percorso dell'installazione di Grafana:


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

Se non disponi già di una Grafana standalone o hai bisogno di una versione più recente, puoi installare una nuova istanza. Per istruzioni su come configurare un Grafana autonomo, consulta [Installa Grafana nella documentazione di Grafana](#). Per informazioni su come iniziare a usare Grafana, vedi [Guida introduttiva a Grafana nella documentazione di Grafana](#).

Account AWS— Devi disporre delle autorizzazioni corrette per accedere alle metriche di Amazon Managed Service for Prometheus. Account AWS

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](#).

La sezione successiva descrive la configurazione dell'autenticazione da Grafana in modo più dettagliato.

Passaggio 1: configurare AWS SigV4

Amazon Managed Service for Prometheus funziona AWS Identity and Access Management con (IAM) per proteggere tutte le chiamate a Prometheus con credenziali IAM. APIs 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 Amazon Managed Grafana, SIGv4 l'autenticazione 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
```

Passaggio 2: 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.

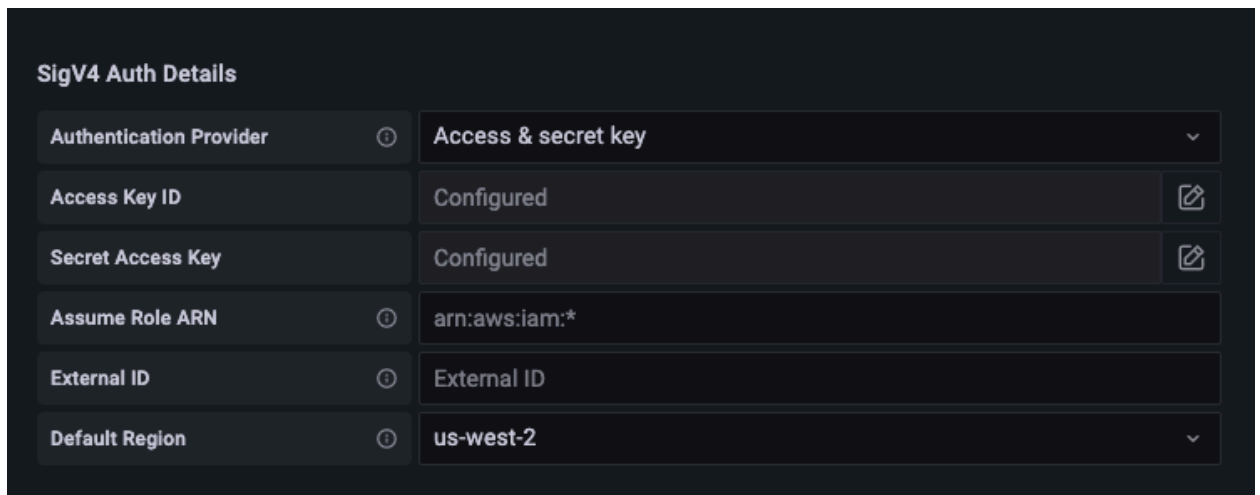
6. Nell'URL HTTP che hai appena specificato, rimuovi la `/api/v1/query` stringa aggiunta all'URL, perché l'origine dati Prometheus la aggiungerà automaticamente.

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

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.



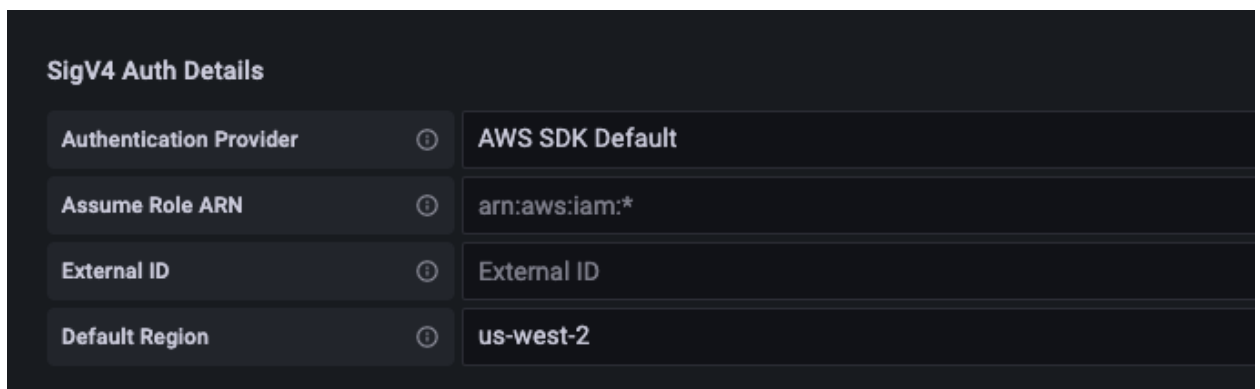
SigV4 Auth Details		
Authentication Provider	①	Access & secret key
Access Key ID		Configured
Secret Access Key		Configured
Assume Role ARN	①	arn:aws:iam:*
External ID	①	External ID
Default Region	①	us-west-2

- 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

Se il messaggio non viene visualizzato, nella sezione successiva vengono forniti suggerimenti per la risoluzione dei problemi di connessione.

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



SigV4 Auth Details		
Authentication Provider	①	AWS SDK Default
Assume Role ARN	①	arn:aws:iam:*
External ID	①	External ID
Default Region	①	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
```

Passaggio 3: (opzionale) Risoluzione dei problemi se Save & 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 `AmazonPrometheusQueryAccess` politica. 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 Signature Version 4 (SigV4).
AWS

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](#).

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 AWS dell'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-iamp-proxy-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 del servizio per le domande dei parametri](#) 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.

JSON

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

```

    "Principal": {
      "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.us-east-1.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "oidc.eks.us-east-1.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": [
          "system:serviceaccount:aws-amp:amp-iamproxy-query-service-account",
          "system:serviceaccount:grafana-namespace:grafana-service-account-name"
        ],
        "oidc.eks.us-east-1.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
      }
    }
  }
}

```

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 Prometheus compatibile APIs

Sebbene l'utilizzo di uno strumento come [Amazon Managed Grafana](#) sia il modo più semplice per visualizzare e interrogare i parametri, Amazon Managed Service for Prometheus supporta anche diversi modelli compatibili con Prometheus che puoi utilizzare per interrogare i tuoi parametri. APIs Per ulteriori informazioni su tutte le versioni compatibili con Prometheus APIs disponibili, vedere.

[Compatibile con Prometheus APIs](#)

I dispositivi compatibili con Prometheus utilizzano APIs il linguaggio di query Prometheus, PromQL, per specificare i dati che si desidera restituire. Per informazioni dettagliate su PromQL e sulla relativa sintassi, vedere Interrogazione di Prometheus nella [documentazione di Prometheus](#).

Quando li usi APIs 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 la compatibilità con Prometheus APIs](#) illustra come configurare SigV4. `awscurl` AWS

Argomenti

- [Usa awscurl per interrogare con Prometheus compatibile APIs](#)

Usa awscurl per interrogare con Prometheus compatibile APIs

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 *Region* gli *QUERY* input *Workspace-id* e 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. È possibile trovare la chiave di accesso e la chiave segreta per il ruolo in <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  
$ awscli -X POST --region <Region> \  
    --profile <PROFILE_NAME>  
    --service aps "$AMP_QUERY_ENDPOINT?query=<QUERY>"
```

- Utilizza il profilo di istanza associato all' EC2 istanza.

Esecuzione di richieste di interrogazione utilizzando il contenitore awscli

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

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

Ottieni statistiche sull'utilizzo delle query per ogni query

I [prezzi](#) delle interrogazioni si basano sul numero totale di esempi di interrogazioni elaborate in un mese a partire dalle interrogazioni eseguite. Puoi ottenere statistiche su ogni query che effettui per tenere traccia dei campioni elaborati. La risposta alla query per una query o un `queryRangeAPI` può includere i dati statistici sugli esempi di query elaborati includendo il parametro di query `stats=all` nella richiesta. Un `samples` oggetto viene creato 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.
<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  
      ]  
    ]  
  }  
}
```

Utilizzo di regole per modificare o monitorare le metriche man mano che vengono ricevute

Puoi impostare regole per agire in base alle metriche ricevute da Amazon Managed Service for Prometheus. Queste regole possono monitorare le metriche o persino creare nuove metriche calcolate in base alle metriche ricevute.

Il servizio gestito da Amazon per Prometheus supporta due tipi di 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 al [gestore degli avvisi](#), che può essere configurato per gestire le regole o inoltrarle alla 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

- [Comprensione delle autorizzazioni IAM necessarie per l'utilizzo delle regole](#)
- [Crea un file di regole](#)
- [Carica un file di configurazione delle regole su Amazon Managed Service for Prometheus](#)
- [Modificare o sostituire un file di configurazione delle regole](#)
- [Risolvi i problemi relativi alle valutazioni delle regole](#)
- [Risoluzione dei problemi per ruler](#)

Comprensione delle autorizzazioni IAM necessarie per l'utilizzo delle regole

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.

JSON

```
{
  "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 politica, sostituisci *<account>*, *<region><workspace-id>*, e *<namespace-name>* con i valori appropriati per il tuo account.

JSON

```

{
  "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:*:111122223333:workspace/*",
        "arn:aws:aps:us-east-1:111122223333:rulegroupnamespace/workspace-id/namespace-name"
      ]
    }
  ]
}

```

```
]
}
```

Crea 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 di Amazon Managed Service for Prometheus è un file di testo YAML che 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.

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

```
groups:
- name: cpu_metrics
  interval: 60s
  rules:
  - record: avg_cpu_usage
    expr: avg(rate(node_cpu_seconds_total[5m])) by (instance)
  - alert: HighAverageCPU
    expr: avg_cpu_usage > 0.8
    for: 10m
    keep_firing_for: 20m
    labels:
      severity: critical
    annotations:
      summary: "Average CPU usage across cluster is too high"
```

Questo esempio crea un gruppo di regole `cpu_metrics` che viene valutato ogni 60 secondi. Questo gruppo di regole crea una nuova metrica utilizzando una regola di registrazione, chiamata `avg_cpu_usage` e quindi la utilizza in un avviso. Di seguito vengono descritte alcune delle proprietà utilizzate. Per ulteriori informazioni sulle regole di avviso e altre proprietà che è possibile includere, vedere [Regole di avviso nella documentazione di Prometheus](#).

- `record: avg_cpu_usage`— Questa regola di registrazione crea una nuova metrica chiamata `avg_cpu_usage`
- L'intervallo di valutazione predefinito dei gruppi di regole è 60 secondi se la `interval` proprietà non è specificata.

- **expr:** `avg(rate(node_cpu_seconds_total[5m])) by (instance)`— Questa espressione per la regola di registrazione calcola il tasso medio di utilizzo della CPU negli ultimi 5 minuti per ciascun nodo, raggruppato in base all'etichetta. `instance`
- **alert:** `HighAverageCPU`— Questa regola di avviso crea un nuovo avviso chiamato `HighAverageCPU`
- **expr:** `avg_cpu_usage > 0.8` — Questa espressione indica all'avviso di cercare esempi in cui l'utilizzo medio della CPU supera l'80%.
- **for:** `10m`— L'avviso si attiva quando l'espressione viene soddisfatta per 10 minuti. In questo caso, i campioni sono in media superiori a 5 minuti, quindi l'avviso si attiva quando riceve almeno 2 campioni che superano la soglia.
- **keep_firing_for:** `20m`— Questo avviso continuerà ad attivarsi finché i campioni non saranno al di sotto della soglia per almeno 20 minuti. Questo può essere utile per evitare che l'avviso si alzi e si abbassi ripetutamente in successione.

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. [Carica un file di configurazione delle regole su Amazon Managed Service for Prometheus](#)

Carica un file di configurazione delle regole su Amazon Managed Service for Prometheus

Una volta individuate le regole da inserire nel file di configurazione delle regole, puoi crearlo e modificarlo all'interno della console oppure caricare un file 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 Amazon Managed Service for 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.

Modificare o sostituire un file di configurazione delle regole

Se desideri modificare le regole in un file di regole che hai già caricato su Amazon Managed Service for Prometheus, puoi caricare un nuovo file di regole per sostituire la 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 Amazon Managed Service for 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-namespaces --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.

Risolvi i problemi relativi alle valutazioni delle regole

Questa guida fornisce procedure di step-by-step risoluzione dei problemi più comuni relativi alla valutazione delle regole in Amazon Managed Service for Prometheus (AMP). Segui queste procedure per diagnosticare e risolvere i problemi relativi alle regole di avviso e registrazione.

Argomenti

- [Convalida lo stato di attivazione degli avvisi](#)
- [Risolvi le notifiche di avviso mancanti](#)
- [Controlla lo stato di integrità della regola](#)
- [Utilizzate l'offset nelle query per gestire i ritardi di inserimento](#)
- [Problemi e soluzioni comuni](#)
- [Le migliori pratiche per la valutazione delle regole](#)

Convalida lo stato di attivazione degli avvisi

Quando risolvi i problemi relativi alla valutazione delle regole, verifica innanzitutto se l'avviso è stato attivato interrogando le serie temporali sintetiche. **ALERTS** Le serie **ALERTS** temporali includono le seguenti etichette:

- **alertname** — Il nome dell'avviso.
- **alertstate** — In sospeso o in corso.
 - in sospeso: l'avviso è in attesa della durata specificata nella clausola. **for**
 - attivazione: l'avviso ha soddisfatto le condizioni per la durata specificata. Le etichette aggiuntive sono definite nella regola di avviso.

 Note

Mentre un avviso è attivo o in sospeso, il valore di esempio è 1. Quando l'avviso è inattivo, non viene prodotto alcun campione.

Risolvi le notifiche di avviso mancanti

Se gli avvisi vengono attivati ma le notifiche non arrivano, verifica le seguenti impostazioni di Alertmanager:

1. Verifica la configurazione di Alertmanager: verifica che i percorsi, i ricevitori e le impostazioni siano configurati correttamente. Rivedi le impostazioni dei blocchi dei percorsi, inclusi i tempi di attesa, gli intervalli di tempo e le etichette obbligatorie, che possono influire sulla attivazione degli avvisi. Confronta le regole di avviso con i percorsi e i ricevitori corrispondenti per confermare la corretta corrispondenza. Per i percorsi `contime_interval`, verifica che i timestamp rientrino negli intervalli specificati.
2. Verifica le autorizzazioni del destinatario degli avvisi: quando utilizzi un argomento Amazon SNS, verifica che AMP disponga delle autorizzazioni necessarie per pubblicare le notifiche. Per ulteriori informazioni, consulta [Autorizzare Amazon Managed Service for Prometheus a inviare messaggi di avviso al tuo argomento Amazon SNS](#).
3. Convalida la compatibilità del payload del ricevitore: conferma che il destinatario degli avvisi accetti il formato di payload di Alertmanager. Per i requisiti di Amazon SNS, consulta [Comprendere le regole di convalida dei messaggi di Amazon SNS](#).
4. Rivedi i log di Alertmanager: AMP fornisce i log forniti da Alertmanager per aiutare a risolvere i problemi di notifica. Per ulteriori informazioni, consulta [Monitora gli eventi di Amazon Managed Service for Prometheus con i log CloudWatch](#).

Per ulteriori informazioni su Alertmanager, consulta [Gestione e inoltro di avvisi in Amazon Managed Service for Prometheus con alert manager](#)

Controlla lo stato di integrità della regola

Le regole non valide possono causare errori di valutazione. Utilizzate i seguenti metodi per identificare il motivo per cui una regola non è stata valutata:

Example

Usa l' ListRules API

L'[ListRules](#) API fornisce informazioni sullo stato delle regole. Controlla i `lastError` campi `health` e per diagnosticare i problemi.

Esempio di risposta:

```
{
  "status": "success",
  "data": {
    "groups": [
      {
        "name": "my_rule_group",
        "file": "my_namespace",
        "rules": [
          {
            "state": "firing",
            "name": "broken_alerting_rule",
            "query": "...",
            "duration": 0,
            "keepFiringFor": 0,
            "labels": {},
            "annotations": {},
            "alerts": [],
            "health": "err",
            "lastError": "vector contains metrics with the same labelset after applying
alert labels",
            "type": "alerting",
            "lastEvaluation": "1970-01-01T00:00:00.000000000Z",
            "evaluationTime": 0.08
          }
        ]
      }
    ]
  }
}
```

Example

Usa registri venduti

L' `ListRules` API mostra solo le informazioni più recenti. Per una cronologia più dettagliata, abilita i [registri venduti](#) nel tuo spazio di lavoro per accedere a:

- Timestamp degli errori di valutazione
- Messaggi di errore dettagliati
- Dati di valutazione storici

Esempio di messaggio di registro fornito:

```
{
  "workspaceId": "ws-a2c55905-e0b4-4065-a310-d83ce597a391",
  "message": {
    "log": "Evaluating rule failed, name=broken_alerting_rule, group=my_rule_group, namespace=my_namespace, err=vector contains metrics with the same labelset after applying alert labels",
    "level": "ERROR",
    "name": "broken_alerting_rule",
    "group": "my_rule_group",
    "namespace": "my_namespace"
  },
  "component": "ruler"
}
```

Per altri esempi di log da Ruler o Alertmanager, vedi e. [Risoluzione dei problemi per ruler](#) [Gestione e inoltro di avvisi in Amazon Managed Service for Prometheus con alert manager](#)

Utilizzate l'offset nelle query per gestire i ritardi di inserimento

Per impostazione predefinita, le espressioni vengono valutate senza offset (query istantanea), utilizzando i valori al momento della valutazione. Se l'inserimento delle metriche viene ritardato, le regole di registrazione potrebbero non rappresentare gli stessi valori di quando si valuta manualmente l'espressione dopo che tutte le metriche sono state inserite.

Tip

L'utilizzo del modificatore di offset può ridurre i problemi causati dai ritardi di inserimento. Per ulteriori informazioni, vedere [Modificatore Offset](#) nella documentazione di Prometheus.

Esempio: gestione delle metriche ritardate

Se la regola viene valutata alle 12:00, ma l'ultimo campione per la metrica risale alle 11:45 a causa del ritardo di inserimento, la regola non troverà alcun campione al timestamp delle 12:00. Per mitigare questo problema, aggiungi un offset, ad esempio: **`my_metric_name offset 15m`**

Esempio: gestisci le metriche da più fonti

Quando le metriche provengono da fonti diverse, ad esempio due server, potrebbero essere inserite in momenti diversi. Per mitigare questo problema, forma un'espressione, ad esempio: **`metric_from_server_A / metric_from_server_B`**

Se la regola calcola tra i tempi di inserimento del server A e del server B, otterrai risultati inaspettati. L'uso di un offset può aiutare ad allineare i tempi di valutazione.

Problemi e soluzioni comuni

Lacune nella registrazione dei dati delle regole

Se notate delle lacune nei dati delle regole di registrazione rispetto alla valutazione manuale (quando eseguite direttamente l'espressione ProMQL originale della regola di registrazione tramite l'API di interrogazione o l'interfaccia utente), ciò potrebbe essere dovuto a uno dei seguenti fattori:

1. Tempi di valutazione lunghi: un gruppo di regole non può avere più valutazioni simultanee. Se il tempo di valutazione supera l'intervallo configurato, è possibile che le valutazioni successive non vengano effettuate. Più valutazioni consecutive mancate che superano l'intervallo configurato possono far sì che la regola di registrazione diventi obsoleta. Per ulteriori informazioni, vedere [Staleness nella documentazione](#) di Prometheus. È possibile monitorare la durata della valutazione utilizzando la CloudWatch metrica `RuleGroupLastEvaluationDuration` per identificare i gruppi di regole la cui valutazione richiede troppo tempo.
2. Monitoraggio delle valutazioni mancate: AMP fornisce la `RuleGroupIterationsMissed` CloudWatch metrica per tracciare quando le valutazioni vengono saltate. L' `ListRules` API mostra l'ora di valutazione e l'ora dell'ultima valutazione per ogni regola/gruppo, il che può aiutare a identificare i modelli di valutazioni mancate. Per ulteriori informazioni, consulta [ListRules](#).

Raccomandazione: suddividi le regole in gruppi separati

Per ridurre la durata delle valutazioni, suddividi le regole in gruppi di regole separati. Le regole all'interno di un gruppo vengono eseguite in sequenza, mentre i gruppi di regole possono essere

eseguite in parallelo. Mantieni le regole correlate che dipendono l'una dall'altra nello stesso gruppo. In genere, gruppi di regole più piccoli garantiscono valutazioni più coerenti e meno lacune.

Le migliori pratiche per la valutazione delle regole

1. Ottimizza le dimensioni dei gruppi di regole: mantieni piccoli i gruppi di regole per garantire valutazioni coerenti. Raggruppa le regole correlate, ma evita i gruppi di regole di grandi dimensioni.
2. Imposta intervalli di valutazione appropriati: equilibrio tra avvisi tempestivi e carico del sistema. Esamina i modelli di stabilità delle metriche monitorate per comprenderne i normali intervalli di fluttuazione.
3. Usa modificatori di offset per le metriche ritardate: aggiungi offset per compensare i ritardi di inserimento. Regola la durata dell'offset in base ai modelli di ingestione osservati.
4. Monitora le prestazioni di valutazione: monitora la metrica. `RuleGroupIterationsMissed`
Rivedi i tempi di valutazione nell' `ListRules` API.
5. Convalida le espressioni delle regole: assicurati che le espressioni corrispondano esattamente tra le definizioni delle regole e le query manuali. Prova le espressioni con intervalli di tempo diversi per comprendere il comportamento.
6. Verifica regolarmente lo stato delle regole: verifica la presenza di errori nelle valutazioni delle regole. Monitora i log forniti per individuare eventuali problemi ricorrenti.

Seguendo questi passaggi e le best practice per la risoluzione dei problemi, puoi identificare e risolvere i problemi più comuni con le valutazioni delle regole in Amazon Managed Service for Prometheus.

Risoluzione dei problemi per ruler

Utilizzando [Monitora gli eventi di Amazon Managed Service for Prometheus con i log CloudWatch](#), 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

```
{
  "workspaceId": "ws-12345c67-89c0-4d12-345b-f14db70f7a99",
  "message": {
```

```

    "log": "Evaluating rule failed, name=failure,
group=canary_long_running_v1_namespace, namespace=canary_long_running_v1_namespace,
err=found duplicate series for the match group {dimension1=\\\\"1\\\\\\"} on the right
hand-side of the operation: [{__name__=\\\\"fake_metric2\\\\\\", dimension1=\\\\"1\\\\\\
\\", dimension2=\\\\"b\\\\\\"}, {__name__=\\\\"fake_metric2\\\\\\", dimension1=\\\\"1\\\\\\",
dimension2=\\\\"a\\\\\\"}];many-to-many matching not allowed: matching labels must be
unique on one side",
    "level": "ERROR",
    "name": "failure",
    "group": "canary_long_running_v1_namespace",
    "namespace": "canary_long_running_v1_namespace"
  },
  "component": "ruler"
}

```

Ciò significa che si è verificato un errore durante l'esecuzione della regola.

Operazione da eseguire

Utilizza il messaggio di errore per risolvere i problemi dell'esecuzione della regola.

Gestione e inoltro di avvisi in Amazon Managed Service for Prometheus con 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

Prometheus standalone supporta la creazione di modelli, utilizzando file modello separati. 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

- [Comprensione delle autorizzazioni IAM necessarie per lavorare con Alert Manager](#)
- [Crea una configurazione di gestione degli avvisi in Amazon Managed Service for Prometheus per gestire e indirizzare gli avvisi](#)
- [Inoltra gli avvisi a un ricevitore di avvisi con il gestore degli avvisi in Amazon Managed Service for Prometheus](#)
- [Carica il file di configurazione del gestore degli avvisi su Amazon Managed Service for Prometheus](#)
- [Integra gli avvisi con Amazon Managed Grafana o Grafana open source](#)
- [Risolvi i problemi relativi al gestore degli avvisi con Logs CloudWatch](#)

Comprensione delle autorizzazioni IAM necessarie per lavorare con Alert Manager

Devi concedere agli utenti le autorizzazioni per utilizzare Alert Manager in Amazon Managed Service for Prometheus. Crea una policy AWS Identity and Access Management (IAM) con le seguenti autorizzazioni e assegna la policy ai tuoi utenti, gruppi o ruoli.

JSON

```
{
  "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": "*"
}
]
}

```

Crea una configurazione di gestione degli avvisi in Amazon Managed Service for Prometheus per gestire e indirizzare gli avvisi

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 [Carica il file di configurazione del gestore degli avvisi su Amazon Managed Service for 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 }}

```

Inoltra gli avvisi a un ricevitore di avvisi con il gestore degli avvisi in Amazon Managed Service for Prometheus

Quando un avviso viene generato da una regola di avviso, viene inviato a Alert Manager. Alert Manager esegue funzioni come la deduplicazione degli avvisi, l'inibizione degli avvisi durante la manutenzione o il raggruppamento degli avvisi in base alle esigenze. Quindi inoltra l'avviso come messaggio a un destinatario degli avvisi. È possibile configurare un ricevitore di avvisi in grado di notificare gli operatori, disporre di risposte automatiche o rispondere agli avvisi in altri modi.

L'unico ricevitore di avvisi supportato in Amazon Managed Service for Prometheus è Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni, consulta [Cos'è Amazon SNS?](#) Amazon SNS può essere utilizzato per rispondere agli avvisi in un'ampia varietà di modi, incluso l'inoltro ad altri sistemi, come e-mail, SMS o endpoint HTTP.

I seguenti argomenti descrivono le attività associate alla creazione e alla configurazione del ricevitore di avvisi Amazon SNS.

Argomenti

- [Creazione di un nuovo argomento Amazon SNS da utilizzare come ricevitore di avvisi in Amazon Managed Service for Prometheus](#)
- [Autorizzare Amazon Managed Service for Prometheus a inviare messaggi di avviso al tuo argomento Amazon SNS](#)
- [Configura il gestore degli avvisi per inviare messaggi al tuo argomento Amazon SNS](#)
- [Configurare il gestore degli avvisi per inviare messaggi ad Amazon SNS come JSON](#)
- [Configura Amazon SNS per inviare messaggi di avviso ad altre destinazioni](#)
- [Comprendere le regole di convalida dei messaggi di Amazon SNS](#)

Creazione di un nuovo argomento Amazon SNS da utilizzare come ricevitore di avvisi in Amazon Managed Service for Prometheus

Puoi utilizzare un argomento esistente di Amazon SNS come ricevitore di avvisi per Amazon Managed Service for Prometheus oppure puoi 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](#).

Indipendentemente dal fatto che utilizzi un argomento Amazon SNS nuovo o esistente, avrai bisogno dell'Amazon Resource Name (ARN) del tuo argomento Amazon SNS per completare le seguenti attività.

Autorizzare Amazon Managed Service for Prometheus a inviare messaggi di avviso 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 politica fornirà tale autorizzazione. Include una Condition dichiarazione per aiutare a prevenire un problema di sicurezza noto come problema confuso del vice. 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 nella versione v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
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 Amazon SNS è abilitato alla crittografia lato servizio (SSE), devi consentire ad Amazon Managed Service for Prometheus di inviare messaggi a questo argomento crittografato aggiungendo le `kms:Decrypt` autorizzazioni `kms:GenerateDataKey*` e alla politica chiave della AWS KMS chiave utilizzata per crittografare l'argomento.

Ad esempio, puoi aggiungere quanto segue alla policy:

```

{
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": "aps.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey*",
      "kms:Decrypt"
    ],
    "Resource": "*"
  }]
}

```

Per ulteriori informazioni, consulta [AWS Autorizzazioni KMS per argomenti SNS](#).

6. Scegli **Save changes** (Salva 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

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Nel AWS, l'impersonificazione tra servizi può portare alla confusione del 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 [Autorizzare Amazon Managed Service for Prometheus a inviare messaggi di avviso 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".

Configura il gestore degli avvisi per inviare messaggi al tuo argomento Amazon SNS

Dopo aver creato un argomento Amazon SNS di tipo standard (nuovo o esistente), puoi aggiungerlo alla configurazione del gestore degli avvisi come ricevitore di avvisi. Il gestore degli avvisi può inoltrare gli avvisi a un ricevitore di avvisi configurato. Per completare questa operazione, devi conoscere l'Amazon Resource Name (ARN) del tuo 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: Regione AWS
        topic_arn: ARN_of_SNS_topic
        subject: yoursubject
        attributes:
          key: yourkey
          value: yourvalue
```

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 [Configurare il gestore degli avvisi per inviare messaggi ad Amazon SNS come JSON](#) 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 [Carica il file di configurazione del gestore degli avvisi su Amazon Managed Service for Prometheus](#).

Configurare il gestore degli avvisi per inviare messaggi ad Amazon SNS come JSON

Per impostazione predefinita, il gestore degli avvisi di Amazon Managed Service for Prometheus emette i messaggi in un formato di elenco di testo semplice. Questo può essere più difficile da analizzare per altri servizi. Puoi invece configurare il gestore degli avvisi per inviare avvisi in formato JSON. JSON può semplificare l'elaborazione dei messaggi downstream da Amazon SNS negli endpoint di ricezione dei webhook o negli AWS Lambda endpoint di ricezione dei webhook. 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 [Crea una configurazione di gestione degli avvisi in Amazon Managed Service for Prometheus per gestire e indirizzare gli avvisi](#).
- Caricamento del file di configurazione, consulta [Carica il file di configurazione del gestore degli avvisi su Amazon Managed Service for Prometheus](#).

Configura Amazon SNS per inviare messaggi di avviso ad altre destinazioni

Amazon Managed Service for Prometheus può inviare messaggi di avviso solo ad Amazon Simple Notification Service (Amazon SNS). Per inviare questi messaggi ad altre destinazioni, come e-mail, webhook, Slack o OpsGenie, devi configurare Amazon SNS per inoltrare i messaggi a tali endpoint.

Le seguenti sezioni descrivono la configurazione di Amazon SNS per inoltrare avvisi ad altre destinazioni.

Argomenti

- [E-mail](#)
- [Webhook](#)
- [Slack](#)
- [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](#).

Comprendere le regole di convalida dei messaggi di Amazon SNS

Amazon Simple Notification Service (Amazon SNS) richiede che i messaggi soddisfino determinati standard. I messaggi che non soddisfano questi standard verranno modificati quando vengono ricevuti. I messaggi di avviso verranno convalidati, troncati o modificati, se necessario, dal ricevitore Amazon SNS in base alle seguenti regole:

- Il messaggio contiene caratteri non utf.
- Il messaggio verrà sostituito da Error - non è una stringa con codifica UTF-8 valida.

- Verrà aggiunto un attributo del messaggio con la chiave truncated e il valore true.
- Verrà aggiunto un attributo del messaggio con la chiave di modified e il valore di Message: Error - not a valid UTF-8 codificata.
- Il messaggio è vuoto.
 - Il messaggio verrà sostituito da Error - Il messaggio non deve essere vuoto.
 - Verrà aggiunto un attributo del messaggio con la chiave di modified e il valore di Message: Error - 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 di Message: Error - Message has been truncated from **X** KB, perché supera il limite di dimensione di 256 KB.
- L'oggetto contiene caratteri di controllo o non ASCII.
 - Se l'oggetto contiene caratteri di controllo o caratteri non ASCII, SNS sostituisce l'oggetto con Error - contiene caratteri di controllo o non ASCII.
 - Per gli oggetti delle email SNS, rimuovi i caratteri di controllo, come newline: \n
- 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 di modified e il valore di Subject: Error - contiene caratteri ASCII non stampabili.
- L'oggetto è stato troncato.
 - L'oggetto avrà il contenuto troncato.
 - Un attributo del messaggio verrà aggiunto con la chiave di modified e il valore di Subject: Error - Subject è stato troncato dai **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 di modifica e il valore MessageAttribute: Error - degli attributi **X** del messaggio sono stati rimossi a causa di un o 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 modificata e il valore MessageAttribute: Errore - **X** degli attributi del messaggio è stato rimosso perché supera il limite di dimensione di 256 KB.

Carica il file di configurazione del gestore degli avvisi su Amazon Managed Service for Prometheus

Una volta che sai cosa vuoi nel tuo file di configurazione di Alert Manager, puoi crearlo e modificarlo all'interno della console oppure puoi caricare un file esistente con la console Amazon Managed Service for Prometheus 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 Amazon Managed Service for 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 file://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.

Integra gli avvisi con Amazon Managed Grafana o Grafana open source

Le regole di avviso che hai creato in Alertmanager all'interno del servizio gestito da Amazon per Prometheus possono essere inoltrate e visualizzate in [Grafana gestito da Amazon](#) e [Grafana](#),

unificando le regole di avviso e gli avvisi in un unico ambiente. All'interno di Grafana gestito da Amazon, puoi visualizzare le regole di avviso e gli avvisi generati.

Prerequisiti

Prima di iniziare a integrare il servizio gestito da Amazon per Prometheus in Grafana gestito da Amazon, devi aver completato i seguenti prerequisiti:

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

Per ulteriori informazioni sulla creazione di credenziali An e IAM, consulta Account AWS .

[Configurare AWS](#)

- Devi disporre di un'area di lavoro del servizio gestito da Amazon per Prometheus e inserirvi dati. Per configurare un nuovo spazio di lavoro, consulta [Creazione di un'area di lavoro del servizio gestito da Amazon per Prometheus](#). 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 nel servizio gestito da Amazon per Prometheus. Per ulteriori informazioni su Alertmanager nel servizio gestito da Amazon per Prometheus, consulta [Gestione e inoltro di avvisi in Amazon Managed Service for Prometheus con alert manager](#). Per ulteriori informazioni sulle regole, consulta [Utilizzo di regole per modificare o monitorare le metriche man mano che vengono ricevute](#).
- Devi avere configurato Grafana gestito da Amazon o la versione open source di Grafana in esecuzione.
 - Se utilizzi Grafana gestito da Amazon, 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 il servizio gestito da Amazon per Prometheus. Per ulteriori informazioni, consulta [Configurazione di Grafana open source o Grafana Enterprise per l'utilizzo con il servizio gestito da Amazon per Prometheus](#).

- Grafana gestito da Amazon 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 Grafana gestito da Amazon

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

Per configurare Grafana gestito da Amazon 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 [Passaggio 2: 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-east-1.amazonaws.com/workspaces/ws-example-1234-5678-abcd-xyz00000001/alertmanager.

- In Auth, attiva Sigv4Auth. In questo modo Grafana userà l'[AWS autenticazione](#) 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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus nella pagina degli avvisi Grafana.

Risolvi i problemi relativi al gestore degli avvisi con Logs CloudWatch

Utilizzando [Monitora gli eventi di Amazon Managed Service for Prometheus con i log CloudWatch](#), 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

- [Avvisi attivi \(avviso\)](#)
- [Aggregazione degli avvisi \(avviso sulla dimensione del gruppo\)](#)
- [Le dimensioni degli avvisi sono troppo grandi \(avviso\).](#)
- [Avviso di contenuto vuoto](#)
- [Avviso non valido key/value](#)
- [Avviso di limite dei messaggi](#)
- [Nessun errore di policy basata su risorse](#)
- [Avviso non ASCII](#)
- [Non autorizzato a chiamare KMS](#)
- [Errore nel modello](#)

Avvisi attivi (avviso)

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "too many alerts, limit: 1000",
    "level": "WARN"
  },
  "component": "alertmanager"
}
```

Ciò significa che la quota di avvisi attivi di Alert Manager è stata superata.

Operazione da eseguire

Richiedi un aumento delle quote. Accedi AWS Management Console e apri la console Service Quotas all'indirizzo. <https://console.aws.amazon.com/servicequotas/>

Aggregazione degli avvisi (avviso sulla dimensione del gruppo)

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "Too many aggregation groups, cannot create new group for alert, groups=1000, limit=1000, alert=sample-alert",
    "level": "WARN"
  },
  "component": "alertmanager"
}
```

Ciò significa che la quota di dimensione del gruppo di aggregazione degli avvisi di Alert Manager è stata superata.

Operazione da eseguire

Ridurre la dimensione del gruppo di aggregazione degli avvisi utilizzando il parametro. `group_by`
Per ulteriori informazioni, vedere [Impostazioni relative al percorso nella documentazione di Prometheus](#).

È possibile anche richiedere un aumento delle quote. Accedi AWS Management Console e apri la console Service Quotas all'indirizzo. <https://console.aws.amazon.com/servicequotas/>

Le dimensioni degli avvisi sono troppo grandi (avviso).

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "alerts too big, total size limit: 20000000 bytes",
    "level": "WARN"
  },
  "component": "alertmanager"
}
```

Ciò significa che è stata superata la quota di dimensioni degli avvisi di Alert manager per area di lavoro.

Operazione da eseguire

Rimuovi le annotazioni e le etichette non necessarie per ridurre le dimensioni degli avvisi.

Avviso di contenuto vuoto

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-abcd1234-ef56-78ab-cd90-1234abcd0000",
  "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 valido **key/value**

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-abcd1234-ef56-78ab-cd90-1234abcd0000",
  "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 non keys/values 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-abcd1234-ef56-78ab-cd90-1234abcd0000",
  "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-abcd1234-ef56-78ab-cd90-1234abcd0000",
  "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 consenta al servizio `aps.amazonaws.com` (Amazon Managed Service for Prometheus) di accedere 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](#).

Avviso non ASCII

Quando il registro contiene il seguente avviso

```
{
  "workspaceId": "ws-abcd1234-ef56-78ab-cd90-1234abcd0000",
  "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.

Non autorizzato a chiamare KMS

Quando il registro contiene il seguente errore AWS KMS

```
{
  "workspaceId": "ws-abcd1234-ef56-78ab-cd90-1234abcd0000",
  "message": {
    "log": "Notify for alerts failed, AMP is not authorized to call KMS",
    "level": "ERROR"
  },
  "component": "alertmanager"
}
```

Operazione da eseguire

Verifica che la policy chiave della chiave utilizzata per crittografare l'argomento Amazon SNS consenta al responsabile del servizio Amazon Managed Service for Prometheus di eseguire le seguenti azioni: `aps.amazonaws.com kms:GenerateDataKey* kms:Decrypt` Per ulteriori informazioni, consulta [AWS Autorizzazioni KMS per argomenti SNS](#).

Errore nel modello

Quando il registro contiene il seguente errore

```
{
  "workspaceId": "ws-efdc5b42-b051-11ec-b123-4567ac120002",
  "message": {
    "log": "Notify for alerts failed. There is an error in a receiver that is using templates in the AlertManager definition. Make sure that the syntax is correct and only template functions and variables that exist are used in the receiver 'default', sns_configs position #2, section 'attributes'"
    "level": "ERROR"
  },
  "component": "alertmanager"
}
```



```
}
```

Ciò significa che c'è un errore in un modello utilizzato nella AlertManager definizione. La voce di errore contiene indicazioni sul ricevitore, sulla posizione in `sns_configs` e sulla proprietà che contiene gli errori.

Operazione da eseguire

Convalida la definizione di Alert Manager. Assicurati che la sintassi sia corretta e di fare riferimento alle variabili e alle funzioni del modello esistenti. Per ulteriori informazioni, vedere il [Notification Template Reference](#) nella documentazione open source di Prometheus.

Registrazione e monitoraggio di Amazon Managed Service per le aree di lavoro Prometheus

Amazon Managed Service for Prometheus utilizza CloudWatch Amazon per fornire dati sul suo funzionamento. Puoi utilizzare i CloudWatch parametri per conoscere l'utilizzo delle risorse e le richieste ai tuoi spazi di lavoro Amazon Managed Service for Prometheus. Puoi attivare il supporto CloudWatch Logs per ottenere i log degli eventi che si verificano nelle tue aree di lavoro.

I seguenti argomenti descrivono l'utilizzo CloudWatch in modo più dettagliato.

Usa i CloudWatch parametri per monitorare le risorse di Amazon Managed Service for Prometheus

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 informazioni sui parametri di utilizzo, consulta [parametri di utilizzo di CloudWatch](#).

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount*	RemoteWriteTPS	AWS/Usage	Operazioni di scrittura remota al secondo
ResourceCount	HAReplicaGroupCount	AWS/Usage	Numero di gruppi di repliche ad alta disponibilità
ResourceCount*	QueryMetricsTPS	AWS/Usage	Operazioni di interrogazione al secondo
ResourceCount	IngestionRate	AWS/Usage	Frequenza di acquisizione del campione

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
			Unità: conteggio 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 Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ResourceCount	ActiveAlerts	AWS/Usage	Numero di avvisi attivi per area di lavoro Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount	SizeOfAlerts	AWS/Usage	Dimensione totale di tutti gli avvisi nell'area di lavoro, in byte Unità: byte Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ResourceCount	SuppressedAlerts	AWS/Usage	Numero di avvisi in stato soppresso per area di lavoro. Un avviso può essere soppresso mediante un silenzio o un'inibizione. Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount	UnprocessedAlerts	AWS/Usage	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. Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ResourceCount	AllAlerts	AWS/Usage	Numero di avvisi in qualsiasi stato per area di lavoro. Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
ResourceCount	AllRules	AWS/Usage	Numero di regole in qualsiasi stato per area di lavoro. Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ActiveSeriesPerLabelSet	-	AWS/Prometheus	L'attuale utilizzo della serie attiva per ogni set di etichette definito dall'utente Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
ActiveSeriesLimitPerLabelSet	-	AWS/Prometheus	Il valore limite attuale delle serie attive per ogni set di etichette definito dall'utente Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
AlertManagerAlertsReceived	-	AWS/Prometheus	Totale degli avvisi riusciti ricevuti dal gestore degli avvisi Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
AlertManagerNotificationsFailed	-	AWS/Prometheus	Numero di consegne di avvisi non andate a buon fine Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
AlertManagerNotificationsThrottled	-	AWS/Prometheus	Numero di avvisi limitati Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
Discarded Samples ^{**}	-	AWS/Prometheus	Numero di campioni scartati per motivo Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
Discarded SamplesPerLabelSet	-	AWS/Prometheus	Il numero di campioni scartati per ogni set di etichette definito dall'utente Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
Ingestion RatePerLabelSet	-	AWS/Prometheus	La velocità di ingestione per ogni set di etichette definito dall'utente Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
QuerySamplesProcessed	-	AWS/Prometheus	Numero di esempi di interrogazione elaborati Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
RuleEvaluations	-	AWS/Prometheus	Numero totale di valutazioni delle regole Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
RuleEvaluationFailures	-	AWS/Prometheus	Numero di errori di valutazione delle regole nell'intervallo Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

CloudWatch nome della metrica	Nome risorsa	CloudWatch spazio dei nomi	Descrizione
RuleGroup IterationsMissed	-	AWS/Prometheus	Numero di iterazioni del gruppo di regole mancate nell'intervallo. Unità: conteggio Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)
RuleGroup LastEvaluationDuration	-	AWS/Prometheus	Durata dell'ultima valutazione di un gruppo di regole. Unità: secondi Statistiche valide: Average (Media), Minimum (Minimo), Maximum (Massimo), Sum (Somma)

* Le metriche TPS vengono generate ogni minuto e rappresentano una media al secondo per quel minuto. I periodi di burst brevi non verranno inclusi nelle metriche TPS.

** Alcuni dei motivi per cui i campioni vengono scartati sono i seguenti.

Motivo	Significato
greater_than_max_sample_age	Eliminare campioni che hanno più di un'ora.
new-value-for-timestamp	I campioni duplicati vengono inviati con un timestamp diverso da quello registrato in precedenza.

Motivo	Significato
per_labelset_series_limit	L'utente ha raggiunto il limite totale di serie attive per set di etichette.
per_metric_series_limit	L'utente ha raggiunto il limite delle serie attive per metrica.
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, RuleEvaluationsRuleEvaluationFailures, e RuleGroupLastEvaluationDuration 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.

Monitora gli eventi di Amazon Managed Service for Prometheus con i log 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 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

JSON

```
{
  "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. Scegli Save changes (Salva 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.

Gestione del costo delle query in Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus offre la possibilità di limitare i costi delle query fornendo limiti alla quantità di Query Samples Processed (QSP) che può essere utilizzata da una singola query. Puoi configurare due tipi di soglie per QSP, avvisi ed errori, per gestire e controllare efficacemente i costi delle query.

Quando le query raggiungono la soglia di avviso, viene visualizzato un messaggio di avviso nella risposta alla query API. Per le query visualizzate tramite Amazon Managed Grafana, l'avviso sarà visibile nell'interfaccia utente di Amazon Managed Grafana, aiutando gli utenti a identificare le query costose. Le query che raggiungono la soglia di errore non vengono addebitate e verranno rifiutate con un errore.

Oltre alla limitazione delle query, Amazon Managed Service for Prometheus offre la possibilità di registrare i dati sulle prestazioni delle query in Logs. CloudWatch Questa funzionalità ti consente di analizzare le query in dettaglio, aiutandoti a ottimizzare le query di Amazon Managed Service for Prometheus e a gestire i costi in modo più efficace. La registrazione delle query acquisisce informazioni sulle query che superano le soglie di Query Samples Processed (QSP) specificate. Questi dati vengono quindi pubblicati in CloudWatch Logs, per consentire di esaminare e analizzare le prestazioni delle query. Le query registrate includono sia le query API che le query Rule. Per impostazione predefinita, la registrazione delle query è disabilitata per ridurre al minimo l'utilizzo

non necessario dei log. CloudWatch È possibile abilitare questa funzionalità quando necessario per l'analisi delle query.

Argomenti

- [Configurazione della registrazione delle interrogazioni](#)
- [Configurazione delle soglie di limitazione delle query](#)
- [Contenuto del registro](#)
- [Limitazioni](#)

Configurazione della registrazione delle interrogazioni

Puoi configurare la registrazione delle query nella console Amazon Managed Service for Prometheus o nella AWS CLI chiamando la richiesta API. `create-query-logging-configuration` Questo corpo dell'API contiene un elenco di destinazioni, ma per ora supportiamo solo CloudWatch i log come destinazione e le destinazioni devono contenere esattamente un elemento con configurazioni. CloudWatch

Prerequisiti

Assicurati che `logGroup` sia già stato creato. L'ID o il ruolo utilizzato per la configurazione devono avere la seguente politica o autorizzazioni equivalenti.

JSON

```
{
  "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:CreateQueryLoggingConfiguration",

```



```

        "aps:UpdateQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps>DeleteQueryLoggingConfiguration"
    ],
    "Resource": "*"
}
]
}

```

Configura i registri CloudWatch

Puoi configurare CloudWatch i log accedendo ad Amazon Managed Service for Prometheus utilizzando o. AWS Management Console AWS CLI

Per configurare la registrazione delle query utilizzando la console Amazon Managed Service for Prometheus

1. Vai alla scheda Log nel pannello dei dettagli dell'area di lavoro.
2. In Query Insights, scegli Crea.
3. Seleziona il menu a discesa Log Group e scegli il gruppo di log per pubblicare i log.

Puoi anche creare un nuovo gruppo di log nella CloudWatch console.

4. Inserisci la soglia (QSP).
5. Scegli Save (Salva).

Per configurare la registrazione delle query utilizzando il AWS CLI comando

```

aws amp create-query-logging-configuration \
--workspace-id my_workspace_ID \
--destinations '[{"cloudWatchLogs":{"logGroupArn":"$my-log-group-arn"}, "filters": {"qspThreshold":$qspThreshold}}]'

```

Per informazioni su come aggiornare, eliminare e descrivere le operazioni, consulta [Amazon Managed Service for Prometheus API Reference](#).

Configurazione delle soglie di limitazione delle query

[Per configurare le soglie QSP, è necessario fornire i parametri di query nell'API. QueryMetrics](#)

- `max_samples_processed_warning_threshold` — Imposta la soglia di avviso per i campioni di query elaborati
- `max_samples_processed_error_threshold` — Imposta la soglia di errore per i campioni di query elaborati

Per gli utenti di Amazon Managed Grafana, puoi utilizzare la configurazione dell'origine dati grafana per applicare limiti a tutte le query provenienti dall'origine dati:

1. Accedi alla configurazione dell'origine dati Amazon Managed Service for Prometheus in Amazon Managed Grafana.
2. In Parametri di query personalizzati, aggiungi le intestazioni di soglia.
3. Scegli Save (Salva).

Contenuto del registro

Per le interrogazioni che hanno origine da regole, nei CloudWatch log verranno visualizzate le seguenti informazioni sulla query:

```
{
  workspaceId: "workspace_id",
  message: {
    query: "avg(rate(go_goroutines[1m])) > 1",
    name: "alert_rule",
    kind: "alerting",
    group: "test-alert",
    namespace: "test",
    samples: "59321",
  },
  component: "ruler"
}
```

Per le query che provengono da chiamate API, nei log verranno visualizzate le seguenti informazioni sulla query: CloudWatch

```
{
  workspaceId: "ws-5e7658c2-7ccf-4c30-9de9-2ab26fa30639",
  message: {
    query: "sum by (instance) (go_memstats_alloc_bytes{job=\"node\"})",
    queryType: "range",
  }
}
```

```
    start: "1683308700000",
    end: "1683913500000",
    step: "300000",
    samples: "11496",
    userAgent: "AWSPrometheusDPJavaClient/2.0.436.0 ",
    dashboardUid: "11234",
    panelId: "12"
  },
  component: "query-frontend"
}
```

Limitazioni

Limiti di dimensione delle policy: le policy relative CloudWatch alle risorse dei log sono limitate a 5120 caratteri. Quando CloudWatch Logs rileva che la policy si avvicina al limite di dimensione, abilita automaticamente i gruppi di log che iniziano con. `/aws/vendedlogs/` Quando abiliti la registrazione delle query, 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/`

Comprendi e ottimizza i costi in Amazon Managed Service for Prometheus

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 raccogliatore 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, vedere `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.

Per informazioni su come configurare il periodo di conservazione di un'area di lavoro, vedere.

[Configura il tuo spazio di lavoro](#)

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 [Gestione e inoltro di avvisi in Amazon Managed Service for Prometheus con alert manager](#)

Quali parametri posso utilizzare per monitorare i miei costi?

Monitora `IngestionRate` in Amazon CloudWatch per tenere traccia dei costi di ingestione.

Note

`IngestionRate` fornisce un valore stimato e potrebbe non corrispondere esattamente ai costi di fatturazione finali.

Per ulteriori informazioni sul monitoraggio dei parametri di Amazon Managed Service for Prometheus in, consulta [CloudWatch Usa i CloudWatch parametri per monitorare le risorse di Amazon Managed Service for Prometheus](#)

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 si integra con altri servizi AWS. Questa sezione descrive l'integrazione con il monitoraggio dei costi di Amazon Elastic Kubernetes Service (Amazon EKS) (con Kubecost) e come inserire i parametri dall'uso di Amazon Data Firehose, CloudWatch. Descrive inoltre la configurazione e la gestione di Amazon Managed Service for Prometheus AWS con i moduli Observability Accelerator Terraform o l'utilizzo di Controller for Kubernetes. AWS

Argomenti

- [Integrazione con il monitoraggio dei costi di Amazon EKS](#)
- [Configura Amazon Managed Service per Prometheus con Observability Accelerator AWS](#)
- [Gestisci Amazon Managed Service for AWS Prometheus con Controller per Kubernetes](#)
- [Integrazione delle CloudWatch metriche con Amazon Managed Service for Prometheus](#)

Integrazione con il monitoraggio dei costi di Amazon EKS

Il servizio gestito da Amazon per 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 il servizio gestito da Amazon per 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 multi-cluster. Puoi generare report su più container 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 post sul blog AWS [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 [Multi-cluster cost monitoring for Amazon EKS using Kubecost and Amazon Managed Service for Prometheus](#).

 Note

Per ulteriori informazioni sull'uso di Kubecost, consulta la pagina [Monitoraggio dei costi](#) nella Guida per l'utente di Amazon EKS.

Configura Amazon Managed Service per Prometheus con Observability Accelerator AWS

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 AWS Grafana](#), Distro for e altri strumenti. OpenTelemetry Per aiutarti a utilizzare questi strumenti insieme, AWS fornisce moduli Terraform che configurano l'osservabilità con questi servizi, chiamati [AWS Observability Accelerator](#).

AWS [Observability Accelerator fornisce esempi per il monitoraggio dell'infrastruttura, delle implementazioni di NGINX e 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 Observability Accelerator for Terraform.AWS GitHub](#) Puoi anche leggere il [post sul blog](#) che annuncia Observability Accelerator. AWS

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 account. AWS Per ulteriori informazioni su come configurare il AWS provider per Terraform, consulta [AWS provider](#) 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 configurare 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 la pagina Existing [Cluster with the 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 per il tuo 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 Grafana gestito da Amazon, 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 Grafana gestito da Amazon.
5. Crea due variabili per consentire a Terraform di utilizzare l'area di lavoro Grafana eseguendo i seguenti comandi dalla riga di comando. Dovrai sostituirlo *grafana-workspace-id* con l'ID del tuo spazio 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 Amazon Managed Service for Prometheus esistente, aggiungi l'ID al file, come nell'esempio seguente, sostituendo l'ID dell'area di lavoro Prometheus con `terraform.tfvars` il tuo ID dell'area di lavoro Prometheus. *prometheus-workspace-id* 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 account, tra cui: AWS

- Una nuova area di lavoro del servizio gestito da Amazon per 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 Grafana gestito da Amazon nella tua area di lavoro attuale. La fonte di dati verrà chiamata `aws-observability-accelerator`. Le dashboard verranno elencate nelle dashboard di Observability Accelerator.
- Una [AWS distribuzione per OpenTelemetry](#) operatori configurata nel cluster Amazon EKS fornito, per inviare metriche al tuo spazio di lavoro Amazon Managed Service for Prometheus.

Per visualizzare le tue nuove dashboard, apri la dashboard specifica nella tua area di lavoro Grafana gestito da Amazon. Per ulteriori informazioni sull'uso di Grafana gestito da Amazon, consulta [Lavorare nell'area di lavoro di Grafana](#), nella Guida utente di Grafana gestito da Amazon.

Gestisci Amazon Managed Service for AWS Prometheus con Controller per Kubernetes

Il servizio gestito da Amazon per 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 di AWS Controllers for Kubernetes (CRDs) e gli oggetti Kubernetes nativi senza dover definire alcuna risorsa 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 AWS funzionalità dalla riga di comando.
- 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 il servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus. Per ulteriori informazioni, consulta [Installare un controller ACK](#) nella documentazione di Controllers for Kubernetes su AWS GitHub Usa quello corretto *region* 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 del servizio [gestito da Amazon per 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`. Sostituiscilo **WORKSPACE-ID** con l'ID dell'area di lavoro del passaggio 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 del passaggio precedente. Sostituiscilo **TOPIC-ARN** con l'ARN per l'argomento Amazon SNS a cui inviare notifiche **REGION** e con Regione AWS quello che stai utilizzando. Ricorda che il servizio gestito da Amazon per 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 `WorkspaceAlertManagerDefinition`, o. `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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per 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 parametri 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`. Sostituiscilo *account* con l'ID del tuo account, *workspaceURL* con l'URL appena trovato e *region* con quello appropriato 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 *PrometheusChartName* *PrometheusNamespace*, 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 del servizio gestito da Amazon per Prometheus tramite `awscurl`. Sostituiscilo *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 definizioni di risorse personalizzate (CRDs), risiedono all'interno del 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 Amazon Managed Service for Prometheus

Può essere utile avere tutte le metriche in un unico posto. Amazon Managed Service for Prometheus non acquisisce automaticamente i parametri di Amazon. CloudWatch Tuttavia, puoi utilizzare Amazon Data Firehose e inviare i CloudWatch parametri AWS Lambda ad Amazon Managed Service for Prometheus.

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 metrici 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 [Typescript AWS CDK](#) 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 sul servizio gestito da Amazon per Prometheus. Crea la tua area di lavoro per il servizio gestito da Amazon per 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 sul servizio gestito da Amazon per Prometheus, consulta la Guida per l'utente del [servizio gestito da Amazon per Prometheus](#).

Per installare dipendenze

1. Installare le dipendenze

Dalla radice del repository `aws-o11y-recipes`, 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 cartella /lambda, 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 del servizio gestito da Amazon per Prometheus sostituendo `{workspace}` con l'ID dello spazio di lavoro appena creato e la regione in cui si trova l'area di lavoro del servizio gestito da Amazon per 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, a <https://console.aws.amazon.com/cloudwatch/home#metric-streams:StreamsList> e seleziona Crea flusso metrico.
2. Seleziona i parametri necessari, tutti o solo quelli dei 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 flusso Kinesis Data Firehose, seleziona il flusso creato in precedenza. Avrà un nome simile a CdkStack-KinesisFirehoseStream123456AB-sample1234.
5. Imposta l'output sul formato JSON.
6. Assegna al flusso di parametri un nome significativo per te.
7. Scegli Create metric stream (Crea flusso di parametri).
8. (Facoltativo) Per verificare l'invocazione della funzione Lambda, accedi alla console [Lambda](#) e scegli la funzione KinesisMessageHandler. Seleziona la scheda Monitora e la sottoscheda Registri e in Invocazioni recenti dovrebbero essere visualizzate le voci della funzione Lambda che viene attivata.

 Note

Potrebbero essere necessari fino a 5 minuti prima che le invocazioni inizino a essere visualizzate nella scheda Monitora

Le tue metriche vengono ora trasmesse in streaming da Amazon ad 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 flusso di 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 nel servizio gestito da Amazon per Prometheus

La sicurezza del cloud è la massima priorità. AWS In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per maggiori informazioni sui programmi di conformità applicabili ad Amazon Managed Service for Prometheus, [AWS consulta Services in Scope by Compliance Program Services in Scope by Compliance AWS](#) .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio 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 il servizio gestito da Amazon per Prometheus. Gli argomenti seguenti descrivono come configurare il servizio gestito da Amazon per Prometheus per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di 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 nel servizio gestito da Amazon per Prometheus](#)
- [Sicurezza dell'infrastruttura nel servizio gestito da Amazon per Prometheus](#)
- [Utilizzo di ruoli collegati ai servizi per il servizio gestito da Amazon per Prometheus](#)
- [Registrazione delle chiamate API del servizio gestito da Amazon per Prometheus tramite AWS CloudTrail](#)

- [Imposta ruoli IAM per gli account del servizio.](#)
- [Utilizzo del servizio gestito da Amazon per 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 o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Managed Service for Prometheus o Servizi AWS altro utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per 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

Il tenant unico IDs isola i dati di diversi clienti. Questi IDs limitano i dati dei clienti accessibili. I clienti non possono cambiare inquilino. IDs

Amazon Managed Service for Prometheus crittografa i dati archiviati con le chiavi (). 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 gratuitamente.

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 [raccoglitori 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 for 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 il. AWS Management Console AWS KMS APIs 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 per 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:amp:arn` e il valore è l'[Amazon Resource Name](#) (ARN) dell'area di lavoro.

Example

```
"encryptionContext": {
  "aws:amp: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 specificata. 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":
"0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
},
"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](#)

- [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 sul metodo consigliato per la firma delle richieste, consulta [Signature Version 4 AWS per le richieste API](#) nella Guida per l'utente IAM.

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi

AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente IAM.

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

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

Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi [passare da un ruolo utente a un ruolo IAM \(console\)](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente IAM.

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

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Create a role for a third-party identity provider \(federation\)](#) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso inoltrato (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon](#) nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

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

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

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

Policy basate sull'identità

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

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

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

Liste di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica della lista di controllo degli accessi \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

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

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente IAM.
- **Politiche di controllo del servizio (SCPs):** SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell'Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- **Politiche di controllo delle risorse (RCPs):** RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere [Resource control policies \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

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

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
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	No
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	No
● Ruoli di servizio	No
Ruoli collegati al servizio	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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

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 sulle risorse: sì

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Policy definite dal servizio gestito da Amazon per Prometheus

Supporta le operazioni di policy: si

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

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

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

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. In altre parole, 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 \(ARN\)](#). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco dei tipi di risorse Amazon Managed Service for Prometheus e ARNs relativi, consulta [Resources defined by Amazon Managed Service for Prometheus nel Service Authorization Reference](#). 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 delle condizioni delle policy specifiche del servizio: No

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

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. È possibile compilare espressioni

condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

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

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

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per 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](#).

Elenchi di controllo degli accessi (ACLs) in Amazon Managed Service for Prometheus

Supporti: no ACLs

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

Controllo degli accessi basato su attributi (ABAC) con Amazon Managed Service per Prometheus

Supporta ABAC (tag nelle policy): sì

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

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

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

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

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

Utilizzo di credenziali temporanee con il servizio gestito da Amazon per Prometheus

Supporta le credenziali temporanee: sì

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 accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Passaggio da un ruolo utente a un ruolo IAM \(console\)](#) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API o l'AWS CLI. AWS è quindi possibile utilizzare tali credenziali temporanee per accedere. 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](#).

Inoltra le sessioni di accesso per Amazon Managed Service for Prometheus

Supporta l'inoltro delle sessioni di accesso (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 [Create a role to delegate permissions to an 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 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 \(console\)](#) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Amazon Managed Service for Prometheus, incluso il formato di per ogni tipo di ARNs risorsa, [consulta Azioni, risorse e chiavi di condizione per Amazon Managed Service for Prometheus nel Service](#) Authorization Reference.

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 ai tuoi 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. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Protezione dell'accesso API con MFA](#) nella Guida per l'utente IAM.

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

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": "*"
    }
  ]
}
```

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per 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 IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Autorizzazioni e policy IAM

L'accesso alle azioni e ai dati del servizio gestito da Amazon per Prometheus richiede delle credenziali. Tali credenziali devono disporre delle autorizzazioni per eseguire le azioni e accedere alle AWS risorse, ad esempio recuperare i dati di Amazon Managed Service for Prometheus sulle tue risorse cloud. Le seguenti sezioni forniscono dettagli su come utilizzare AWS Identity and Access Management (IAM) e Amazon Managed Service for Prometheus per proteggere le risorse, controllando chi può accedervi. Per ulteriori informazioni, consulta [Policy e autorizzazioni in IAM](#).

Permessi di Amazon Managed Service per Prometheus

Per visualizzare l'elenco delle possibili azioni di Amazon Managed Service for Prometheus, i tipi di risorse e le chiavi di condizione, [consulta Azioni, risorse e chiavi di condizione per Amazon Managed Service for Prometheus](#).

Esempio di policy IAM

Questa sezione fornisce esempi di altre policy autogestite che puoi creare.

La seguente politica IAM garantisce l'accesso completo al servizio gestito da Amazon per Prometheus e consente inoltre a un utente di scoprire i cluster Amazon EKS e visualizzarne i dettagli.

JSON

```
{
  "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:

- [Governance e conformità per la sicurezza](#): queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- [Riferimenti sui servizi conformi ai requisiti HIPAA](#): elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- [AWS Risorse per la 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 nel servizio gestito da Amazon per Prometheus

L'infrastruttura AWS globale è costruita attorno a regioni e zone di disponibilità. AWS AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, 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 su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

[Oltre all'infrastruttura AWS globale, Amazon Managed Service for Prometheus offre diverse funzionalità per aiutarti a supportare le tue esigenze di resilienza e backup dei dati, incluso il supporto per dati ad alta disponibilità.](#)

Sicurezza dell'infrastruttura nel servizio gestito da Amazon per Prometheus

In quanto servizio gestito, Amazon Managed Service for Prometheus è protetto dalla sicurezza di rete globale. AWS [Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per

la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizza chiamate API AWS pubblicate per accedere ad Amazon Managed Service for Prometheus attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. 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 `AWSService RoleForAmazonPrometheusScraper` 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 per `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, è possibile 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. AWSService RoleForAmazonPrometheusScraper 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. AWSService RoleForAmazonPrometheusScraper 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 del servizio gestito da Amazon per Prometheus tramite AWS CloudTrail

Amazon Managed Service for Prometheus è integrato [AWS CloudTrail](#)on, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un. Servizio AWS CloudTrailacquisisce tutte le chiamate API per Amazon Managed Service for Prometheus come eventi. Le chiamate acquisite includono chiamate dalla console Amazon Managed Service per Prometheus e chiamate in codice verso le operazioni dell'API Amazon Managed Service for Prometheus. 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, quando è stata effettuata e ulteriori dettagli.

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

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità 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 Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrail Lake](#).

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail [Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC](#). ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail](#)

Amazon Managed Service per gli eventi di gestione di Prometheus in CloudTrail

[Gli eventi di gestione](#) forniscono informazioni sulle operazioni di gestione eseguite sulle risorse del tuo. Account AWS Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Amazon Managed Service for Prometheus registra tutte le operazioni del piano di controllo di Amazon Managed Service for Prometheus come eventi di gestione. [Per un elenco delle operazioni del piano di controllo Amazon Managed Service for Prometheus a cui accede Amazon Managed Service for Prometheus, consulta il riferimento all' CloudTrailAPI Amazon Managed Service for Prometheus.](#)

Esempi di eventi Amazon Managed Service per Prometheus

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sul funzionamento dell'API richiesto, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

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":
    "Z3JvdXBzOgogIC0gYmFtZTogdGVzdFJ1bGVHcm91cHN0YWw1c3BhY2UKICAgIHJ1bGVzOgogICAgLSBhbGVydDogdGVzd
    "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"
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

Imposta ruoli IAM per gli account del servizio.

Grazie ai ruoli IAM per gli account del servizio, è possibile 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](#).

I ruoli IAM per gli account del servizio sono noti anche come ruoli di servizio.

Nel servizio gestito da Amazon per Prometheus, l'utilizzo dei ruoli del servizio può aiutarti a ottenere i ruoli necessari per l'autorizzazione e l'autenticazione tra il servizio gestito da Amazon per Prometheus, i server Prometheus e i server Grafana.

Prerequisiti

Le procedure in questa pagina richiedono che sia installata l'interfaccia a riga AWS CLI di comando EKSCTL.

Configura i ruoli di servizio per l'acquisizione di parametri dai cluster Amazon EKS.

Per configurare i ruoli del servizio per consentire al servizio gestito da Amazon per 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 del servizio per l'acquisizione nel servizio gestito da Amazon per Prometheus

1. Creare un archivio denominato `createIRSA-AMPIngest.sh` con i seguenti contenuti. Sostituire `<my_amazon_eks_clusternamespace>` con il nome del cluster e sostituirlo `<my_prometheus_namespace>` con il namespace Prometheus.

```
#!/bin/bash -e
CLUSTER_NAME=<my_amazon_eks_clusternamespace>
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
  fi
}

```

```

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 del servizio per le domande dei parametri

Per configurare il ruolo IAM per l'account del servizio (service role) per abilitare l'interrogazione dei parametri dagli spazi di lavoro del servizio gestito da Amazon per Prometheus, devi accedere a un account con le seguenti autorizzazioni:

- iam:CreateRole
- iam:CreatePolicy
- iam:GetRole
- iam:AttachRolePolicy
- iam:GetOpenIDConnectProvider

Configurare ruoli del servizio per l'interrogazione dei parametri del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus con endpoint VPC di interfaccia

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi stabilire connessioni private tra il tuo VPC e Amazon Managed Service for Prometheus. È possibile utilizzare queste connessioni per abilitare il servizio gestito da Amazon per Prometheus in modo da comunicare con le risorse nel VPC senza accedere all'Internet pubblico.

Amazon VPC è un AWS servizio che puoi utilizzare per avviare AWS risorse in una rete virtuale definita dall'utente. 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 al servizio gestito da Amazon per Prometheus, è necessario definire un endpoint VPC di interfaccia per connettere il VPC ai servizi AWS. L'endpoint offre una connettività scalabile e affidabile al servizio gestito da Amazon per 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 sono alimentati da AWS PrivateLink, una AWS tecnologia che consente la comunicazione privata tra AWS i servizi utilizzando 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 lavorare con APIs Prometheus compatibile. Per ulteriori informazioni, consulta [Prometheus-compatible nella APIs](#) Amazon Managed Service for Prometheus User Guide.

- `com.amazonaws.region.aps`

Scegli questo nome di servizio per eseguire attività di gestione dell'area di lavoro. Per ulteriori informazioni, consulta [Amazon Managed Service for Prometheus](#) nella Guida per l'utente di Amazon Managed Service for APIs Prometheus.

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 un endpoint VPC per AWS STS, consulta Using [interface AWS STS VPC endpoint](#) nella Guida per l'utente. AWS Identity and Access Management [È necessario impostare l'utilizzo di endpoint AWS STS regionalizzati.](#)

Per ulteriori informazioni, incluse step-by-step le istruzioni per creare un endpoint VPC di interfaccia, consulta [Creazione di un endpoint di interfaccia nella](#) Amazon VPC User Guide.

Note

Puoi utilizzare le policy degli endpoint VPC per controllare l'accesso al tuo endpoint VPC con interfaccia del servizio gestito da Amazon per 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. Il servizio gestito da Amazon per 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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus. Questa policy consente agli utenti con ruolo che si `PromUser` connettono al servizio gestito da Amazon per Prometheus tramite VPC di visualizzare aree di lavoro e gruppi di regole, ma non, ad esempio, di creare o eliminare aree di lavoro.

JSON

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

```

    "Action": [
      "aps:DescribeWorkspace",
      "aps:DescribeRuleGroupsNamespace",
      "aps:ListRuleGroupsNamespaces",
      "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-5555555555555"
        }
      }
    }
  ]
}

```

Risolvi gli errori di Amazon Managed Service for Prometheus

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 429 simile al seguente esempio, le tue richieste hanno superato la quota di Amazon Managed Service for Prometheus per la velocità (transazioni al secondo) con cui puoi inviare dati al tuo spazio di lavoro utilizzando l'API compatibile con Prometheus. RemoteWrite

```
ts=2024-03-26T16:50:21.780708811Z caller=dedupe.go:112 component=remote level=error
remote_name=ab123c
url=https://aps-workspaces.us-east-1.amazonaws.com/workspaces/workspace_id/api/v1/
remote_write
msg="non-recoverable error" count=1000 exemplarCount=0 err="server returned HTTP status
429 Too Many Requests: {\\"message\\":\\"Rate 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 [Quote predefinite della serie attiva](#)

```
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 Prom 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](#).

- se il limite di serie per utente è stato `<value>` superato, contatta l'amministratore per aumentarlo
- se il limite di serie per metrico è stato `<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>	
Most-to-least elenco di serie attive per nome metrico	<code>sort_desc(count by(__name__))</code> <code>({__name__!=""})</code>	
Numero di etichette per serie di parametri	<code>group by(mylabelname)</code> <code>({__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 [Usa i CloudWatch parametri per monitorare le risorse di Amazon Managed Service for Prometheus](#).

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

Inserimento di tag in Amazon Managed Service per Prometheus

Un tag è un'etichetta di attributo personalizzata che tu o AWS assegnate a una risorsa. AWS Ogni AWS tag è composto 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 ti aiutano a identificare e organizzare AWS le tue risorse. Molti AWS servizi supportano l'etichettatura, quindi puoi assegnare lo stesso tag a risorse di servizi diversi per indicare che le risorse sono correlate. Ad esempio, puoi assegnare a un workspace del servizio gestito da Amazon per Prometheus lo stesso tag che assegni a un bucket Amazon S3. Per ulteriori informazioni sulle strategie di tag, consulta [Tag delle AWS risorse](#).

Nel servizio gestito da Amazon per Prometheus, è possibile contrassegnare sia nelle aree di lavoro che i namespace dei gruppi di regole. È possibile utilizzare la console, o SDKs per aggiungere, gestire e rimuovere tag per queste risorse. AWS CLI APIs 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 del servizio gestito da Amazon per 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 tagging viene utilizzato su più AWS servizi e risorse, ricorda che altri servizi potrebbero avere restrizioni 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' AWS uso. Non è possibile modificare né eliminare le chiavi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati ai fini del tags-per-resource limite.

Argomenti

- [Etichetta: Amazon Managed Service per le aree di lavoro Prometheus](#)
- [Tag dei namespace dei gruppi di regole.](#)

Etichetta: Amazon Managed Service per le aree di lavoro Prometheus

I tag sono etichette personalizzate che possono essere assegnate a una risorsa. Includono una chiave univoca e un valore opzionale (in una coppia chiave-valore). I tag aiutano a identificare e a organizzare le risorse AWS . In Amazon Managed Service for Prometheus, gli spazi di lavoro (e i namespace dei gruppi di regole) possono essere etichettati. Puoi utilizzare la console, la AWS CLI o SDKs aggiungere APIs, gestire e rimuovere tag per queste risorse. Oltre a identificare, organizzare e tracciare i tuoi spazi di lavoro con i tag, puoi utilizzare i tag nelle policy IAM per controllare chi può visualizzare e interagire con le tue risorse Amazon Managed Service for Prometheus.

Utilizza le procedure descritte in questa sezione per utilizzare i tag per le aree di lavoro del servizio gestito da Amazon per Prometheus.

Argomenti

- [Aggiunta di un 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 un tag a un'area di lavoro

L'aggiunta di tag al servizio gestito da Amazon per 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 aggiungere tag AWS CLI a un'area di lavoro di 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 del servizio gestito da Amazon per Prometheus al momento della creazione, consulta [Crea un'area di lavoro Amazon Managed Service per Prometheus](#).

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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per 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 [Crea un'area di lavoro Amazon Managed Service per Prometheus](#).

In questi passaggi, supponiamo che tu abbia già installato una versione recente di AWS CLI o 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, eseguire 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 di Amazon Managed Service for Prometheus denominata `My-Workspace` con due tag, una chiave tag denominata con il valore del tag e una chiave di tag *Status* denominata con il valore *Secret* del tag di: *Team My-Team*

```
aws amp tag-resource --resource-arn arn:aws:aps:us-  
west-2:123456789012:workspaces/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 tue AWS risorse e a gestirne l'accesso. Per ulteriori informazioni sulle strategie di tagging, consulta [Tagging AWS](#) Resources.

Visualizzazione dei tag per un'area di lavoro del servizio gestito da Amazon per Prometheus (console)

Puoi utilizzare la console per visualizzare i tag associati a un'area di lavoro del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (AWS CLI)

Segui questi passaggi per utilizzare per visualizzare i AWS tag AWS CLI di 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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (console)

Puoi utilizzare la console per modificare i tag associati a un'area di lavoro del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (AWS CLI)

Segui questi passaggi per utilizzare per aggiornare un tag AWS CLI 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 del servizio gestito da Amazon per 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 AWS risorse associate a quel tag.

Important

La rimozione dei tag per un'area di lavoro del servizio gestito da Amazon per 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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (AWS CLI)

Segui questi passaggi per utilizzare per rimuovere un tag da un'area di lavoro. AWS CLI La rimozione di un tag non lo elimina completamente, ma rimuove semplicemente l'associazione tra il tag e l'area di lavoro.

Note

Se elimini un'area di lavoro del servizio gestito da Amazon per 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 su uno spazio di lavoro denominato 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.

I tag sono etichette personalizzate che possono essere assegnate a una risorsa. Includono una chiave univoca e un valore opzionale (in una coppia chiave-valore). I tag aiutano a identificare e a organizzare le risorse AWS. In Amazon Managed Service for Prometheus, i namespace (e gli spazi di lavoro) dei gruppi di regole possono essere etichettati. Puoi utilizzare la console, la AWS CLI o SDKs aggiungere APIs, gestire e rimuovere tag per queste risorse. Oltre a identificare, organizzare e tracciare i namespace dei tuoi gruppi di regole con i tag, puoi utilizzare i tag nelle policy IAM per controllare chi può visualizzare e interagire con le tue risorse Amazon Managed Service for Prometheus.

Utilizza le procedure in questa sezione per lavorare con i tag per i namespace dei gruppi di regole del servizio gestito da Amazon per 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 ai namespace di un gruppo di regole di Amazon Managed Service for Prometheus può aiutarti a identificare e organizzare le tue risorse e a gestirne l'accesso. AWS 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 uno spazio dei nomi dei gruppi di regole di 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 [Crea 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 del servizio gestito da Amazon per 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 per utilizzare lo spazio dei nomi AWS CLI per aggiungere un tag a uno spazio dei nomi dei gruppi di regole Amazon Managed Service for Prometheus. Per aggiungere un tag a un namespace dei gruppi di regole durante la creazione, consulta [Carica un file di configurazione delle regole su Amazon Managed Service for Prometheus](#).

In questi passaggi, supponiamo che tu abbia già installato una versione recente AWS CLI o 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 etichettare uno spazio dei nomi Amazon Managed Service for Prometheus denominato `My-Workspace` con due tag, una chiave tag denominata con il valore del tag e una chiave di tag *Status* denominata con il valore *Secret* del tag di: *Team 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 tue AWS risorse e a gestirne l'accesso. Per ulteriori informazioni sulle strategie di tagging, consulta [Tagging AWS Resources](#).

Visualizza i tag per un namespace dei gruppi di regole del servizio gestito da Amazon per Prometheus (console)

Puoi utilizzare la console per visualizzare i tag associati a un namespace dei gruppi di regole del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (AWS CLI)

Segui questi passaggi per utilizzare lo spazio dei nomi AWS CLI per un gruppo di regole per visualizzare i AWS tag. 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 tutti i criteri 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 del servizio gestito da Amazon per Prometheus (console)

Puoi utilizzare la console per modificare i tag associati a un namespace dei gruppi di regole del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (AWS CLI)

Segui questi passaggi per utilizzare il per aggiornare un tag AWS CLI per un namespace di 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 AWS risorse associate a quel 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 del servizio gestito da Amazon per 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 del servizio gestito da Amazon per Prometheus (AWS CLI)

Segui questi passaggi per rimuovere un tag dallo AWS CLI spazio dei nomi 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 del servizio gestito da Amazon per 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 su un'area di lavoro denominata My-Workspace con la chiave tag: *Status*

```
aws amp untag-resource --resource-arn rn: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 al servizio gestito da Amazon per Prometheus.

Quote del servizio

Il servizio gestito da Amazon per 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 di Amazon, puoi 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 [Quote predefinite della serie attiva](#). 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. Il valore massimo per le serie attive per area di lavoro è di un miliardo.

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

Nome	Predefinita	Adattata	Descrizione
			area di lavoro: 20.000 Nota: se viene raggiunto il limite, viene registrato il campione metrico, ma i metadati che superano il limite vengono eliminati.
Serie attive per area di lavoro	Ogni regione supportata: 50.000.000	Sì	Il numero di serie attive uniche per area di lavoro (fino a un massimo di 1 miliardo). Una serie è attiva se un campione è stato segnalato nelle ultime 2 ore. La capacità da 2 M a 50 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	Sì	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	No	La dimensione massima di un file di definizione di Alert Manager, in megabyte.

Nome	Predefinita	Adattata	Descrizione
Dimensione del payload degli avvisi in Alert Manager	Ogni regione supportata: 20	No	La dimensione massima del payload degli avvisi di Alert Manager per area di lavoro, in megabyte. La dimensione degli avvisi dipende dalle etichette e dalle annotazioni.
Avvisi in Alert Manager	Ogni regione supportata: 1.000	Sì	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.
Tasso di importazione per area di lavoro	Ogni regione supportata: 170.000	Sì	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	Sì	Il numero massimo di regole di inibizione nel file di definizione di alert manager.
Dimensione etichetta	Ogni regione supportata: 7	No	La dimensione massima combinata di tutte le etichette e i valori delle etichette accettati per una serie, in kilobyte.

Nome	Predefinita	Adattata	Descrizione
LabelSet limiti per area di lavoro	Ogni regione supportata: 100	Sì	Il numero massimo di limiti di labelset che possono essere creati per area di lavoro.
Etichette per serie di parametri	Ogni regione supportata: 150	Sì	Numero di etichette per serie di parametri.
Lunghezza dei metadati	Ogni regione supportata: 1	No	La lunghezza massima accettata per i metadati metrici, in kilobyte. I metadati si riferiscono al nome della metrica, al tipo, all'unità e al testo di aiuto.
Metadati per parametro	Ogni regione supportata: 10	No	Numero di metadati per parametro. Nota: se il limite viene raggiunto, il campione metrico viene registrato, ma i metadati che superano il limite vengono eliminati.
Nodi nell'albero di instradamento di alert manager	Ogni regione supportata: 100	Sì	Il numero massimo di nodi nell'albero di instradamento di alert manager.

Nome	Predefinita	Adatta e	Descrizione
Numero di operazioni API per regione in transazioni al secondo	Ogni regione supportata: 10	Sì	Il numero massimo di operazioni API al secondo per regione per tutti gli Amazon Managed Service for APIs Prometheus, inclusi workspace APIs CRUD, APIs tagging, group di regole, namespace CRUD e alert manager definition CRUD. APIs APIs
Numero e operazioni API per area di lavoro nelle transazioni GetSeries al secondo GetLabels GetMetricMetadata	Ogni regione supportata: 10	No	Il numero massimo di GetSeries operazioni API GetMetric Metadata compatibili con Prometheus al secondo per area di lavoro. GetLabels
Numero di operazioni QueryMetrics API per area di lavoro in transazioni al secondo	Ogni regione supportata: 300	No	Il numero massimo di operazioni API QueryMetrics compatibili con Prometheus al secondo per area di lavoro.
Numero di operazioni RemoteWrite API per area di lavoro in transazioni al secondo	Ogni regione supportata: 3.000	No	Il numero massimo di operazioni API RemoteWrite compatibili con Prometheus al secondo per area di lavoro.

Nome	Predefinita	Adatta e	Descrizione
Numero di altre operazioni API compatibili con Prometheus per area di lavoro in transazioni al secondo	Ogni regione supportata: 100	No	Il numero massimo di operazioni API al secondo per area di lavoro per tutte le altre applicazioni compatibili con Prometheus APIs , tra cui, ecc. ListAlerts ListRules
Byte di query per query istantanee	Ogni Regione supportata: 5	No	Il numero massimo di byte che possono essere scansionati da una singola query istantanea, in gigabyte.
Byte di query per query di intervallo	Ogni Regione supportata: 5	No	Il numero massimo di byte che è possibile scansionare per intervall o di 24 ore in una query a intervallo singolo, in gigabyte.
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.

Nome	Predefinita	Adatta e	Descrizione
Intervallo di tempo delle query in giorni	Ogni regione supportata: 95	No	L'intervallo di tempo massimo di QueryMetrics GetSeries, e GetLabels APIs.
Dimensione richiesta	Ogni regione supportata: 1	No	La dimensione massima della richiesta per l'inserimento o l'interrogazione, in megabyte.
Intervallo di valutazione delle regole	Ogni regione supportata: 30	Sì	L'intervallo minimo di valutazione delle regole di un gruppo di regole per area di lavoro, in secondi.
Dimensione del file di definizione del namespace del gruppo di regole	Ogni regione supportata: 1	No	La dimensione massima di un file di definizione dello spazio dei nomi di un gruppo di regole, in megabyte.
Regole per area di lavoro	Ogni regione supportata: 2.000	Sì	Il numero massimo di regole per area di lavoro.
Silenzi per area di lavoro	Ogni regione supportata: 1.000	Sì	Numero massimo di silenzi, inclusi quelli scaduti, attivi e in sospeso, per area di lavoro.
Modelli nel file di definizione di alert manager	Ogni regione supportata: 100	Sì	Il numero massimo di modelli nel file di definizione di alert manager.

Nome	Predefinita	Adatta e	Descrizione
Area di lavoro per regione per account	Ogni regione supportata: 25	Sì	Il numero massimo di aree di lavoro per regione.

Quote predefinite della serie attiva

Le aree di lavoro di Amazon Managed Service for Prometheus si adattano automaticamente all'utilizzo di importazione. All'aumentare dell'utilizzo, il servizio aumenta automaticamente la capacità delle serie temporali fino alla quota predefinita.

L'area di lavoro Amazon Managed Service for Prometheus si ridimensiona automaticamente, in base all'utilizzo, in due modi:

1. Quando l'utilizzo medio di 30 minuti è inferiore a 5 milioni di serie, la capacità raddoppia (ad esempio, un'area di lavoro con 3,5 milioni di utilizzo ottiene 7 milioni di capacità).
2. Quando l'utilizzo supera i 5 milioni di serie, l'area di lavoro aggiunge un buffer di 10 milioni (ad esempio, un'area di lavoro con 25 milioni di utilizzo ottiene 35 milioni di capacità).

Amazon Managed Service for Prometheus alloca automaticamente più capacità all'aumentare dell'ingestione, fino a raggiungere la quota stabilita. Questo aiuta a garantire che il carico di lavoro non subisca un rallentamento prolungato. Tuttavia, si può verificare una limitazione se si raddoppiano o si superano i 10 milioni rispetto al valore di base precedente calcolato negli ultimi 30 minuti. Per evitare limitazioni, Amazon Managed Service for Prometheus consiglia di aumentare gradualmente l'ingestione quando si supera il livello di riferimento precedente.

Note

La capacità minima per le serie temporali attive è di 2 milioni e 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](#).

Scalare al di sopra della quota predefinita

Quando richiedi un aumento della quota oltre la quota predefinita delle serie attive, Amazon Managed Service for Prometheus regola di conseguenza la capacità del tuo spazio di lavoro. Se non utilizzi appieno la maggiore capacità, il servizio recupererà la parte inutilizzata nel tempo. Man mano che l'utilizzo aumenta, l'area di lavoro verrà nuovamente ridimensionata automaticamente.

Tuttavia, si può verificare una limitazione se si raddoppiano o si superano i 50 milioni di serie temporali attive rispetto alla precedente baseline calcolata nelle ultime 2 ore. Per esempio:

- Se la tua quota è di 100 milioni e la tua linea di base è di 30 milioni, puoi aumentare fino a 60 milioni entro 2 ore senza limitazioni.
- Se la tua quota è di 100 milioni e la tua linea di base è di 50 milioni, puoi aumentare fino a raggiungere tutti i 100 milioni entro 2 ore senza limitazioni.

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 utilizzarlo CloudWatch per monitorare l'ingestione e per creare un allarme per avvisarti quando stai per raggiungere i limiti di limitazione. Per ulteriori informazioni, consulta [Usa i CloudWatch parametri per monitorare le risorse di Amazon Managed Service for Prometheus](#).

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 raccoglitore, 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

Il servizio gestito da Amazon per 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.

Riferimento all'API Amazon Managed Service per Prometheus

Amazon Managed Service per Prometheus offre due tipi di: APIs

1. Amazon Managed Service for APIs Prometheus: consentono di creare e gestire APIs le aree di lavoro di Amazon Managed Service for Prometheus, tra cui operazioni per aree di lavoro, scraper, definizioni di alert manager, namespace di gruppi di regole e registrazione. Per interagire con questi linguaggi di programmazione, usi il, disponibile per vari linguaggi di programmazione. AWS SDKs APIs
2. Compatibile con Prometheus APIs: Amazon Managed Service for Prometheus supporta HTTP compatibili con Prometheus. APIs Questi APIs consentono di creare applicazioni personalizzate, automatizzare i flussi di lavoro, integrarsi con altri servizi o strumenti e interrogare e interagire con i dati di monitoraggio utilizzando il linguaggio di query Prometheus (PromQL).

Questa sezione elenca le operazioni API e le strutture di dati supportate dal servizio gestito da Amazon per Prometheus.

Per informazioni sulle quote per le serie, le etichette e le richieste API, consulta le quote del servizio [Amazon Managed Service for Prometheus nella Guida per l'utente di Amazon Managed Service for Prometheus](#).

Argomenti

- [Servizio gestito Amazon per Prometheus APIs](#)
- [Compatibile con Prometheus APIs](#)

Servizio gestito Amazon per Prometheus APIs

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 APIs aree di lavoro, scraper, definizioni di alert manager, gruppi di regole, namespace e registrazione.

Per informazioni dettagliate su Amazon Managed Service for Prometheus, consulta l'[Amazon Managed Service for APIs Prometheus API Reference](#).

Utilizzo di Amazon Managed Service per Prometheus con un SDK AWS

AWS i kit di sviluppo software (SDKs) 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 nella loro lingua preferita. Per un elenco degli strumenti SDKs 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 altra SDKs versione utilizzata nei tuoi progetti e di mantenerla SDKs aggiornata. L' AWS SDK offre le caratteristiche e le funzionalità più recenti e anche aggiornamenti di sicurezza.

Compatibile con Prometheus APIs

Amazon Managed Service for Prometheus supporta le seguenti versioni compatibili con Prometheus. APIs

Per ulteriori informazioni sull'uso della compatibilità con Prometheus APIs, vedere. [Interrogazione tramite Prometheus compatibile APIs](#)

Argomenti

- [CreateAlertManagerAlerts](#)
- [DeleteAlertManagerSilence](#)
- [GetAlertManagerStatus](#)
- [GetAlertManagerSilence](#)
- [GetLabels](#)
- [GetMetricMetadata](#)
- [GetSeries](#)
- [ListAlerts](#)
- [ListAlertManagerAlerts](#)
- [ListAlertManagerAlertGroups](#)
- [ListAlertManagerReceivers](#)

- [ListAlertManagerSilences](#)
- [ListRules](#)
- [PutAlertManagerSilences](#)
- [QueryMetrics](#)
- [RemoteWrite](#)

CreateAlertManagerAlerts

L'CreateAlertManagerAlerts operazione crea un avviso nell'area di lavoro.

Verbi HTTP validi:

POST

Valido: URIs

/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

Valido URIs:

`/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

Valido URIs:

/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

Valido URIs:

`/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'GetLabeloperazione recupera le etichette associate a una serie temporale.

Verbi HTTP validi:

GET, POST

Valido URIs:

`/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'GetMetricMetadata operazione 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

Valido URIs:

/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'GetSeries operazione recupera l'elenco delle serie temporali che corrispondono a un determinato set di etichette.

Verbi HTTP validi:

GET, POST

Valido URIs:

/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": "servicesstackprometheusc14a6d7-node-exporter",
  "kubernetes_namespace": "default",
  "kubernetes_node": "ip-10-0-100-36.us-west-2.compute.internal",
  "mode": "iowait",
  "release": "servicesstackprometheusc14a6d7"
},
...
]
```

ListAlerts

L'ListAlerts operazione recupera gli avvisi attualmente attivi nell'area di lavoro.

Verbi HTTP validi:

GET

Valido URIs:

/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

Valido URIs:

/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'ListAlertManagerAlertGroupsoperazione recupera un elenco di gruppi di avvisi configurati in alert manager nell'area di lavoro.

Verbi HTTP validi:

GET

Valido URIs:

/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 tvero, 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'ListAlertManagerReceivers operazione recupera informazioni sui ricevitori configurati in alert manager.

Verbi HTTP validi:

GET

Valido URIs:

/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'ListAlertManagerSilences operazione recupera informazioni sui silenzi di avviso configurati nell'area di lavoro.

Verbi HTTP validi:

GET

Valido URIs:

/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

Valido URIs:

/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

Valido URIs:

/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

Valido URIs:

`/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.

`max_samples_processed_warning_threshold=<integer>` (Facoltativo) Imposta la soglia di avviso per Query Samples Processed (QSP). Quando le query raggiungono questa soglia, nella risposta dell'API viene restituito un messaggio di avviso.

`max_samples_processed_error_threshold=<integer>` (Facoltativo) Imposta la soglia di errore per Query Samples Processed (QSP). Le query che superano questa soglia verranno rifiutate con un errore e non verranno addebitate. Utilizzato per evitare costi di interrogazione eccessivi.

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

Valido URIs:

`/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 in [https://github.com/prometheus/prometheus/blob/1c624c58ca934f618be737b4995e22051f5724c1/prompb/remote.pb.go](https://github.com/prometheus/prometheus/blob/1c624c58ca934f618be737b4995e22051f5724c1/prompb/remote.pb.go#L64) #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, è possibile sottoscrivere un feed RSS.

Modifica	Descrizione	Data
È stato aggiunto il supporto di policy basate sulle risorse	Le seguenti azioni API sono ora disponibili: • DeleteResourcePolicy • DescribeResourcePolicy • PutResourcePolicy	15 agosto 2025
Aggiornamento alla policy IAM AmazonPrometheusConsoleFullAccess gestita.	La AmazonPrometheusConsoleFullAccess policy è stata aggiornata. Le <code>aps:DescribeQueryLoggingConfiguration</code> autorizzazioni <code>aps:CreateQueryLoggingConfiguration</code> <code>aps:UpdateQueryLoggingConfiguration</code> <code>aps>DeleteQueryLoggingConfiguration</code> „„ sono state aggiunte alla politica.	5 maggio 2025
Aggiunta la modifica dei file di definizione delle regole e dei file di configurazione di Alert Manager nella console	Amazon Managed Service for Prometheus aggiunge il supporto per la modifica dei file di configurazione di Alert Manager e dei file di definizione delle regole	16 maggio 2024

dall'interno della console
Amazon Managed Service for
Prometheus.

[Aggiunta una configurazione
del raccoglitore AWS gestito
più semplice con voci di
accesso per Amazon EKS](#)

[Amazon Managed Service
for Prometheus aggiunge il
supporto per le voci di accesso
Amazon EKS per semplificare la configurazione dei
raccoglitori gestiti.](#) AWS La
politica [AmazonPrometheusSc
raperServiceRolePolicy](#) gestita
per i raccoglitori AWS gestiti
viene aggiornata per consentir
e l'eliminazione delle voci di
accesso che non vengono più
utilizzate.

2 maggio 2024

[Sposta AWS l'API in una guida
di riferimento API separata](#)

Gli Amazon Managed
Service for AWS APIs
Prometheus sono ora
disponibili nel loro riferimen
to, l'[Amazon Managed
Service](#) for Prometheus API
Reference. La compatibi
lità con Prometheus APIs
continua a essere documenta
ta nella Guida per l'utente di
[Amazon Managed Service for
Prometheus](#).

7 febbraio 2024

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
Aggiunto supporto per l'integrazione con Grafana gestito da Amazon	Il servizio gestito da Amazon per Prometheus aggiunge il supporto per l' integrazione con gli avvisi Grafana gestito da Amazon .	23 novembre 2022

[Sono state aggiunte nuove autorizzazioni a AmazonPrometheusConsoleFullAccess](#)

Sono state aggiunte nuove autorizzazioni alla politica [AmazonPrometheusConsoleFullAccess](#) gestita per supportare la registrazione degli eventi del gestore degli avvisi e dei rigelli nei registri. CloudWatch

24 ottobre 2022

[È stata aggiunta la soluzione di osservabilità Amazon EKS.](#)

Amazon Managed Service for Prometheus aggiunge una nuova soluzione utilizzando Observability Accelerator. AWS Per maggiori informazioni, consulta [Utilizzo di AWS Observability Accelerator.](#)

14 ottobre 2022

[È stato aggiunto il supporto per l'integrazione nel monitoraggio dei costi di Amazon EKS.](#)

Il servizio gestito da Amazon per Prometheus aggiunge il supporto per l'integrazione nel monitoraggio dei costi di Amazon EKS. Per ulteriori informazioni, consulta [Integrazione con il monitoraggio dei costi di Amazon EKS.](#)

22 settembre 2022

[È stato lanciato il supporto per i log di Alert Manager e Ruler in Amazon CloudWatch Logs.](#)

Amazon Managed Service for Prometheus lancia il supporto per i log di errore di Alert Manager e Ruler in Amazon Logs. CloudWatch Per ulteriori informazioni, consulta [Amazon CloudWatch Logs.](#)

1 settembre 2022

[È stato aggiunto il supporto personalizzato per la conservazione degli archivi.](#)

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. [Per ulteriori informazioni sulle quote nel servizio gestito da Amazon per Prometheus, consulta Quote del servizio.](#)

12 agosto 2022

[Aggiunte metriche di utilizzo ad Amazon CloudWatch.](#)

Amazon Managed Service for Prometheus aggiunge il supporto per l'invio di metriche di utilizzo ad Amazon CloudWatch. Per ulteriori informazioni, consulta i [CloudWatchparametri di Amazon.](#)

6 maggio 2022

[Aggiunta del supporto per la regione Europa \(Londra\).](#)

Aggiunto il supporto del servizio gestito da Amazon per Prometheus per la regione Europa (Londra).

4 maggio 2022

[Il servizio gestito da Amazon per Prometheus è disponibile a livello generale e aggiunge il supporto per le regole e alert manager.](#)

Il servizio gestito da Amazon per Prometheus è disponibile a livello generale. Supporta anche regole e alert manager. Per ulteriori informazioni, consulta [Regole di registrazione e regole di avviso](#) e [Alert manager e templating.](#)

29 settembre 2021

<u>Aggiunto il supporto di tag.</u>	Il servizio gestito da Amazon per Prometheus supporta il tag delle aree di lavoro del servizio gestito da Amazon per Prometheus.	7 settembre 2021
<u>Le quote delle serie attive e del tasso di importazione sono aumentate.</u>	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
<u>Rilascio anteprima del servizio gestito da Amazon per Prometheus.</u>	Viene rilasciata l'anteprima del servizio gestito da Amazon per Prometheus.	15 dicembre 2020

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