aws

Guida per l'utente

AWS Health

AWS Health: Guida per l'utente

Table of Contents

Che cos'è AWS Health? 1
Concetti per AWS Health 2
AWS Health evento 2
Evento specifico dell'account 3
Evento pubblico 3
AWS Health Dashboard 3
AWS Health Dashboard: stato del servizio 4
Codice del tipo di evento 4
Categorie di tipi di evento 4
Stato dell'evento 6
Entità interessate 6
AWS Health eventi su Amazon EventBridge 6
AWS Health API 7
Visualizzazione organizzativa 7
Notifiche all'utente AWS 7
Nozioni di base 8
Configurazione 8
Registrati per un Account AWS 9
Crea un utente con accesso amministrativo 9
Visualizza gli eventi dell'account nella AWS Health Dashboard 10
Problemi aperti e recenti 11
Modifiche pianificate 12
Altre notifiche 13
Log degli eventi 13
Dettagli dell'evento 14
Tipi di eventi 16
Visualizzazione del calendario 16
Visualizzazione delle risorse interessate 17
Impostazioni del fuso orario 19
Lo stato di salute della tua organizzazione 19
Avvisi per eventi AWS Health 20
Configurazione di Amazon EventBridge 20
Gestisci le notifiche in Notifiche all'utente AWS 21
Configura il tuo abbonamento alle notifiche AWS gestite per gli eventi AWS Health 22

AWS Domande frequenti sulle notifiche gestite 23
AWS Health Cruscotto 25
Eventi pianificati del ciclo di vita per AWS Health 28
Cosa sono gli eventi pianificati del ciclo di vita? 28
Cosa devo aspettarmi quando ricevo una notifica relativa a un evento relativo al ciclo di vita pianificato? 29
Modello di responsabilità condivisa per la resilienza 32
Accesso agli eventi pianificati del ciclo di vita 32
Integrazione con altri sistemi tramite l'API AWS Health 33
Firma AWS Health delle richieste API 33
Scelta degli endpoint per le richieste AWS Health API 34
Demo: recupero programmatico dei dati degli ultimi sette giorni degli eventi 36
Demo: recupero dei dati degli ultimi sette giorni degli AWS Health eventi tramite Java 36
Demo: recupero dei dati degli ultimi sette giorni degli AWS Health eventi utilizzando Python 39
Tutorial: Utilizzo dell' AWS Health API con esempi in Java 42
Fase 1: inizializzare le credenziali 42
Fase 2: inizializzazione di un client API AWS Health 43
Fase 3: Utilizza le operazioni AWS Health API per ottenere informazioni sugli eventi 43
Sicurezza 47
Protezione dei dati 48
Crittografia dei dati 49
Gestione dell'identità e degli accessi 49
Destinatari 50
Autenticazione con identità 50
Gestione dell'accesso con policy 54
Come AWS Health funziona con IAM 57
Esempi di policy basate su identità 62
Risoluzione dei problemi 75
Uso di ruoli collegati ai servizi 78
AWS politiche gestite per AWS Health 79
Registrazione e monitoraggio AWS Health 85
Convalida della conformità 86
Resilienza 87
Sicurezza dell'infrastruttura 87
Analisi della configurazione e delle vulnerabilità 88

Best practice di sicurezza 88
Concedi AWS Health agli utenti le autorizzazioni minime possibili 88
Visualizza il AWS Health Dashboard 88
Integrazione AWS Health con Amazon Chime o Slack 88
Monitora gli AWS Health eventi 88
Aggregazione AWS Health di eventi 90
Prerequisiti 90
Abilitazione della visualizzazione organizzativa 91
Visualizzazione della vista organizzativa 95
Disabilitazione della visualizzazione organizzativa 100
Gestione delle viste degli amministratori delegati per un'organizzazione 101
Registrazione di un account amministratore delegato 102
Rimozione di un account amministratore delegato 103
Monitoraggio degli eventi Health con EventBridge 104
Creazione di EventBridge regole per la copertura Regione AWS 105
Monitoraggio degli eventi pubblici e specifici dell'account per AWS Health 106
Installazione di un ruolo collegato al servizio per utilizzare AWS Incident Detection and Response 108
Informazioni correlate 108
Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge 108
Aggregazione degli AWS Health eventi utilizzando la visualizzazione organizzativa e l'accesso amministrativo delegato 109
Integrazione del monitoraggio e delle notifiche degli AWS Health eventi con JIRA e ServiceNow 109
Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi 110
Creazione di una regola per più servizi e categorie 114
Configurazione di Amazon Q Developer nelle applicazioni di chat per inviare notifiche sugli eventi 116
Prerequisiti 116
Esecuzione automatica di operazioni sulle EC2 istanze in risposta agli eventi 118
Prerequisiti 119
Crea una regola per EventBridge 123
Riferimento: Amazon EventBridge schema AWS Health degli eventi 126
AWS Health schema degli eventi 126
Public Health Event - Problema EC2 operativo di Amazon 139
AWS Health Evento specifico dell'account - Problema dell'API Elastic Load Balancing 140

AWS Health Evento specifico dell'account: prestazioni ridotte di Amazon EC2 Instance Store Drive 141
Monitoraggio AWS Health 143
Registrazione delle chiamate AWS Health API con AWS CloudTrail 143
AWS Health informazioni in CloudTrail 144
Esempio: AWS Health voci dei file di registro 145
Cronologia dei documenti 147
Aggiornamenti precedenti 155
..... clvi

Che cos'è AWS Health?

AWS Health offre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità delle tue Servizi AWS e dei tuoi account. È possibile utilizzare AWS Health gli eventi per scoprire in che modo le modifiche ai servizi e alle risorse potrebbero influire sulle applicazioni in esecuzione AWS. AWS Health fornisce informazioni pertinenti e tempestive per aiutarvi a gestire gli eventi in corso. AWS Health ti aiuta anche a conoscere e a prepararti per le attività pianificate. Il servizio fornisce avvisi e notifiche attivati da cambiamenti nello stato delle AWS risorse, in modo da ottenere visibilità quasi istantanea degli eventi e indicazioni per accelerare la risoluzione dei problemi.

Tutti i clienti possono utilizzare la AWS Health Dashboard AWS , basata sull' AWS Health API. La dashboard non richiede alcuna configurazione ed è pronta per l'uso per AWS gli utenti autenticati. Per altre caratteristiche salienti del servizio, consulta la AWS Health pagina dei dettagli della AWS Health dashboard Pagina dashboard.

AWS Health fornisce una console, denominata AWS Health Dashboard, a tutti i clienti. Per configurare il pannello di controllo non occorre scrivere codici o eseguire operazioni.

Per apprendere le nozioni di base AWS Health e i termini che incontrerai durante l'utilizzo del servizio, per comprendere le nozioni di base di AWS Health see. Concetti per AWS Health

> **Note**
>
> - La AWS Health Dashboard è disponibile per tutti AWS i clienti senza costi aggiuntivi.
> - Tutti AWS i clienti possono ricevere AWS Health eventi tramite EventBridge Amazon senza costi aggiuntivi.
> - Se disponi di un piano Business, Enterprise On-Ramp o Enterprise Support, puoi utilizzare l' AWS Health API per l'integrazione con sistemi interni e di terze parti. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Health.
> - Per ulteriori informazioni sui Supporto AWS piani disponibili, consulta. Supporto AWS

Concetti per AWS Health

Scopri AWS Health i concetti e scopri come utilizzare il servizio per mantenere l'integrità delle tue applicazioni, dei servizi e delle risorse del tuo Account AWS.

Argomenti

- AWS Health evento
- AWS Health Dashboard
- Codice del tipo di evento
- Categorie di tipi di evento
- Stato dell'evento
- Entità interessate
- AWS Health eventi su Amazon EventBridge
- AWS Health API
- Visualizzazione organizzativa
- Notifiche all'utente AWS

AWS Health evento

AWS Health gli eventi, noti anche come eventi Health, sono notifiche AWS Health inviate per conto di altri AWS servizi. Puoi utilizzare questi eventi per conoscere le modifiche imminenti o programmate che potrebbero influire sul tuo account. Ad esempio, AWS Health puoi inviare un evento se AWS Identity and Access Management (IAM) prevede di rendere obsoleta una policy gestita o AWS Config prevede di rendere obsoleta una regola gestita. AWS Health invia anche eventi in caso di problemi di disponibilità del servizio in un. Regione AWSÈ possibile esaminare la descrizione dell'evento per comprendere il problema, identificare le risorse interessate e intraprendere le azioni consigliate.

Esistono due tipi di eventi Health:

Indice

- Evento specifico dell'account
- Evento pubblico

Evento specifico dell'account

Gli eventi specifici dell'account riguardano l'utente Account AWS o un account dell'organizzazione. AWS Ad esempio, se c'è un problema con un tipo di istanza Amazon Elastic Compute Cloud (Amazon EC2) in una regione che utilizzi, AWS Health fornisce informazioni sull'evento e il nome delle risorse interessate.

Puoi trovare eventi specifici dell'account dalla AWS Health dashboard, dall'AWS Health API o utilizzare Amazon EventBridge o AWS User Notifications per ricevere notifiche.

Evento pubblico

Gli eventi pubblici sono eventi di servizio segnalati che non sono specifici di un account. Ad esempio, se si verifica un problema di servizio per Amazon Simple Storage Service (Amazon S3) nella regione Stati Uniti orientali (Ohio) AWS Health , fornisce informazioni sull'evento, anche se non utilizzi quel servizio o disponi di bucket S3 in quella regione. Ti consigliamo di esaminare le notifiche pubbliche prima di agire su di esse.

Puoi trovare gli eventi pubblici dalla tua AWS Health Dashboard e dalla AWS Health Dashboard — Service health.

Se hai un account, consultaGuida introduttiva alla AWS Health dashboard.

Se non disponi di un account, consulta AWS Health Cruscotto.

AWS Health Dashboard

Se ne hai una Account AWS, la tua AWS Health dashboard mostra sia gli eventi pubblici che gli eventi specifici dell'account.

Ti consigliamo di utilizzare la AWS Health dashboard per conoscere gli eventi che forniscono informazioni generali, come un imminente problema di manutenzione per un servizio in una regione. Puoi anche utilizzare la AWS Health Dashboard per conoscere gli eventi che potrebbero interessarti direttamente, come una risorsa obsoleta nel tuo account.

Puoi accedere alla Dashboard per AWS Management Console visualizzare la AWS Health dashboard da casa. https://health.aws.amazon.com/health/

Per ulteriori informazioni, consulta Guida introduttiva alla AWS Health dashboard.

AWS Health Dashboard: stato del servizio

Se non disponi di un account, puoi utilizzare la AWS Health Dashboard — Service health at https://health.aws.amazon.com/health/status per visualizzare gli eventi pubblici. Gli eventi pubblici sono problemi di servizio segnalati AWS che forniscono informazioni sulla disponibilità del servizio. Questo sito Web mostra solo eventi pubblici, che non sono specifici di alcun account. Non è necessario accedere o disporre di un account per visualizzare questa pagina.

Per ulteriori informazioni, consulta AWS Health Cruscotto.

Codice del tipo di evento

I codici dei tipi di evento mostrati in un evento Health includono il servizio interessato e il tipo di evento. Ad esempio, se ricevi un evento Health con il codice del tipo di `AWS_EC2_SYSTEM_MAINTENANCE_EVENT` evento, significa che il servizio sta pianificando un evento di manutenzione che potrebbe interessarti. Utilizza queste informazioni per pianificare in anticipo o intraprendere azioni per il tuo account.

Categorie di tipi di evento

A tutti gli eventi Health è associata una categoria di tipo di evento. Per alcuni eventi, la categoria del tipo di evento potrebbe apparire nel codice del tipo di evento, ad esempio nel `AWS_RDS_MAINTENANCE_SCHEDULED` codice. In questo esempio, la categoria è pianificata. È possibile utilizzare queste informazioni per comprendere le categorie di eventi a un livello elevato.

È consigliabile monitorare tutte le categorie di tipi di eventi. Tieni presente che ogni categoria viene visualizzata per diversi tipi di eventi. Puoi anche utilizzare l'operazione DescribeEventTypesAPI per trovare la categoria del tipo di evento.

Notifica dell'account

> Questi eventi forniscono informazioni sull'amministrazione o sulla sicurezza degli account e dei servizi. Questi eventi potrebbero essere informativi o richiedere un intervento urgente da parte tua. Ti consigliamo di prestare attenzione a questi tipi di eventi e di esaminare tutte le azioni consigliate.
>
> Di seguito sono riportati alcuni esempi di codici di tipo di evento per le notifiche degli account:

- `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`— Hai un bucket Amazon S3 che potrebbe consentire l'accesso pubblico.
- `AWS_BILLING_SUSPENSION_NOTICE`— Il tuo account presenta addebiti in sospeso ed è stato sospeso oppure lo hai disattivato.
- `AWS_WORKSPACES_OPERATIONAL_NOTIFICATION`— C'è un problema di servizio per Amazon WorkSpaces.

Problema

Si tratta di eventi imprevisti che influiscono su AWS servizi o risorse. Gli eventi più comuni di questa categoria includono comunicazioni relative a problemi operativi che causano il degrado del servizio o problemi localizzati a livello di risorse di cui l'utente deve essere informato.

Di seguito sono riportati alcuni esempi di codici relativi ai tipi di evento relativi ai problemi:

- `AWS_EC2_OPERATIONAL_ISSUE`— Un problema operativo di un servizio, ad esempio ritardi nell'utilizzo di un servizio.
- `AWS_EC2_API_ISSUE`— Un problema operativo per l'API di un servizio, ad esempio una maggiore latenza per un'operazione API.
- `AWS_EBS_VOLUME_ATTACHMENT_ISSUE`— Un problema localizzato a livello di risorsa che potrebbe influire sulle tue risorse Amazon Elastic Block Store (Amazon EBS).
- `AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT`— Questo evento significa che il tuo account potrebbe essere sospeso se non agisci.

Modifica programmata

Questi eventi forniscono informazioni sulle modifiche imminenti ai servizi e alle risorse. Questi eventi includono eventi pianificati del ciclo di vita come end-of-support notifiche e aggiornamenti automatici per diverse versioni. Alcuni eventi potrebbero consigliarti di intervenire per evitare interruzioni del servizio, mentre altri si verificheranno automaticamente senza alcuna azione da parte dell'utente. Durante l'attività di modifica pianificata, la tua risorsa potrebbe essere temporaneamente non disponibile. Tutti gli eventi in questa categoria sono eventi specifici dell'account.

Di seguito sono riportati alcuni esempi di codici di tipo di evento per le modifiche pianificate:

- `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`— Un' EC2 istanza Amazon richiede un riavvio.
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— SageMaker L'intelligenza artificiale richiede un evento di manutenzione, ad esempio la risoluzione di un problema di servizio.

- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— Amazon RDS sta pianificando un evento del ciclo di vita pianificato, ad esempio un end-of-support evento per una delle sue versioni, che richiede l'intervento del cliente.

> **Tip**
>
> Se utilizzi l' AWS Health API o il AWS Command Line Interface (AWS CLI) per restituire i dettagli dell'evento, l'`Event`oggetto contiene il `eventScopeCode` campo con il valore. `ACCOUNT_SPECIFIC` Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Health.

Stato dell'evento

Lo stato dell'evento indica se l'evento Health è aperto, chiuso o imminente. Puoi visualizzare gli eventi Health nella AWS Health Dashboard o nell' AWS Health API per un massimo di 90 giorni.

Entità interessate

Le entità interessate sono AWS risorse che potrebbero essere interessate dall'evento. Ad esempio, se ricevi un evento pianificato per la EC2 manutenzione di Amazon per un tipo specifico di istanza che stai utilizzando nel tuo account, puoi utilizzare l'evento Health per determinare l'ID delle istanze interessate. Utilizza queste informazioni per risolvere qualsiasi potenziale problema di servizio, ad esempio la creazione o l'obsolescenza di risorse.

AWS Health eventi su Amazon EventBridge

Puoi configurare EventBridge regole Amazon per i tuoi account per automatizzare le azioni dopo che l' AWS Health evento appropriato viene ricevuto da un account. Queste possono essere azioni generiche, come l'invio di tutti i messaggi relativi agli eventi del ciclo di vita pianificato a un'interfaccia di chat. Oppure possono essere azioni specifiche, come l'attivazione di un flusso di lavoro in uno strumento di gestione dei servizi IT.

Per ulteriori informazioni, consulta Monitoraggio degli eventi AWS Health con Amazon EventBridge.

AWS Health API

Puoi utilizzare l' AWS Health API per accedere in modo programmatico alle informazioni visualizzate nella AWS Health Dashboard, come le seguenti:

- Ottieni informazioni sugli eventi che potrebbero influire sui tuoi AWS servizi e risorse
- Abilita o disabilita la funzionalità di visualizzazione organizzativa per la tua AWS organizzazione
- Filtra i tuoi eventi per servizi specifici, categorie di tipi di evento e codici di tipo di evento

Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Health.

> **Note**
>
> È necessario disporre di un piano Business, Enterprise On-Ramp o Enterprise Support Supporto AWSper utilizzare l' AWS Health API. Se chiami l' AWS Health API da un account che non dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, ricevi un `SubscriptionRequiredException` errore.

Visualizzazione organizzativa

Puoi utilizzare questa funzione per aggregare tutti gli eventi sanitari AWS relativi agli account in un'unica visualizzazione AWS Organizations nella Dashboard. AWS Health Puoi quindi accedere all'account di gestione della tua organizzazione o utilizzare l' AWS Health API per visualizzare tutti gli eventi che potrebbero influire sui diversi account e risorse. È possibile abilitare questa funzionalità dalla AWS Health console o dall'API. Per ulteriori informazioni, consulta Aggregazione di AWS Health eventi tra account.

Notifiche all'utente AWS

AWS Health si integra per Notifiche all'utente AWSconsentirti di ricevere e controllare facilmente le notifiche sugli eventi che riguardano i tuoi Account AWS e i tuoi servizi. Notifiche all'utente offre notifiche gestite per AWS Health gli eventi per impostazione predefinita. Puoi configurare questi abbonamenti per controllare la frequenza con cui ricevi messaggi tramite l'aggregazione basata sul tempo, per quali tipi di AWS Health eventi ricevi notifiche e dove vengono recapitate le notifiche. Per iniziare, apri Notifiche all'utente in. AWS Management Console Per ulteriori informazioni, consulta Gestisci AWS Health le notifiche in Notifiche all'utente AWS

Guida introduttiva alla AWS Health dashboard

Puoi usare la AWS Health dashboard per conoscere AWS Health gli eventi. Questi eventi possono influire sul tuo Servizi AWS o Account AWS. Dopo aver effettuato l'accesso al tuo account, la AWS Health Dashboard mostra le informazioni nei seguenti modi:

- Eventi del tuo account: questa pagina mostra gli eventi specifici del tuo account. Puoi visualizzare le modifiche aperte, recenti e pianificate. Puoi anche visualizzare le notifiche e un registro degli eventi che mostra tutti gli eventi degli ultimi 90 giorni.
- Eventi della tua organizzazione: questa pagina mostra gli eventi specifici della tua organizzazione in AWS Organizations. Puoi visualizzare le modifiche aperte, recenti e pianificate per la tua organizzazione. Puoi anche visualizzare le notifiche e un registro degli eventi che mostra tutti gli eventi dell'organizzazione degli ultimi 90 giorni.

> **Note**
>
> Se non ne hai uno Account AWS, puoi utilizzarlo AWS Health Cruscotto per conoscere la disponibilità generale del servizio.
> Se disponi di un account, ti consigliamo di accedere alla AWS Health dashboard per ottenere informazioni più approfondite sugli eventi e sulle modifiche imminenti che potrebbero influire sui tuoi servizi e risorse.

Argomenti

- Configurazione del tuo AWS account
- Visualizzazione degli eventi del tuo account nella AWS Health Dashboard
- Configurazione di Amazon EventBridge
- Gestisci AWS Health le notifiche in Notifiche all'utente AWS

Configurazione del tuo AWS account

Prima di poter abilitare AWS Health, è necessario disporre di un Account AWS. Se non disponi di un AWS account, completa i seguenti passaggi per crearne uno.

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 AWSviene 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 Consolecome 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 .

Visualizzazione degli eventi del tuo account nella AWS Health Dashboard

Puoi accedere al tuo account per ricevere eventi e consigli personalizzati.

Per visualizzare gli eventi dell'account nella AWS Health dashboard

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Nel pannello di navigazione, per lo stato del tuo account, puoi scegliere le seguenti opzioni:
   a. Problemi aperti e recenti: visualizza gli eventi aperti e chiusi di recente.
   b. Modifiche pianificate: visualizza gli eventi imminenti che potrebbero influire sui tuoi servizi e risorse.
   c. Altre notifiche: visualizza tutte le altre notifiche e gli eventi in corso degli ultimi sette giorni che potrebbero influire sul tuo account.
   d. Registro eventi: visualizza tutti gli eventi degli ultimi 90 giorni.

Problemi aperti e recenti

Utilizza la scheda Problemi aperti e recenti per visualizzare tutti gli eventi in corso degli ultimi sette giorni che potrebbero influire sul tuo account.

Quando scegli un evento dalla dashboard, viene visualizzato il riquadro Dettagli con informazioni sull'evento e un elenco delle risorse interessate. Per ulteriori informazioni, consulta Dettagli dell'evento.

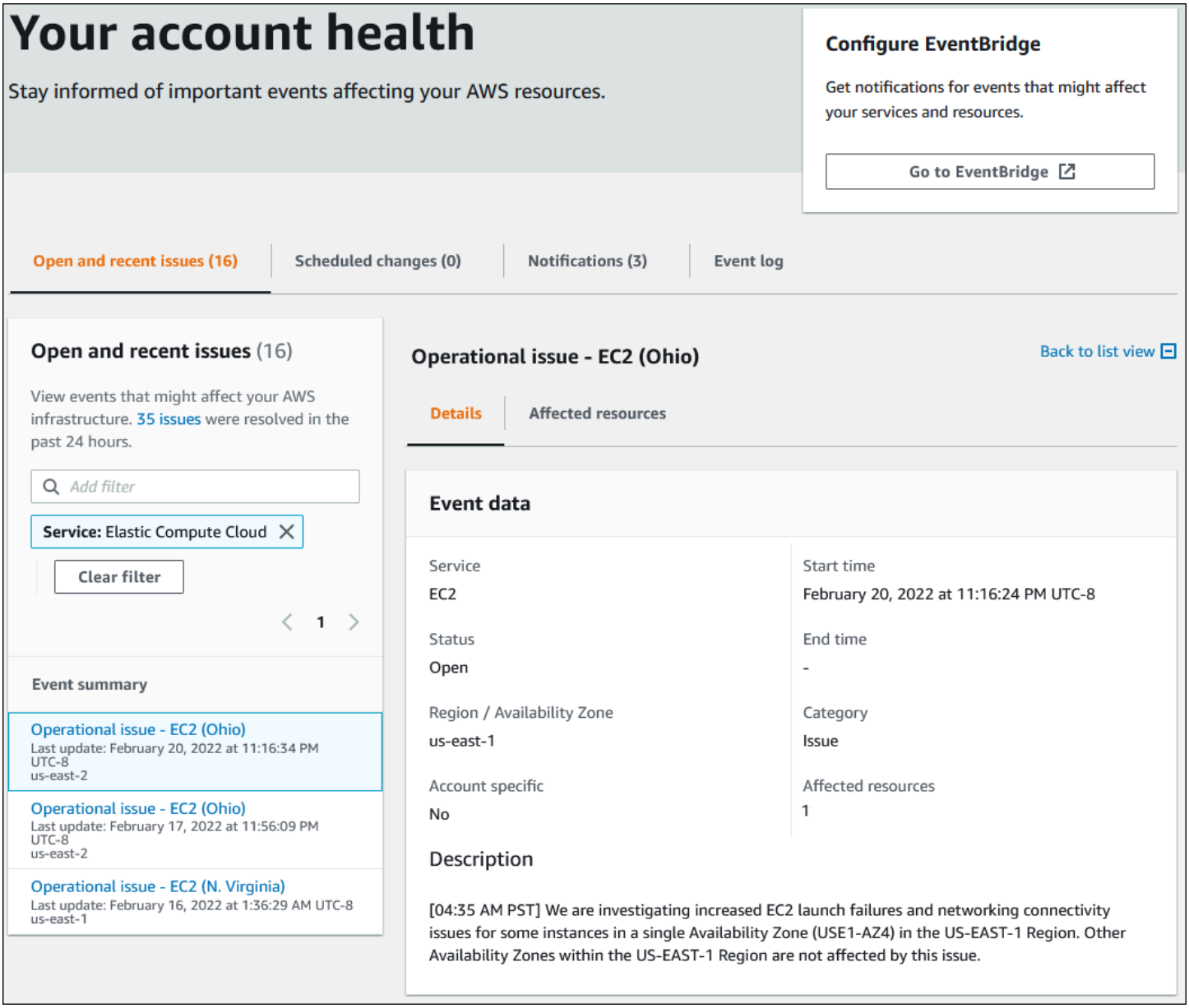
È possibile filtrare gli eventi visualizzati in qualsiasi scheda scegliendo le opzioni dall'elenco dei filtri. Ad esempio, puoi restringere i risultati per zona di disponibilità, regione, ora di fine dell'evento o ora dell'ultimo aggiornamento e così via. Servizio AWS

Per visualizzare tutti gli eventi, anziché quelli recenti visualizzati nella dashboard, scegli la Log degli eventischeda.

> **Note**
>
> Al momento, non puoi eliminare le notifiche per gli eventi che appaiono nella tua AWS Health dashboard. Dopo aver Servizio AWS risolto un evento, la notifica viene rimossa dalla visualizzazione della dashboard.

Example : problema operativo per Amazon Elastic Compute Cloud (Amazon EC2)

L'immagine seguente mostra un evento relativo a errori di avvio e problemi di connettività per le EC2 istanze Amazon.



Modifiche pianificate

Utilizza la scheda Modifiche pianificate per visualizzare gli eventi imminenti che potrebbero influire sul tuo account. Questi eventi possono includere attività di manutenzione programmate per i servizi ed eventi pianificati del ciclo di vita che richiedono un'azione per essere risolti. Per aiutarti a pianificare queste attività, è disponibile una visualizzazione del calendario in modo da poter mappare queste modifiche pianificate in un calendario mensile. I filtri sono disponibili. Per ulteriori informazioni sugli eventi pianificati del ciclo di vita, vedere. Eventi del ciclo di vita pianificati per AWS Health

Altre notifiche

Utilizza la scheda Notifiche per visualizzare tutte le altre notifiche e gli eventi in corso degli ultimi sette giorni che potrebbero influire sul tuo account. Ciò può includere eventi, come rotazioni dei certificati, notifiche di fatturazione e vulnerabilità di sicurezza.

Log degli eventi

Utilizza la scheda Registro eventi per visualizzare tutti gli eventi. AWS Health La tabella di registro include colonne aggiuntive che consentono di filtrare per stato e ora di inizio.

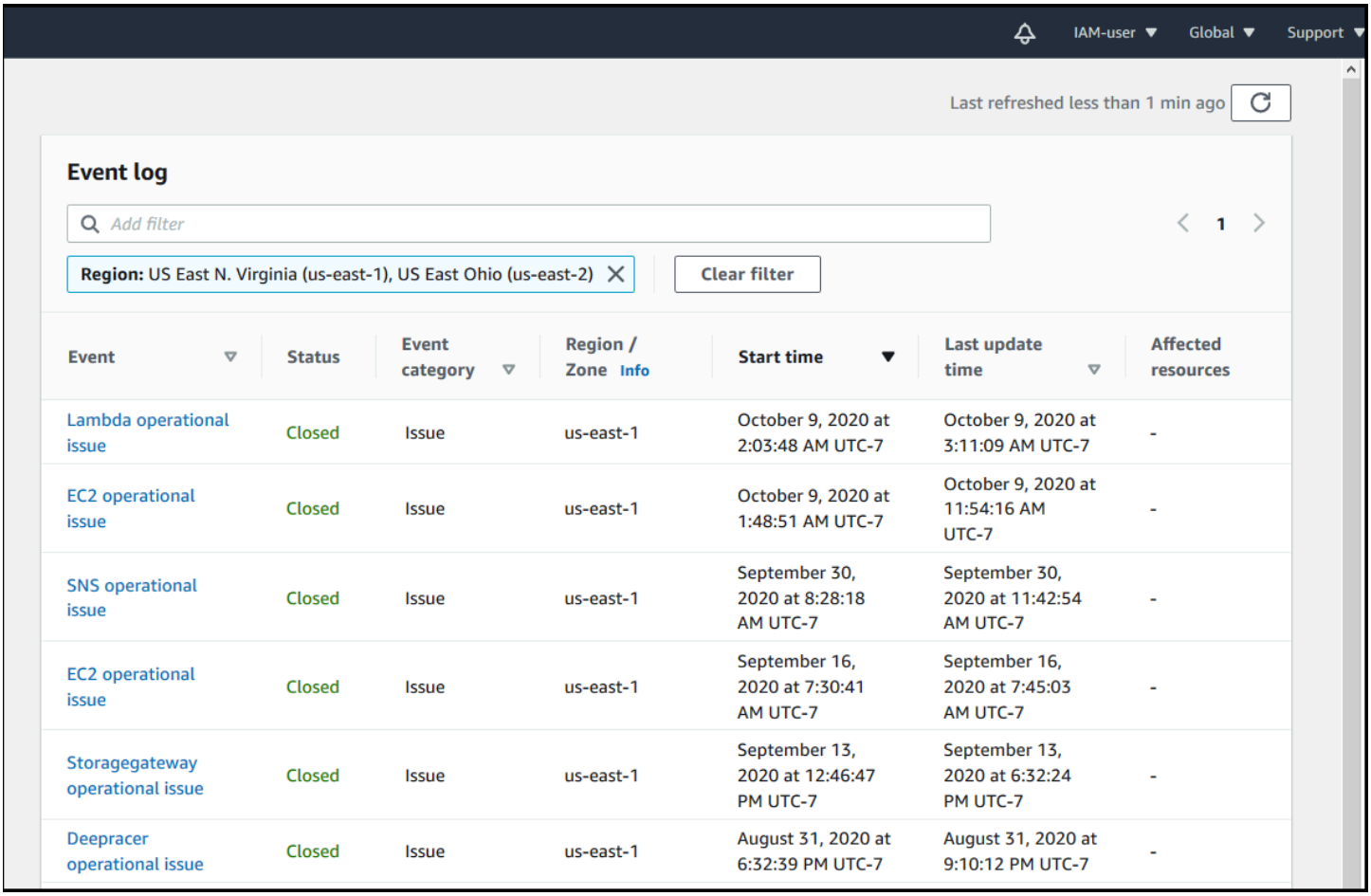
Quando si sceglie un evento nella tabella del registro eventi, viene visualizzato il riquadro Dettagli con informazioni sull'evento e l'elenco delle risorse interessate. Per ulteriori informazioni, consulta Dettagli dell'evento.

È possibile scegliere le seguenti opzioni di filtro per restringere i risultati:

- Zona di disponibilità
- Ora di fine
- Evento
- Evento ARN
- Categoria dell'evento
- Ora dell'ultimo aggiornamento
- Regione
- ID risorsa/ARN
- Servizio
- Ora di inizio
- Stato

Example : registro eventi

L'immagine seguente mostra gli eventi recenti per le regioni Stati Uniti orientali (Virginia settentrionale) e Stati Uniti orientali (Ohio).



Dettagli dell'evento

Quando scegli un evento, vengono visualizzate due schede relative all'evento. La scheda Dettagli mostra le seguenti informazioni:

- Servizio
- Stato
- Regione/ Zona di disponibilità
- Indipendentemente dal fatto che l'evento sia specifico dell'account
- Ora di inizio e fine
- Categoria
- Numero di risorse interessate
- Descrizione e cronologia degli aggiornamenti sull'evento

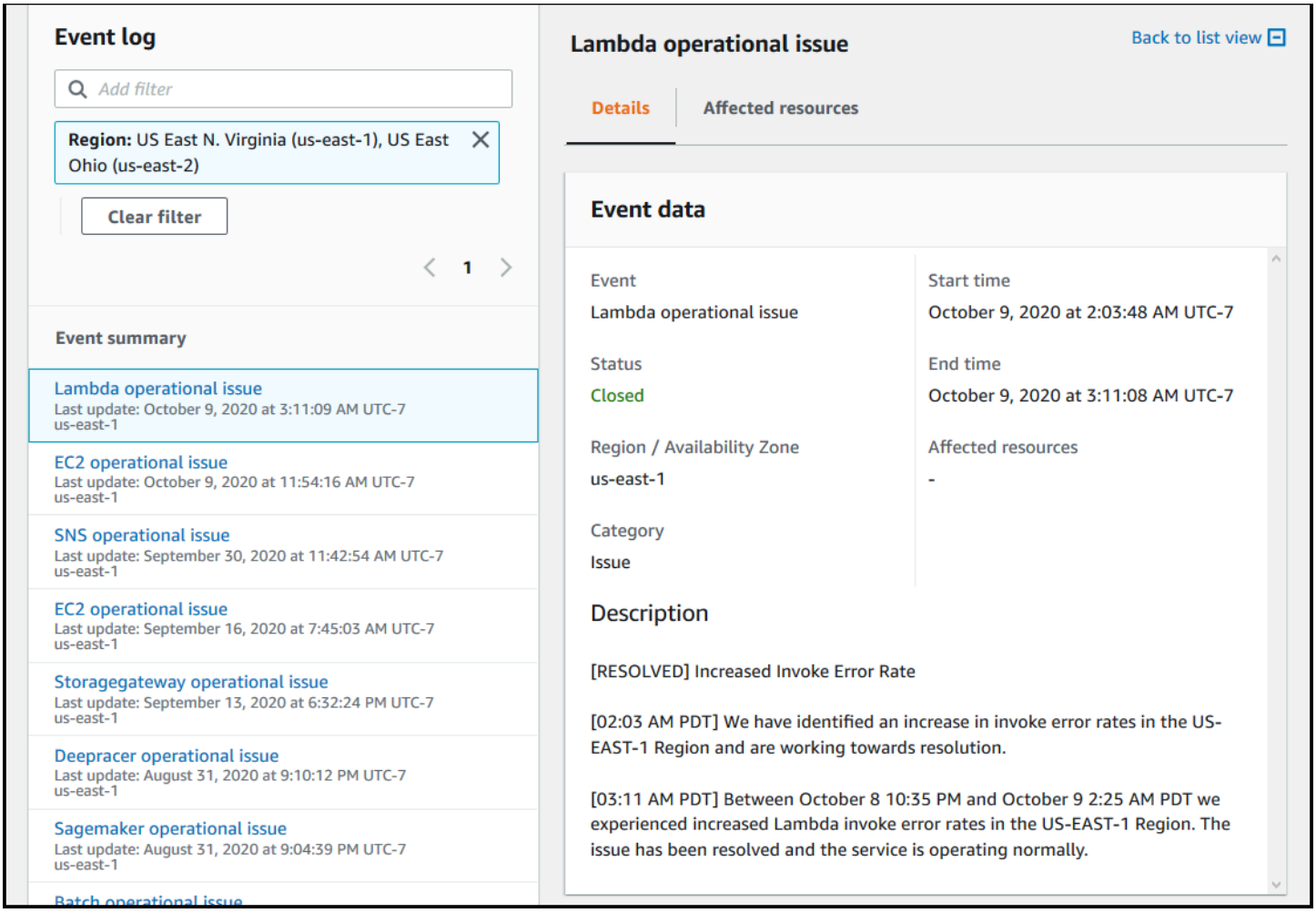
La scheda Risorse interessate mostra le seguenti informazioni su tutte AWS le risorse interessate dall'evento:

- L'ID della risorsa (ad esempio, un ID di volume Amazon EBS come`vol-a1b2c34f`) o Amazon Resource Name (ARN), se disponibile o pertinente.
- Per gli eventi pianificati del ciclo di vita, questo elenco delle risorse interessate contiene anche lo stato più recente delle risorse (In sospeso, Sconosciuto o Risolto). Questo elenco viene in genere aggiornato una volta ogni 24 ore, ma potrebbero essere necessarie fino a 72 ore per riflettere lo stato attuale.

Puoi filtrare gli elementi visualizzati nelle risorse. Puoi restringere i risultati in base all'ID della risorsa o all'ARN.

Example : AWS Health evento per AWS Lambda

La schermata seguente mostra un evento di esempio per Lambda.



Tipi di eventi

Esistono due tipi di AWS Health eventi:

- Gli eventi pubblici sono eventi di servizio che non sono specifici di un account. Ad esempio, se si verifica un problema con Amazon EC2 in un Regione AWS, AWS Health fornisce informazioni sull'evento, anche se non utilizzi servizi o risorse in quella regione.
- Gli eventi specifici dell'account sono specifici del tuo account o di un account della tua organizzazione. Ad esempio, se c'è un problema con un' EC2 istanza Amazon in un Regione AWS dispositivo che utilizzi, AWS Health fornisce informazioni sull'evento e l'elenco delle EC2 istanze Amazon interessate.

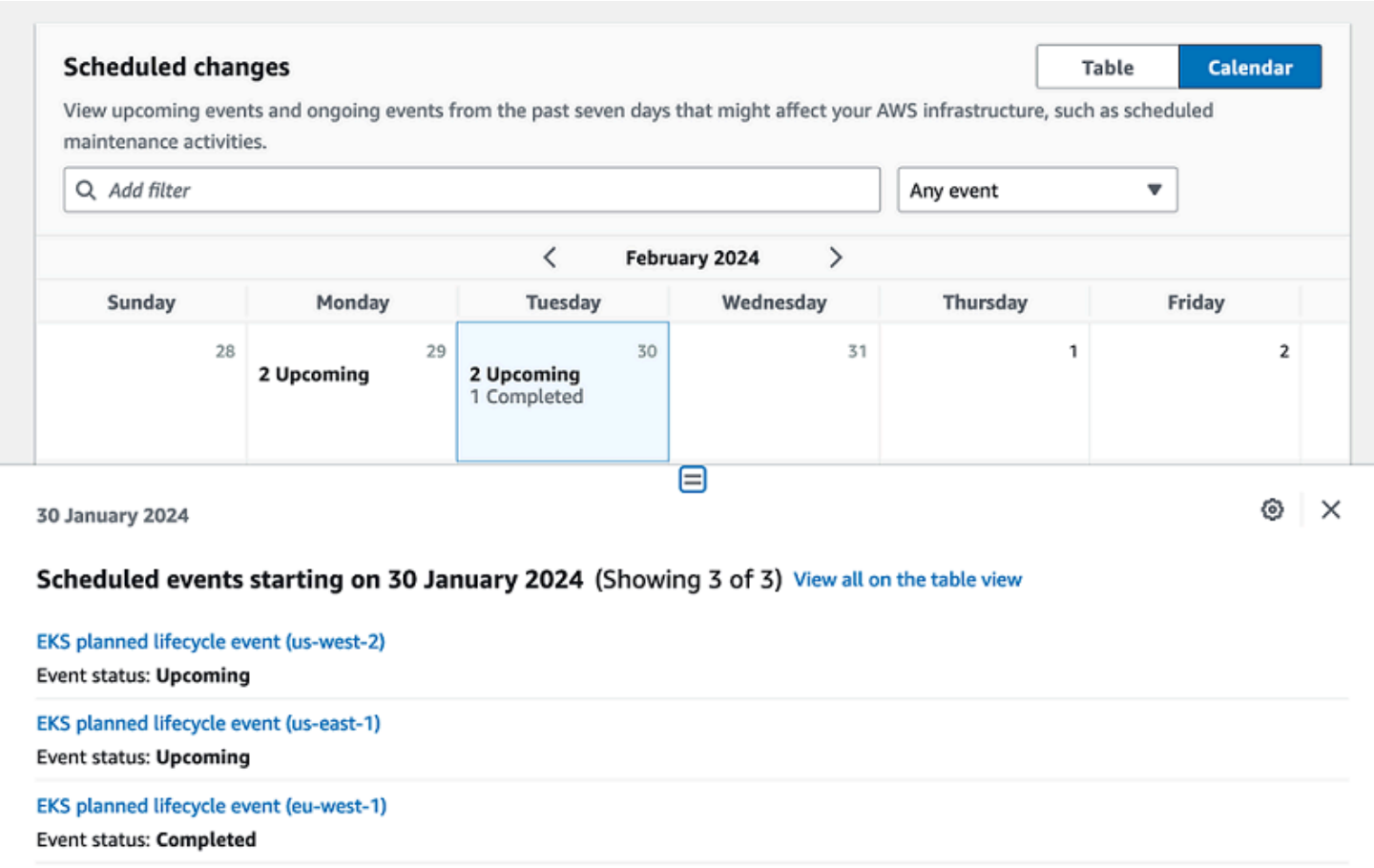
Puoi utilizzare le seguenti opzioni per identificare se un evento è pubblico o specifico dell'account:

- Nella AWS Health Dashboard, scegli la scheda Risorse interessate per un evento. Gli eventi con risorse sono specifici per il tuo account. Gli eventi senza risorse sono pubblici e non sono specifici per il tuo account. Per ulteriori informazioni, consulta Guida introduttiva alla AWS Health dashboard.
- Utilizza l' AWS Health API per restituire il `eventScopeCode` parametro. Gli eventi possono avere il valore `PUBLIC`, `ACCOUNT_SPECIFIC` o `NONE`. Per ulteriori informazioni, consulta l'DescribeEventDetailsoperazione nell'AWS Health API Reference.

Visualizzazione del calendario

La visualizzazione Calendario è disponibile nella scheda Modifiche pianificate per proiettare AWS Health gli eventi in un calendario mensile. Questa visualizzazione consente di visualizzare le modifiche pianificate fino a 3 mesi precedenti e fino a un anno nel futuro.

AWS Health gli eventi vengono visualizzati per data. Seleziona una data per visualizzare un pannello laterale che contiene ulteriori dettagli sull' AWS Health evento. Gli eventi imminenti e in corso vengono visualizzati in nero. Gli eventi completati vengono visualizzati in grigio. Se ci sono più di due eventi in una data, viene mostrato solo il numero di eventi neri e grigi. Seleziona una data per visualizzare un elenco di AWS Health eventi nel pannello laterale. È possibile selezionare un evento nel pannello laterale per visualizzare le informazioni sull'evento. Il pannello laterale contiene delle briciole di navigazione per passare a una visualizzazione precedente.



Visualizzazione delle risorse interessate

AWS Health gli eventi potrebbero specificare le risorse esatte interessate. È possibile visualizzare le risorse interessate nella scheda Risorse interessate dell' AWS Health evento. Per visualizzare lo stato, seleziona l' AWS Health evento. Lo stato viene visualizzato nella scheda delle risorse interessate nel pannello laterale. Per gli eventi pianificati del ciclo di vita, AWS Health gli eventi forniscono aggiornamenti giornalieri sullo stato delle risorse interessate.

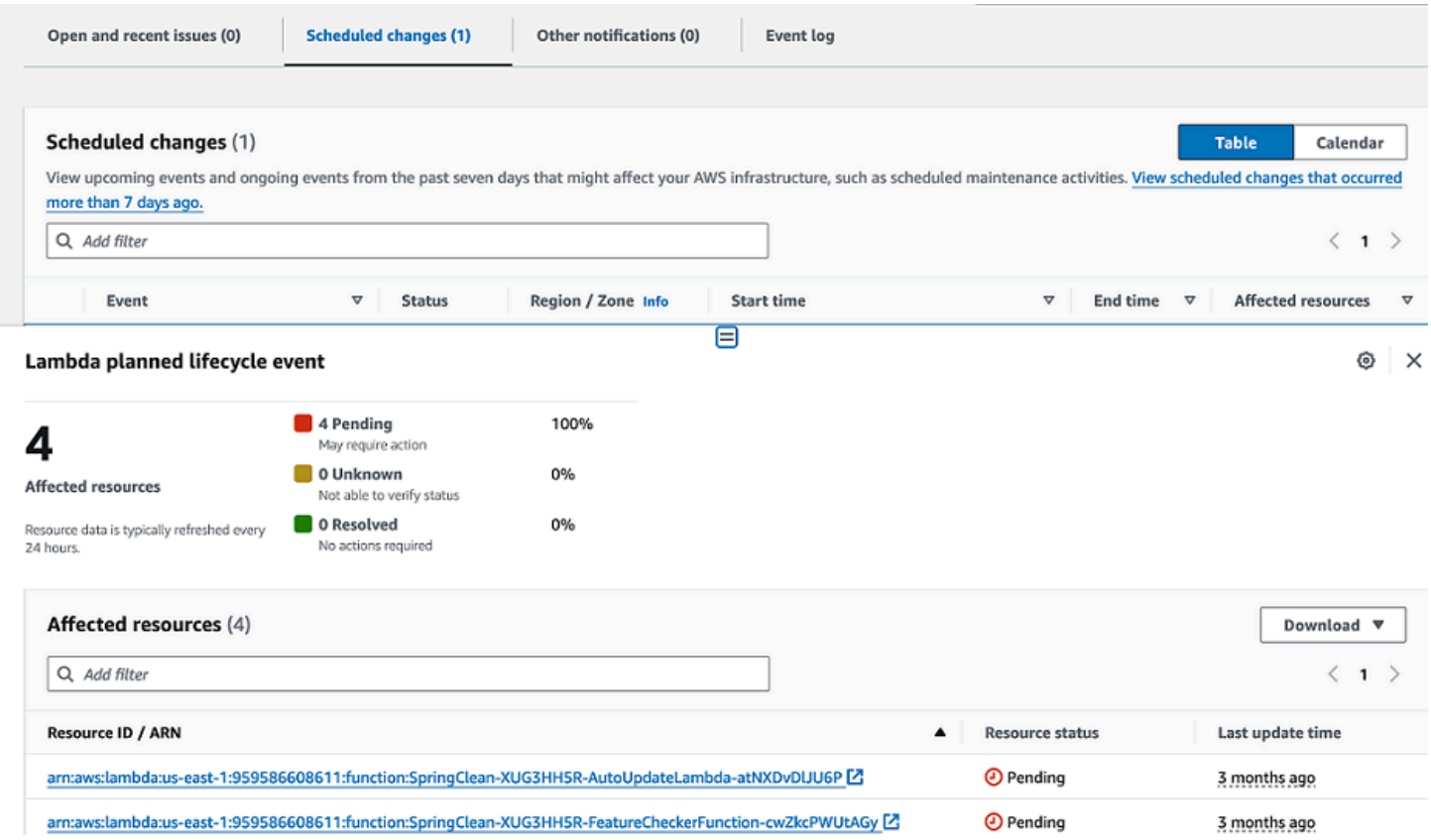
AWS Health Gli eventi a livello di account visualizzano un riepilogo dello stato delle risorse interessate nella parte superiore della scheda Risorse interessate. Un elenco delle risorse interessate viene visualizzato in una tabella insieme allo stato corrispondente. Gli eventi pianificati del ciclo di vita sono un esempio di tipi di eventi che utilizzano il campo dello stato delle risorse. Per ulteriori informazioni sugli eventi pianificati del ciclo di vita, consulta. Eventi del ciclo di vita pianificati per AWS Health

Quando si accede alla visualizzazione dell'organizzazione, AWS Health gli eventi mostrano un riepilogo dello stato di tutte le risorse interessate per tutti gli account inclusi. Dopo il riepilogo c'è

un elenco degli account interessati e il numero di risorse in sospeso per quell'account. Seleziona il numero di conto o il numero di risorse in sospeso per visualizzare il riepilogo della visualizzazione dell'account. Il riepilogo della visualizzazione dell'account contiene delle breadcrumb per tornare all'elenco organizzativo degli account interessati. Un riepilogo dello stato delle risorse interessate viene visualizzato nella parte superiore del pannello diviso.

È possibile scaricare l'elenco delle risorse interessate nella scheda Risorse interessate in formato CSV o JSON. Nella visualizzazione organizzativa, il file scaricato include tutte le risorse degli account elencati. Passa al livello di account nella visualizzazione organizzativa per includere solo le risorse relative a quell'account nel file scaricato. Ogni risorsa interessata nel file scaricato include l' Account AWS ID, l'eventARN, il nome dell'entità, l'entityARN, lo stato e l'ora dell'ultimo aggiornamento della risorsa. Se i filtri sono attivati, il file scaricato include solo i risultati filtrati.

Puoi scaricare solo un file alla volta. I file vengono scaricati automaticamente nella cartella di download predefinita del browser e hanno un nome file preimpostato basato sul titolo dell'evento Regione AWS, sulla data di inizio dell'evento e sulla data di download.



Impostazioni del fuso orario

Puoi visualizzare gli eventi nella AWS Health Dashboard nel tuo fuso orario locale o in UTC. Se modifichi il fuso orario nella AWS Health dashboard, tutti i timestamp nella dashboard e gli eventi pubblici vengono aggiornati in base al fuso orario specificato.

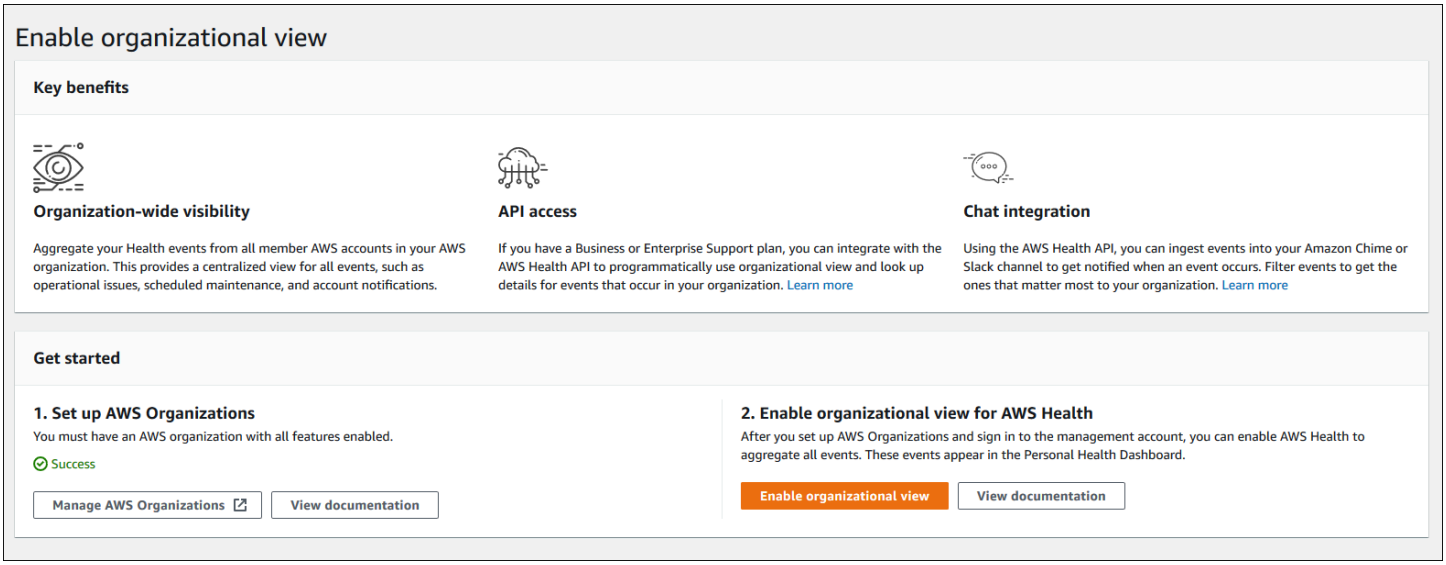
Per aggiornare le impostazioni del fuso orario

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Nella parte inferiore della pagina, scegli Preferenze sui cookie.
3. Seleziona Consentiti per i cookie funzionali. Quindi scegli Salva preferenze.
4. Nel riquadro di navigazione della AWS Health dashboard, scegli Impostazioni del fuso orario.
5. Seleziona un fuso orario per le sessioni della AWS Health Dashboard. Selezionare quindi Save changes (Salva modifiche).

Lo stato di salute della tua organizzazione

AWS Health si integra AWS Organizations in modo da poter visualizzare gli eventi per tutti gli account che fanno parte della tua organizzazione. Ciò fornisce una vista centralizzata per gli eventi che vengono visualizzati nell'organizzazione. È possibile utilizzare questi eventi per monitorare le modifiche apportate alle risorse, ai servizi e alle applicazioni.

Per ulteriori informazioni, consulta Aggregazione di AWS Health eventi tra account.



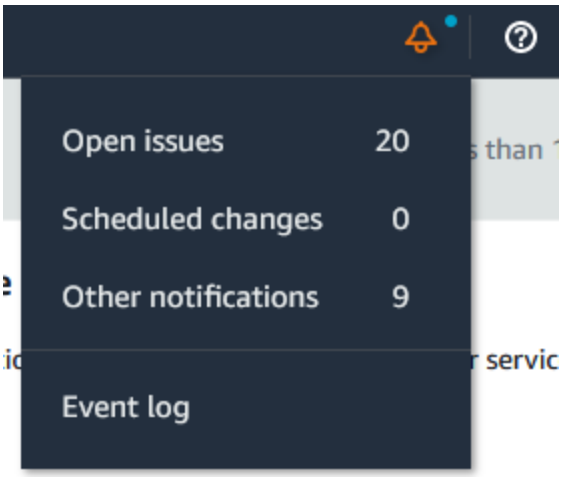
Avvisi per eventi AWS Health

La AWS Health dashboard presenta un'icona a forma di campana nella barra di navigazione della console con un menu di avviso. Questa funzione mostra il numero di AWS Health eventi recenti che appaiono sulla dashboard in ogni categoria. Questa icona a forma di campana appare su diverse AWS console, come quelle per Amazon EC2, Amazon Relational Database Service (Amazon RDS) AWS Identity and Access Management , (IAM) e. AWS Trusted Advisor

Scegli l'icona a forma di campana per vedere se gli eventi recenti influiscono sul tuo account. Puoi quindi scegliere un evento per accedere alla AWS Health dashboard per ulteriori informazioni.

Example : Eventi aperti

L'immagine seguente mostra gli eventi di apertura e notifica per un account.



Configurazione di Amazon EventBridge

Utilizzalo EventBridge per rilevare e reagire alle modifiche degli AWS Health eventi. Puoi monitorare AWS Health eventi specifici che si verificano nel tuo account e quindi impostare regole in modo che ti AWS Health avvisino, o che tu intervenga, quando gli eventi cambiano.

Da utilizzare EventBridge con AWS Health

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Per accedere alla EventBridge console e creare una regola, esegui una delle seguenti operazioni:
   - Dal pannello di navigazione, in Health Integrations, scegli Amazon EventBridge.

- In Configura EventBridge, scegli Vai a. EventBridge

3. Segui questa procedura per creare regole e monitorare gli eventi. Consultare Monitoraggio degli eventi AWS Health con Amazon EventBridge.

Gestisci AWS Health le notifiche in Notifiche all'utente AWS

AWS le notifiche gestite in ti Notifiche all'utente AWS consentono di ricevere e gestire notifiche sugli eventi che riguardano i tuoi Account AWS e i tuoi servizi. Quando utilizzi le notifiche AWS gestite in Notifiche all'utente AWS, puoi specificare quali categorie di AWS Health eventi ricevere, configurare la visualizzazione organizzativa per le e-mail e ricevere notifiche consolidate anziché più e-mail simili. Per informazioni su come abilitare questo servizio, consulta Attivazione o disattivazione delle notifiche AWS gestite per AWS Health in. Notifiche all'utente AWS

Puoi scegliere i seguenti canali aggiuntivi tramite Notifiche all'utente AWS cui ricevere i tuoi AWS Health eventi:

- E-mail
- Chat
- Notifiche push al AWS Console Mobile Application

Sebbene queste notifiche non siano così dettagliate come AWS Health gli strumenti diretti, forniscono un modo efficace per informare le parti interessate di problemi e modifiche.

> **Note**
>
> Per una visibilità completa dei dettagli AWS Health degli eventi, tra cui la risorsa interessata IDs, lo stato attuale (aperto o chiuso) e lo stato delle risorse, è consigliabile utilizzare uno dei seguenti AWS Health strumenti:
>
> - L' AWS Health API
> - La fonte aws.health in Amazon EventBridge
> - La AWS Health Dashboard
>
> Questi strumenti forniscono le informazioni più dettagliate e in tempo reale sugli eventi e le modifiche in corso che potrebbero influire sui carichi di lavoro.

Configura il tuo abbonamento alle notifiche AWS gestite per gli eventi AWS Health

Per configurare l'abbonamento alle notifiche AWS gestite, completa i seguenti passaggi:

1. Apri Notifiche all'utente in AWS Management Console.
2. Nel riquadro di navigazione, scegli Abbonamenti con notifiche AWS gestite.
3. Se non sei abilitato Notifiche all'utente AWS come mittente delle AWS Health notifiche, seleziona Abilita AWS Health notifiche. Ciò disabilita AWS Health e abilita le e-mail provenienti da. Notifiche all'utente Per ulteriori informazioni, consulta Attivazione o disattivazione delle notifiche AWS gestite per in AWS Health Notifiche all'utente AWS
4. Puoi gestire le notifiche AWS Health degli eventi per categoria. Per ulteriori informazioni, consulta Aggiungere e rimuovere i contatti dell'account per le notifiche AWS gestite in Notifiche all'utente AWS.

> **Note**
>
> AWS Health sta migrando il recapito delle e-mail alle notifiche AWS gestite in Notifiche all'utente AWS. Di seguito sono riportate alcune date chiave:
>
> - Fino al 14 settembre 2025: periodo di attivazione per l'utilizzo delle notifiche AWS gestite.
> - 15 settembre 2025: le notifiche AWS gestite sono abilitate per tutte le notifiche esistenti. Account AWS Per le nuove Account AWS notifiche gestite sono abilitate per impostazione predefinita. Puoi abilitare e disabilitare le notifiche gestite fino al 15 dicembre 2025.
> - 15 dicembre 2025: le notifiche AWS gestite sono abilitate per tutti gli account e non è più possibile disabilitarle.
>
> Non è richiesta alcuna azione da parte tua per continuare a ricevere notifiche relative AWS Health agli eventi. Quando le notifiche AWS gestite sono abilitate, verranno apportate alcune modifiche e miglioramenti. Per ulteriori informazioni, vedi Cosa cambia quando abilito le notifiche AWS gestite? nelAWS notifiche gestite nelle domande frequenti sulle notifiche AWS utente.

AWS notifiche gestite nelle domande frequenti sulle notifiche AWS utente

Cosa cambia quando abilito le notifiche AWS gestite?

Per impostazione predefinita, le e-mail relative alle notifiche gestite vengono inviate ai contatti dell'account esistenti (indirizzi e-mail root, operativi, di fatturazione e di sicurezza). Le e-mail che ricevi dalle notifiche AWS gestite provengono da `health@aws.com` invece di `no-reply-aws@amazon.com` e il formato delle e-mail cambia. Se in precedenza hai impostato regole e-mail per le AWS Health notifiche, ad esempio il routing di un'e-mail in base all'ID del mittente o lo scraping del contenuto dell'e-mail, devi aggiornare questa configurazione in modo che corrisponda al nuovo formato di e-mail. Se richiedi l'automazione tramite notifiche push, ti consigliamo di valutare AWS Health gli eventi inviati tramite Amazon EventBridge come alternativa alle notifiche gestite.

Come funziona l'aggregazione per le e-mail e come posso abilitare questa funzionalità?

AWS la notifica gestita aggrega AWS Health gli eventi che hanno un impatto su più account all'interno della stessa AWS Organizations organizzazione in un'unica notifica aggregata. È possibile visualizzare l'organizzazione aggregata nel centro notifiche dell'account di gestione. Le notifiche gestite inviano tramite e-mail la notifica aggregata ai contatti dell'account di gestione. Per ridurre le e-mail duplicate, le notifiche AWS gestite inviano una notifica quando i contatti dell'account vengono condivisi tra gli account di gestione e gli account dei membri.

Per abilitare l'aggregazione, è necessario aver AWS Organizations configurato e concesso un accesso affidabile tra l'account di gestione e il Notifiche all'utente AWS servizio.

Per ulteriori informazioni, consulta Aggregazione AWS gestita delle notifiche in. Notifiche all'utente AWS

Devo abilitare l'accesso AWS Organizations affidabile con Notifiche all'utente AWS per ricevere e-mail aggregate dalle notifiche AWS gestite?

Sì, AWS Organizations è richiesto un accesso affidabile con Notifiche all'utente AWS from.

Qual è la differenza tra consentire l'accesso affidabile tramite AWS Health e AWS Organizations con Notifiche all'utente AWS?

La fiducia organizzativa e i relativi privilegi di amministratore delegato vengono assegnati in base al servizio e fungono da barriera contro le autorizzazioni troppo estese. L'accesso affidabile AWS Health consente la AWS Health Dashboard visualizzazione organizzativa del AWS Health servizio e AWS Health degli eventi inviati tramite Amazon EventBridge. Accesso affidabile per Notifiche

all'utente AWS abilitare le notifiche aggregate all'interno Notifiche all'utente AWS delle AWS Health notifiche. Poiché l'accesso affidabile non è condiviso, la configurazione degli amministratori delegati deve essere aggiunta separatamente per ogni servizio.

Dove posso abilitare le notifiche gestite?

Abilita le notifiche gestite da AWS Management Console. Per ulteriori informazioni, vedere Abilitazione o disabilitazione delle notifiche AWS gestite per AWS Health in Notifiche all'utente AWS

Esiste un modo per conservare le e-mail in testo semplice per il mio caso d'uso specifico?

No. Le attuali AWS Health e-mail in testo semplice vengono disattivate al termine della migrazione. Se utilizzi regole e-mail per gestire flussi di lavoro diversi, ti consigliamo di valutare AWS Health gli eventi inviati tramite Amazon EventBridge come alternativa.

AWS Health Cruscotto

Puoi utilizzare la AWS Health Dashboard — Service health per visualizzare lo stato di salute di tutti Servizi AWS. Questa pagina mostra gli eventi di servizio segnalati per i servizi di tutti Regioni AWS. Non è necessario effettuare l'accesso o disporre di un account Account AWS per accedere alla pagina AWS Health Dashboard - Service Health.

> **Tip**
>
> Questo sito Web mostra solo eventi pubblici, che non sono specifici di un Account AWS. Se hai già un account, ti consigliamo di accedere per visualizzare la AWS Health dashboard e rimanere informato sugli eventi che possono influire sul tuo account e sui tuoi servizi. Per ulteriori informazioni, consulta Guida introduttiva alla AWS Health dashboard.

Per visualizzare la AWS Health Dashboard — Stato del servizio

1. Vai alla pagina https://health.aws.amazon.com/health/di stato.

   > **Note**
   >
   > Se hai già effettuato l'accesso alla tua pagina Account AWS, verrai reindirizzato alla pagina AWS Health Dashboard - Lo stato del tuo account.

2. In Integrità del servizio, scegli Problemi aperti e recenti per visualizzare gli eventi segnalati di recente. Puoi visualizzare le seguenti informazioni sull'evento:

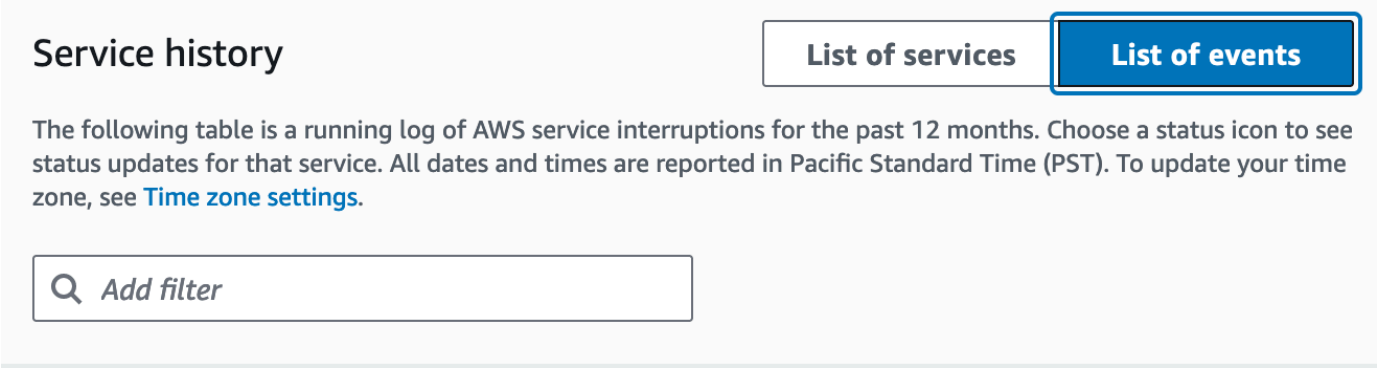
   - Il nome dell'evento e la regione interessata. Ad esempio, problema operativo: Amazon Elastic Compute Cloud (Virginia settentrionale)
   - Il nome del servizio
   - La gravità dell'evento, ad esempio Impatto o Degradato
   - Una cronologia degli aggiornamenti recenti dell'evento
   - Un elenco di Servizi AWS quelli interessati anche da questo evento

> **Note**
>
> Puoi visualizzare gli eventi nel tuo fuso orario locale o in UTC. Per ulteriori informazioni, consulta Impostazioni del fuso orario.

3. (Facoltativo) Accanto all'evento, scegli RSS per sottoscrivere un feed RSS per questo evento. Riceverai notifiche relative a questo servizio specifico nei tempi specificati. Regione AWS
4. Scegli Cronologia dei servizi per visualizzare la tabella Cronologia dei servizi. Questa tabella mostra tutte le Servizio AWS interruzioni degli ultimi 12 mesi.

> **Tip**
>
> Puoi filtrare per servizio Regione AWSe data.

5. Accanto a un evento di servizio in corso, scegli l'icona di stato ( ) per visualizzare ulteriori informazioni sull'evento.
6. (Facoltativo) Per visualizzarlo come elenco di eventi storici, scegliete il pulsante Elenco degli eventi. Scegli un evento nella colonna degli eventi per visualizzare ulteriori informazioni su quell'evento specifico nel pannello laterale pop-up.



> **Note**
>
> Se si seleziona un evento pubblico dopo settembre 2023, nell'URL del browser verrà inserito un link a tale evento pubblico AWS Health . Dopo aver selezionato questo link, accedi alla visualizzazione dell'elenco degli eventi con il pop-up dell'evento.

7. (Facoltativo) Scegli RSS per iscriverti a un feed RSS. Riceverai notifiche su questo servizio specifico nel modo specificato. Regione AWS
8. (Facoltativo) È possibile visualizzare gli eventi nel fuso orario locale o UTC. Per ulteriori informazioni, consulta Impostazioni del fuso orario.
9. (Facoltativo) Se hai un account, scegli Apri il tuo account Health per accedere. Dopo aver effettuato l'accesso, puoi visualizzare gli eventi specifici del tuo account. Per ulteriori informazioni, consulta Guida introduttiva alla AWS Health dashboard.

Eventi del ciclo di vita pianificati per AWS Health

Scopri gli eventi pianificati del ciclo di vita per. AWS Health

Argomenti

- Cosa sono gli eventi pianificati del ciclo di vita?
- Cosa devo aspettarmi quando ricevo una notifica relativa a un evento relativo al ciclo di vita pianificato?
- Modello di responsabilità condivisa per la resilienza
- Accesso agli eventi pianificati del ciclo di vita

Cosa sono gli eventi pianificati del ciclo di vita?

AWS Health comunica importanti cambiamenti che possono influire sulla disponibilità delle applicazioni. Nel modello di responsabilità AWS condivisa, AWS interviene per mantenere aggiornati e sicuri l'hardware e l'infrastruttura sottostanti che supportano le risorse. Tuttavia, alcune modifiche richiedono l'intervento o il coordinamento del cliente per evitare un impatto sulle applicazioni. AWS Health ti avvisa in anticipo di modifiche importanti come:

- Fine del supporto per il software open source: alcuni Servizi AWS eseguono versioni open source del software. Se la comunità open source interrompe il supporto per le versioni del software, AWS comunica all'utente quando è necessario intervenire per effettuare l'aggiornamento ed evitare ripercussioni sulle applicazioni.
  - Fine del supporto per la versione del motore Amazon RDS for MySQL
  - Fine del supporto per la versione Amazon EKS Kubernetes
- Modifiche che influiscono sulle risorse AWS di proprietà che potrebbero richiedere l'intervento dell'utente.
  - Scadenza dei certificati Amazon RDS Certificate Authority.

> **Note**
>
> Tutte le notifiche che soddisfano questi criteri verranno segnalate AWS Health come eventi del ciclo di vita pianificati.

- Ripartizione dinamica delle risorse e metadati migliorati: dal momento in cui si riceve la notifica fino alla durata dell'evento, le risorse interessate vengono associate all' AWS Health AWS Health evento come entità interessate con uno stato di entità specifico. Le risorse interessate sono specificate in formato ARN, ove applicabile. Se le risorse interessate richiedono l'intervento del cliente, vengono elencate con lo stato «IN SOSPESO». Se per le risorse interessate è stata eseguita l'azione richiesta o se le risorse sono state eliminate, lo stato viene aggiornato a «RISOLTO».

  > **Note**
  >
  > - Gli aggiornamenti dello stato delle risorse vengono eseguiti in modo asincrono e periodico e in rare occasioni possono avere un ritardo fino a 72 ore.
  > - Nelle eccezioni in cui non vengono forniti aggiornamenti dinamici, anziché alle risorse con lo stato «IN SOSPESO» o «RISOLTO», alle risorse non verrà assegnato alcuno stato.
  > - Gli aggiornamenti sullo stato delle risorse non sono supportati nelle regioni AWS GovCloud (US) e in Cina.

Cosa devo aspettarmi quando ricevo una notifica relativa a un evento relativo al ciclo di vita pianificato?

L' AWS Health esperienza per gli eventi pianificati del ciclo di vita aiuta i team a conoscere i cambiamenti imminenti del ciclo di vita e a monitorare il completamento delle azioni.

Tipo di categoria: modifica pianificata

Codice del tipo di evento: AWS_ {SERVICE} _PLANNED_LIFECYCLE_EVENT

Ora di inizio dell'evento: l'ora di inizio dell'evento è la data più vicina in cui le tue risorse sono interessate dalla modifica.

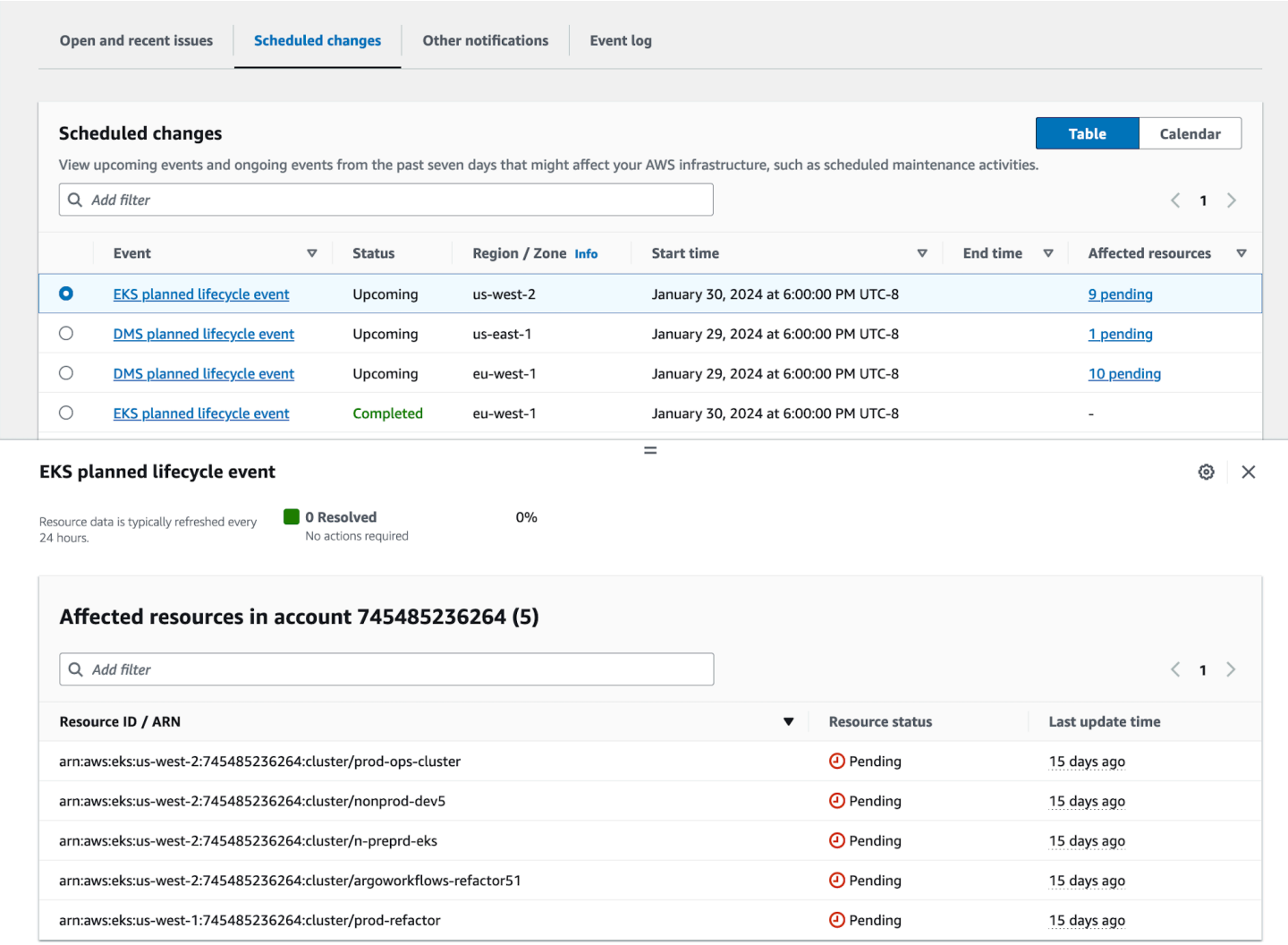
Ora di fine dell'evento: l'ora di fine dell'evento è la data in cui termina la modifica per tutte le AWS risorse. Tieni presente che l'ora di fine non è sempre specificata. È importante considerare l'ora di inizio come la data di modifica.

> **Note**
>
> Le organizzazioni possono aspettarsi di ricevere un singolo ARN per ogni evento del ciclo di vita pianificato, raggruppato per regione in cui sono presenti le risorse interessate. Tuttavia, potrebbero riceverne più di uno ARNs se l'organizzazione dispone di un gran numero di risorse o risorse interessate. Account AWS

Visibilità tempestiva degli eventi pianificati del ciclo di vita: gli eventi pianificati del ciclo di vita sono progettati per avere un lead time minimo di 180 giorni per i principali versions/changes and 90 days for minor versions/changes eventi, ove possibile.

Ripartizione dinamica delle risorse e metadati migliorati: dal momento in cui si riceve la notifica fino alla durata dell' AWS Health evento, le risorse interessate vengono associate all'evento come entità interessate con uno stato di entità specifico AWS Health . Le risorse interessate sono specificate in formato ARN, ove applicabile. Se le risorse interessate richiedono l'intervento del cliente, vengono elencate con lo stato «IN SOSPESO». Se per le risorse interessate è stata eseguita l'azione richiesta o se le risorse sono state eliminate, lo stato viene aggiornato a «RISOLTO».

> **Note**
>
> - AWS Health le notifiche forniscono aggiornamenti sullo stato nel tempo, ove possibile, ad eccezione delle regioni AWS GovCloud (US) e della Cina.
> - Gli aggiornamenti dello stato delle risorse vengono eseguiti in modo asincrono e periodico e in rare occasioni possono avere un ritardo fino a 72 ore.

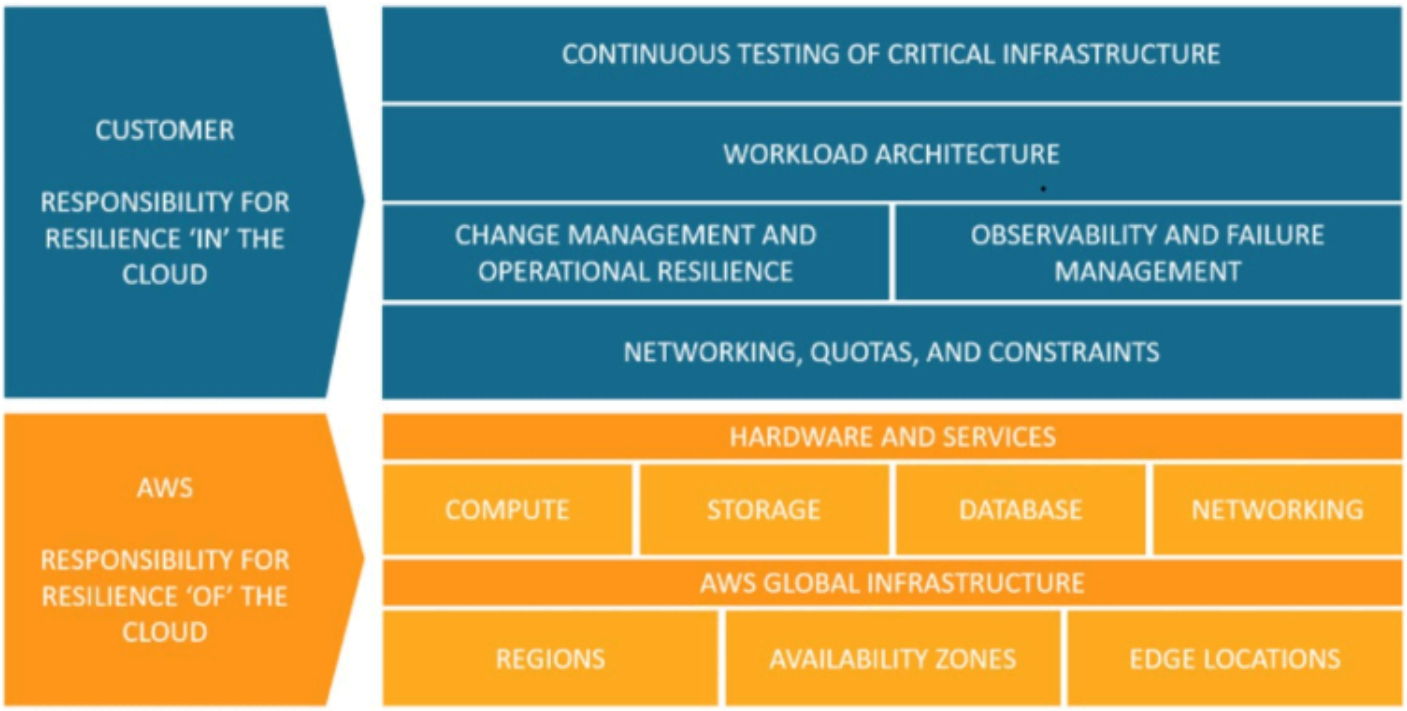


Una volta trascorsa la data pianificata dell'evento:

1. Se applicabile, il servizio potrebbe implementare la modifica descritta alla risorsa in qualsiasi momento dopo la data di inizio dell'evento.
2. Se risolvi tutte le risorse prima della data di fine del supporto, lo stato dell' AWS Health evento cambia`Closed`.
3. Se hai risorse in sospeso dopo la data di modifica che non sono state risolte, l' AWS Health evento rimane aperto per 4 anni dopo la data di inizio o di fine dell'evento (a seconda di quale data sia successiva). Trascorso questo periodo, l' AWS Health evento viene eliminato.

Modello di responsabilità condivisa per la resilienza

La sicurezza e la conformità sono responsabilità condivise tra AWS e il cliente. A seconda dei servizi implementati, questo modello condiviso può contribuire ad alleggerire l'onere operativo del cliente. Questo perché AWS gestisce, gestisce e controlla i componenti dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui opera il servizio. Il cliente si assume la responsabilità e la gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza) e degli altri software applicativi associati, oltre alla configurazione del firewall del gruppo di sicurezza fornito da. AWS Per ulteriori informazioni, consulta Modello di responsabilità condivisa.



Accesso agli eventi pianificati del ciclo di vita

È possibile accedere e monitorare gli eventi pianificati del ciclo di vita utilizzando diversi canali:

- Usa Amazon EventBridge
- Usa la AWS Health dashboard
  - Visualizzazione del calendario
  - Visualizzazione delle risorse interessate
- Usa l' AWS Health API

Integrazione AWS Health con altri sistemi tramite l'API AWS Health

AWS Health è un servizio RESTful Web che utilizza HTTPS come trasporto e JSON come formato di serializzazione dei messaggi. Il codice dell'applicazione può effettuare richieste direttamente all'API di AWS Health . Quando utilizzi direttamente l'API REST, devi scrivere il codice necessario per firmare e autenticare le tue richieste. Per ulteriori informazioni sulle AWS Health operazioni e sui parametri, consulta l'AWS Health API Reference.

> **Note**
>
> È necessario disporre di un piano Business, Enterprise On-Ramp o Enterprise Support Supporto AWSper utilizzare l' AWS Health API. Se chiami l' AWS Health API da un AWS account che non dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, ricevi un `SubscriptionRequiredException` errore.

Puoi utilizzare il AWS SDKs per eseguire il wrapping delle chiamate API AWS Health REST, il che può semplificare lo sviluppo delle applicazioni. Specificate AWS le vostre credenziali e queste librerie si occuperanno dell'autenticazione e della richiesta di firma per voi.

AWS Health fornisce inoltre una AWS Health dashboard AWS Management Console che è possibile utilizzare per visualizzare e cercare eventi ed entità interessate. Per informazioni, consulta Guida introduttiva alla AWS Health dashboard.

Argomenti

- Firma AWS Health delle richieste API
- Scelta degli endpoint per le richieste AWS Health API
- Demo: recupero programmatico dei dati degli ultimi sette giorni degli eventi AWS Health
- Tutorial: Utilizzo dell' AWS Health API con esempi in Java

Firma AWS Health delle richieste API

Quando utilizzi AWS SDKs o the AWS Command Line Interface (AWS CLI) per effettuare richieste a AWS, questi strumenti firmano automaticamente le richieste per te con la chiave di accesso

specificata al momento della configurazione degli strumenti. Ad esempio, se utilizzate la AWS SDK per Java precedente demo dell'endpoint ad alta disponibilità, non è necessario firmare personalmente le richieste.

Esempi di codice Java

Per altri esempi su come utilizzare l' AWS Health API con AWS SDK per Java, consulta questo codice di esempio.

Quando effettui richieste, ti consigliamo vivamente di non utilizzare le credenziali del tuo account AWS root per l'accesso regolare a AWS Health. Puoi utilizzare le credenziali di un utente IAM. Per ulteriori informazioni, consulta Lock Away Your AWS Account Root User Account nella Guida per l'utente IAM.

Se non usi il AWS SDKs o il AWS CLI, devi firmare tu stesso le tue richieste. Ti consigliamo di utilizzare la versione 4 di AWS Signature. Per ulteriori informazioni, consulta Signing AWS API Requests in Riferimenti generali di AWS.

Scelta degli endpoint per le richieste AWS Health API

L' AWS Health API segue un'architettura applicativa multiregionale Architettura applicativa e dispone di due endpoint regionali in una configurazione attiva-passiva. Per supportare il failover DNS attivo-passivo, fornisce un unico endpoint globale. AWS Health È possibile eseguire una ricerca DNS sull'endpoint globale per determinare l'endpoint attivo e la regione di firma corrispondente. AWS In questo modo è possibile sapere quale endpoint utilizzare nel codice, in modo da ottenere le informazioni più recenti. AWS Health

Quando effettui una richiesta all'endpoint globale, devi specificare le tue credenziali di AWS accesso all'endpoint regionale a cui desideri rivolgerti e configurare la firma per la tua regione. In caso contrario, l'autenticazione potrebbe fallire. Per ulteriori informazioni, consulta Firma AWS Health delle richieste API.

Per le IPv6 sole richieste, consigliamo di eseguire una ricerca DNS sull'endpoint globale per determinare l'endpoint attivo Regione AWS e quindi di chiamare l'endpoint dual-stack IPv6 supportato per quella regione.

La tabella seguente rappresenta la configurazione predefinita.

Descrizione	Regione di firma	Endpoint	Protocollo
Attivo	us-east-1	health.us-east-1.amazonaws.com (IPv4solo -) health.us-east-1.api.aws (e supportato) IPv4 IPv6	HTTPS
Passivo	us-east-2	health.us-east-2.amazonaws.com (IPv4solo) health.us-east-2.api.aws (e supportato) IPv4 IPv6	HTTPS
Globale	us-east-1 **Note** Questa è la regione di firma dell'endpoint attualmente attivo.	global.health.amazonaws.com	HTTPS

Per determinare se un endpoint è l'endpoint attivo, esegui una ricerca DNS sull'endpoint globale CNAME, quindi estrai la regione dal nome risolto. AWS

Example : ricerca DNS sull'endpoint globale

Il comando restituisce quindi l'endpoint Region. Questo output indica per quale endpoint utilizzare. AWS Health

```
dig global.health.amazonaws.com | grep CNAME
```

```
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

> **Tip**
>
> Sia gli endpoint attivi che quelli passivi restituiscono AWS Health dati. Tuttavia, i AWS Health dati più recenti sono disponibili solo dall'endpoint attivo. I dati dell'endpoint passivo saranno alla fine coerenti con l'endpoint attivo. Ti consigliamo di riavviare qualsiasi flusso di lavoro quando l'endpoint attivo cambia.

Demo: recupero programmatico dei dati degli ultimi sette giorni degli eventi AWS Health

Nei seguenti esempi di codice, AWS Health utilizza una ricerca DNS sull'endpoint globale per determinare l'endpoint regionale attivo e la regione di firma. AWS Health utilizza queste informazioni per recuperare un rapporto dei dati sugli eventi degli ultimi sette giorni. Il codice riavvia il flusso di lavoro se l'endpoint attivo cambia.

Argomenti

- Demo: recupero dei dati degli ultimi sette giorni degli AWS Health eventi tramite Java
- Demo: recupero dei dati degli ultimi sette giorni degli AWS Health eventi utilizzando Python

Demo: recupero dei dati degli ultimi sette giorni degli AWS Health eventi tramite Java

Prerequisito

È necessario installare Gradle.

Per usare l'esempio Java

1. Scarica la demo degli endpoint AWS Health ad alta disponibilità da GitHub.
2. Vai alla `high-availability-endpoint/java` directory del progetto dimostrativo.
3. In una finestra della riga di comando, immettete il seguente comando.

```
gradle build
```

4. Immettete i seguenti comandi per specificare le vostre AWS credenziali.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. Immettete il seguente comando per eseguire la demo.

```
gradle run
```

Example : output AWS Health dell'evento

L'esempio di codice restituisce l' AWS Health evento recente degli ultimi sette giorni nel tuo AWS account. Nell'esempio seguente, l'output include un AWS Health evento per il AWS Config servizio.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
AWS Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
 (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
 Autoscaling.
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
 Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
 direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a
 resource (A) and another resource (B), and is typically derived from the Describe
 API response of resource (A).
An indirect relationship, on the other hand, is a relationship that AWS Config
 infers (B->A), in order to create a bidirectional relationship.
```

```
For example, EC2 instance -> Security Group is a direct relationship, since
 security groups are returned as part of the describe API response for an EC2
 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances
 are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained
 within a
Configuration Item while reducing AWS Config costs related to relationship
 changes.
This is especially useful in case of ephemeral workloads where there is a high
 volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,
 AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,
 AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the
 corresponding search, and returns resource configurations matching the properties.
 You can use this API to retrieve the same relationship information.
```

```
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'

If you have any questions regarding this deprecation plan, please contact Supporto
 AWS [1]. Additional sample queries to retrieve the relationship information for
 the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Risorse Java

- Per ulteriori informazioni, consulta l'interfaccia HealthClient nell'AWS SDK per Java API Reference e il codice sorgente.
- Per ulteriori informazioni sulla libreria utilizzata in questa demo per le ricerche DNS, consulta dnsjava in. GitHub

Demo: recupero dei dati degli ultimi sette giorni degli AWS Health eventi utilizzando Python

Prerequisito

È necessario installare Python 3.

Per usare l'esempio Python

1. Scarica la demo degli endpoint AWS Health ad alta disponibilità da. GitHub
2. Vai alla `high-availability-endpoint/python` directory del progetto dimostrativo.
3. In una finestra della riga di comando, inserisci i seguenti comandi.

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> Per Python 3.3 e versioni successive, puoi usare il `venv` modulo integrato per creare l'ambiente virtuale, invece di installarlo. `virtualenv` Per ulteriori informazioni, vedere venv - Creazione di ambienti virtuali sul sito Web Python.
>
> ```
> python3 -m venv v-aws-health-env
> ```

4. Immettere il seguente comando per attivare l'ambiente virtuale.

```
source v-aws-health-env/bin/activate
```

5. Immettere il seguente comando per installare le dipendenze.

```
pip install -r requirements.txt
```

6. Immettete i seguenti comandi per specificare le vostre AWS credenziali.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. Immettete il seguente comando per eseguire la demo.

```
python3 main.py
```

Example : output AWS Health dell'evento

L'esempio di codice restituisce l' AWS Health evento recente degli ultimi sette giorni nel tuo AWS account. L'output seguente restituisce un AWS Health evento per una notifica AWS di sicurezza.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
```

```
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
 description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
 an interruption in service, we encourage you to act now, by ensuring that you
 connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
 March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
 where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
 If you need further guidance or assistance, please contact Supporto AWS [2] or
 your Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS Developer Tools on
 your clients,
you can find information on how to properly configure your client's TLS versions
 by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS services also offer FIPS 140-2 endpoints [9] for customers that require use
 of FIPS validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/
security/tag/tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
```

```
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/
blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. Quando hai finito, inserisci il seguente comando per disattivare la macchina virtuale.

```
deactivate
```

Risorse Python

- Per ulteriori informazioni su`Health. Client`, consulta il riferimento all'API AWS SDK for Python (Boto3).
- Per ulteriori informazioni sulla libreria utilizzata in questa demo per le ricerche DNS, consulta il toolkit dnspython e il codice sorgente su. GitHub

Tutorial: Utilizzo dell' AWS Health API con esempi in Java

I seguenti esempi di codice Java mostrano come inizializzare un AWS Health client e recuperare informazioni su eventi ed entità.

Fase 1: inizializzare le credenziali

Sono necessarie credenziali valide per comunicare con l'API. AWS Health Puoi utilizzare la key pair di qualsiasi utente IAM associato all' AWS account.

Crea e inizializza un'AWSCredentialsistanza:

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

Fase 2: inizializzazione di un client API AWS Health

Utilizza l'oggetto credenziali inizializzate nella fase precedente per creare un client AWS Health :

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

Fase 3: Utilizza le operazioni AWS Health API per ottenere informazioni sugli eventi

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
 awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;


DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);
```

```
// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();
```

```
request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

Sicurezza in AWS Health

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che 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 AWS Health, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

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

Argomenti

- Protezione dei dati in AWS Health
- Gestione delle identità e degli accessi per l' AWS Health
- Registrazione e monitoraggio AWS Health
- Convalida della conformità per AWS Health
- Resilienza in AWS Health
- Sicurezza dell'infrastruttura nell' AWS Health
- Analisi della configurazione e delle vulnerabilità in AWS Health
- Best practice relative alla sicurezza di AWS Health

Protezione dei dati in AWS Health

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

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- 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 AWS Health o Servizi AWS utilizzi 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.

Crittografia dei dati

Consulta le seguenti informazioni su come AWS Health crittografa i dati.

La crittografia dei dati si riferisce alla protezione dei dati durante il transito (mentre viaggiano dal servizio all' AWS account) e quando sono inattivi (mentre sono archiviati nei AWS servizi). Puoi proteggere i dati in transito utilizzando Transport Layer Security (TLS) o i dati inattivi utilizzando la crittografia lato client.

AWS Health non registra informazioni di identificazione personale (PII) come indirizzi e-mail o nomi dei clienti negli eventi.

Crittografia a riposo

Tutti i dati archiviati da AWS Health sono crittografati quando sono inattivi.

Crittografia in transito

Tutti i dati inviati e ricevuti AWS Health vengono crittografati durante il transito.

Gestione delle chiavi

AWS Health non supporta chiavi di crittografia gestite dal cliente per i dati crittografati nel AWS cloud.

Gestione delle identità e degli accessi per l' AWS Health

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

Argomenti

- Destinatari
- Autenticazione con identità

- Gestione dell'accesso con policy
- Come AWS Health funziona con IAM
- AWS Health esempi di politiche basate sull'identità
- Risoluzione dei problemi relativi AWS Health all'identità e all'accesso
- Utilizzo di ruoli collegati ai servizi per AWS Health
- AWS politiche gestite per AWS Health

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Health svolgi.

Utente del servizio: se utilizzi il AWS Health servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Health funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Health, consulta Risoluzione dei problemi relativi AWS Health all'identità e all'accesso.

Amministratore del servizio: se sei responsabile delle AWS Health risorse della tua azienda, probabilmente hai pieno accesso a AWS Health. È tuo compito determinare a quali AWS Health funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Health, consultaCome AWS Health funziona con IAM.

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

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.

AWS account 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.

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 an 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.

AWS Health supporta condizioni basate sulle risorse. Puoi specificare gli eventi AWS Health che gli utenti possono visualizzare. Ad esempio, potresti creare una policy che consenta a un utente IAM di accedere solo a EC2 eventi Amazon specifici in AWS Health Dashboard.

Per ulteriori informazioni, consulta Risorse.

Liste di controllo accessi

Le liste di controllo degli accessi (ACLs) controllano quali responsabili (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.

AWS Health non supporta ACLs.

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a

un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

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

Più tipi di policy

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

Come AWS Health funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Health, è necessario comprendere con quali funzionalità IAM è disponibile l'uso AWS Health. Per avere una visione di alto livello di come AWS Health e altri AWS servizi funzionano con IAM, consulta AWS Services That Work with IAM nella IAM User Guide.

Argomenti

- Policy AWS Health basate su identità
- Policy di AWS Health basate sulle risorse
- Autorizzazione basata su tag AWS Health
- AWS Health ruoli IAM

Policy AWS Health basate su identità

Con le policy basate su identità IAM, puoi specificare operazioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. AWS Health supporta operazioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

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

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

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

Le azioni politiche AWS Health utilizzano il seguente prefisso prima dell'azione:`health:`.
Ad esempio, per concedere a qualcuno il permesso di visualizzare informazioni dettagliate su eventi specifici DescribeEventDetailstramite l'operazione API, includi l'`heath:DescribeEventDetails`azione nella politica.

Le dichiarazioni politiche devono includere un `NotAction` elemento `Action` or. AWS Health definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più operazioni in una singola istruzione, separarle con una virgola come mostrato di seguito.

```
"Action": [
      "health:action1",
      "health:action2"
```

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

```
"Action": "health:Describe*"
```

Per visualizzare un elenco di AWS Health azioni, consulta Actions Defined by AWS Health nella IAM User Guide.

Risorse

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": "*"
```

Un AWS Health evento ha il seguente formato Amazon Resource Name (ARN).

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

Ad esempio, per specificare l'evento `EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456` nell'istruzione, utilizza il seguente ARN.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

Per specificare tutti AWS Health gli eventi per Amazon EC2 che appartengono a un account specifico, usa il carattere jolly (*).

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

Per ulteriori informazioni sul formato di ARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Alcune AWS Health azioni non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

AWS Health Le operazioni API possono coinvolgere più risorse. Ad esempio, l'DescribeEventsoperazione restituisce informazioni sugli eventi che soddisfano i criteri di filtro specificati. Ciò significa che un utente IAM deve disporre delle autorizzazioni per visualizzare questo evento.

Per specificare più risorse in una singola istruzione, separale ARNs con virgole.

```
"Resource": [
      "resource1",
      "resource2"
```

AWS Health supporta solo le autorizzazioni a livello di risorsa per gli eventi sanitari e solo per le operazioni e le API. DescribeAffectedEntitiesDescribeEventDetails Per ulteriori informazioni, consulta Condizioni basate su risorse e operazioni.

Per visualizzare un elenco dei tipi di AWS Health risorse e relativi ARNs, consulta Resources Defined by AWS Health nella IAM User Guide. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS Health.

Chiavi di condizione

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.

AWS Health definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella IAM User Guide.

Le operazioni DescribeAffectedEntitiese DescribeEventDetailsAPI supportano le chiavi `health:eventTypeCode` and `health:service` condition.

Per visualizzare un elenco di chiavi di AWS Health condizione, consulta Condition Keys for AWS Health nella IAM User Guide. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da AWS Health.

Esempi

Per visualizzare esempi di politiche AWS Health basate sull'identità, vedere. AWS Health esempi di politiche basate sull'identità

Policy di AWS Health basate sulle risorse

Le politiche basate sulle risorse sono documenti di policy JSON che specificano quali azioni uno specifico principale può eseguire sulla risorsa e in quali condizioni. AWS Health AWS Health supporta politiche di autorizzazione basate sulle risorse per gli eventi sanitari. Le policy basate su risorse consentono di concedere l'autorizzazione all'utilizzo ad altri account per ogni risorsa. Puoi anche utilizzare una politica basata sulle risorse per consentire a un servizio di accedere ai tuoi eventi. AWS AWS Health

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su 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 si trovano in AWS account diversi, è inoltre necessario concedere all'entità principale l'autorizzazione ad accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

AWS Health supporta solo politiche basate sulle risorse per le operazioni DescribeAffectedEntitiese DescribeEventDetailsle API. È possibile specificare queste azioni in una politica per definire quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire azioni sull'evento. AWS Health

Esempi

Per visualizzare esempi di politiche AWS Health basate sulle risorse, vedere. Condizioni basate su risorse e operazioni

Autorizzazione basata su tag AWS Health

AWS Health non supporta l'etichettatura delle risorse o il controllo dell'accesso in base ai tag.

AWS Health ruoli IAM

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con AWS Health

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo. GetFederationToken

AWS Health supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

AWS Health supporta ruoli collegati ai servizi con cui integrarsi. AWS Organizations Il ruolo collegato al servizio viene denominato `AWSServiceRoleForHealth_Organizations`. Al ruolo è associata la politica gestita da Health_ OrganizationsServiceRolePolicy AWS . La policy AWS gestita consente di accedere AWS Health agli eventi sanitari da altri AWS account dell'organizzazione.

È possibile utilizzare l'EnableHealthServiceAccessForOrganizationoperazione per creare il ruolo collegato al servizio nell'account. Tuttavia, se si desidera disabilitare questa funzionalità, è necessario prima richiamare l'DisableHealthServiceAccessForOrganizationoperazione. Puoi quindi eliminare il ruolo tramite la console IAM, l'API IAM o AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta Utilizzo di ruoli collegati a servizi nella Guida per l'utente di IAM .

Per ulteriori informazioni, consulta Aggregazione di AWS Health eventi tra account.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

AWS Health non supporta i ruoli di servizio.

AWS Health esempi di politiche basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse AWS Health . Inoltre, non possono eseguire attività utilizzando l'API AWS

Management Console AWS CLI, o. AWS Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

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

Argomenti

- Best practice delle policy
- Utilizzo della console di AWS Health
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Accesso a e all'API AWS Health DashboardAWS Health
- Condizioni basate su risorse e operazioni

Best practice delle policy

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

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate

utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

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

Utilizzo della console di AWS Health

Per accedere alla AWS Health console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Health risorse del tuo AWS account. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la AWS Health console, puoi allegare la seguente politica AWS gestita, AWSHealthFullAccess.

La `AWSHealthFullAccess` politica concede a un'entità l'accesso completo a quanto segue:

- Abilita o disabilita la funzionalità di visualizzazione AWS Health organizzativa per tutti gli account di un' AWS organizzazione
- AWS Health Dashboard Nella AWS Health console
- AWS Health Operazioni e notifiche delle API
- Visualizza le informazioni sugli account che fanno parte della tua AWS organizzazione

- Visualizza le unità organizzative (OU) dell'account di gestione

Example : AWSHealthFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

> **Note**
>
> È inoltre possibile utilizzare la politica `Health_OrganizationsServiceRolePolicy` AWS gestita, in modo da AWS Health visualizzare gli eventi di altri account dell'organizzazione. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

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 cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

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

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

Accesso a e all'API AWS Health DashboardAWS Health

AWS Health Dashboard È disponibile per tutti gli AWS account. L' AWS Health API è disponibile solo per gli account con un piano Business, Enterprise On-Ramp o Enterprise Support. Per ulteriori informazioni, consulta Supporto.

Puoi utilizzare IAM per creare entità (utenti, gruppi o ruoli) e quindi concedere a tali entità le autorizzazioni per accedere all'API AWS Health Dashboard e all'API. AWS Health

Per impostazione predefinita, gli utenti IAM non hanno accesso all'API AWS Health Dashboard o all' AWS Health API. Consenti agli utenti di accedere alle AWS Health informazioni del tuo account allegando le policy IAM a un singolo utente, a un gruppo di utenti o a un ruolo. Per ulteriori informazioni, consulta Identità (utenti, gruppi e ruoli) e la Panoramica delle policy IAM.

Dopo aver creato utenti IAM, puoi fornire loro una password. Quindi, possono accedere al tuo account e visualizzare le AWS Health informazioni utilizzando una pagina di accesso specifica per l'account. Per ulteriori informazioni, consulta Modalità di accesso degli utenti al tuo account.

> **Note**
>
> Un utente IAM con autorizzazioni di visualizzazione AWS Health Dashboard ha accesso in sola lettura alle informazioni sanitarie su tutti i AWS servizi dell'account, che possono includere, a titolo esemplificativo, AWS risorse IDs come l' EC2 istanza Amazon, gli indirizzi IP delle IDs EC2 istanze e le notifiche di sicurezza generali.
> Ad esempio, se una policy IAM concede l'accesso solo all'API AWS Health Dashboard e all' AWS Health API, l'utente o il ruolo a cui si applica la policy può accedere a tutte le

informazioni pubblicate sui AWS servizi e sulle risorse correlate, anche se altre policy IAM non consentono tale accesso.

Puoi usare due gruppi di APIs for AWS Health.

- Account individuali: puoi utilizzare operazioni come DescribeEventse DescribeEventDetailsper ottenere informazioni sugli AWS Health eventi relativi al tuo account.
- Account organizzativo: puoi utilizzare operazioni come DescribeEventsForOrganizatione DescribeEventDetailsForOrganizationottenere informazioni sugli AWS Health eventi per gli account che fanno parte della tua organizzazione.

Per ulteriori informazioni sulle operazioni API disponibili, consulta l'AWS Health API Reference.

Singole operazioni

Puoi impostare l'`Action`elemento di una policy IAM su`health:Describe*`. Ciò consente l'accesso a AWS Health Dashboard e AWS Health. AWS Health supporta il controllo degli accessi agli eventi basati sul servizio `eventTypeCode` and.

Descrivere l'accesso

Questa dichiarazione politica concede l'accesso a tutte le operazioni API AWS Health Dashboard e a qualsiasi altra. `Describe*` AWS Health Ad esempio, un utente IAM con questa policy può accedere AWS Health Dashboard a in AWS Management Console e richiamare l'operazione AWS Health `DescribeEvents` API.

Example : Descrivere l'accesso

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
```

```
}
```

Negare l'accesso

Questa dichiarazione politica nega l'accesso AWS Health Dashboard e all' AWS Health API. Un utente IAM con questa policy non può visualizzarla AWS Management Console e non può richiamare nessuna delle operazioni AWS Health API. AWS Health Dashboard

Example : Negare l'accesso

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

Visualizzazione organizzativa

Se desideri abilitare la visualizzazione organizzativa per AWS Health, devi consentire l'accesso alle AWS Organizations azioni AWS Health e.

L'`Action`elemento di una policy IAM deve includere le seguenti autorizzazioni:

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListParents`

Per comprendere le autorizzazioni esatte necessarie per ciascuna di esse APIs, consulta Actions AWS Health APIs Defined by e Notifications nella IAM User Guide.

> **Note**
>
> È necessario utilizzare le credenziali dell'account di gestione di un'organizzazione per accedere al AWS Health APIs modulo. AWS Organizations Per ulteriori informazioni, consulta Aggregazione di AWS Health eventi tra account.

Consenti l'accesso alla visualizzazione AWS Health organizzativa

Questa dichiarazione politica garantisce l'accesso a tutte AWS Health le AWS Organizations azioni necessarie per la funzionalità di visualizzazione organizzativa.

Example : Consenti l'accesso alla visualizzazione AWS Health organizzativa

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

Negare l'accesso alla visualizzazione AWS Health organizzativa

Questa dichiarazione politica nega l'accesso alle AWS Organizations azioni ma consente l'accesso alle AWS Health azioni per un singolo account.

Example : nega l'accesso alla visualizzazione AWS Health organizzativa

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
```

```
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

> **Note**
>
> Se l'utente o il gruppo a cui desideri concedere le autorizzazioni dispone già di una policy IAM, puoi aggiungere la dichiarazione AWS Health di policy specifica a tale policy.

Condizioni basate su risorse e operazioni

AWS Health supporta le condizioni IAM per le operazioni DescribeAffectedEntitiese DescribeEventDetailsAPI. Puoi utilizzare condizioni basate su risorse e azioni per limitare gli eventi che l' AWS Health API invia a un utente, gruppo o ruolo.

A tale scopo, aggiorna il `Condition` blocco della policy IAM o imposta l'`Resource`elemento. Puoi utilizzare String Conditions per limitare l'accesso in base a determinati campi di AWS Health eventi.

Puoi utilizzare i seguenti campi quando specifichi un AWS Health evento nella tua politica:

- `eventTypeCode`
- `service`

> **Note**
>
> - Le operazioni DescribeAffectedEntitiese le DescribeEventDetailsAPI supportano le autorizzazioni a livello di risorsa. Ad esempio, puoi creare una politica per consentire o negare eventi specifici. AWS Health

- Le operazioni DescribeAffectedEntitiesForOrganizatione DescribeEventDetailsForOrganizationAPI non supportano le autorizzazioni a livello di risorsa.
- Per ulteriori informazioni, consulta Azioni, risorse e chiavi di condizione per AWS Health APIs e notifiche nel Service Authorization Reference.

Example : Condizione basata su operazioni

Questa informativa sulla politica concede l'accesso AWS Health Dashboard e le operazioni dell' AWS Health `Describe*`API, ma nega l'accesso a qualsiasi AWS Health evento relativo ad Amazon. EC2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
}
```

Example : Condizione basata su risorse

La seguente policy ha lo stesso effetto, ma utilizza l'elemento `Resource`.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*"
  }]
}
```

Example : condizione eventTypeCode

Questa dichiarazione politica concede l'accesso AWS Health Dashboard e le operazioni dell' AWS Health `Describe*`API, ma nega l'accesso a tutti AWS Health gli eventi `eventTypeCode` che corrispondono. `AWS_EC2_*`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
```

```
                }
            }
        }
    ]
}
```

> **Important**
>
> Se chiami le DescribeEventDetailsoperazioni DescribeAffectedEntitiesand e non disponi dell'autorizzazione per accedere all' AWS Health evento, viene `AccessDeniedException` visualizzato l'errore. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi AWS Health all'identità e all'accesso.

Risoluzione dei problemi relativi AWS Health all'identità e all'accesso

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

Argomenti

- Non sono autorizzato a eseguire un'azione in AWS Health
- Non sono autorizzato a eseguire iam: PassRole
- Desidero visualizzare le mie chiavi di accesso
- Sono un amministratore e voglio consentire ad altri di accedere AWS Health
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse AWS Health

Non sono autorizzato a eseguire un'azione in AWS Health

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'`AccessDeniedException`errore viene visualizzato quando un utente non dispone dell'autorizzazione all'uso AWS Health Dashboard o alle operazioni dell' AWS Health API.

In questo caso, l'amministratore dell'utente deve aggiornare la policy per consentire l'accesso dell'utente.

L' AWS Health API richiede un piano Business, Enterprise On-Ramp o Enterprise Support di. Supporto AWS Se chiami l' AWS Health API da un account che non dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, viene restituito il seguente codice di errore:. `SubscriptionRequiredException`

Non sono autorizzato a eseguire iam: PassRole

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

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.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Health. Tuttavia, l'operazione 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 colui che ti ha fornito le credenziali di accesso.

Desidero visualizzare le mie chiavi di accesso

Dopo aver creato le chiavi di accesso utente IAM, è possibile visualizzare il proprio ID chiave di accesso in qualsiasi momento. Tuttavia, non è possibile visualizzare nuovamente la chiave di accesso segreta. Se perdi la chiave segreta, dovrai creare una nuova coppia di chiavi di accesso.

Le chiavi di accesso sono composte da due parti: un ID chiave di accesso (ad esempio `AKIAIOSFODNN7EXAMPLE`) e una chiave di accesso segreta (ad esempio, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Come un nome utente e una password, è necessario utilizzare sia l'ID chiave di accesso sia la chiave di accesso segreta insieme per autenticare le richieste dell'utente. Gestisci le tue chiavi di accesso in modo sicuro mentre crei il nome utente e la password.

> **Important**
>
> Non fornire le chiavi di accesso a terze parti, neppure per aiutare a trovare l'ID utente canonico. In questo modo, potresti concedere a qualcuno l'accesso permanente al tuo Account AWS.

Quando crei una coppia di chiavi di accesso, ti viene chiesto di salvare l'ID chiave di accesso e la chiave di accesso segreta in una posizione sicura. La chiave di accesso segreta è disponibile solo al momento della creazione. Se si perde la chiave di accesso segreta, è necessario aggiungere nuove chiavi di accesso all'utente IAM. È possibile avere massimo due chiavi di accesso. Se se ne hanno già due, è necessario eliminare una coppia di chiavi prima di crearne una nuova. Per visualizzare le istruzioni, consulta Gestione delle chiavi di accesso nella Guida per l'utente di IAM.

Sono un amministratore e voglio consentire ad altri di accedere AWS Health

Per consentire ad altri di accedere AWS Health, devi concedere l'autorizzazione alle persone o alle applicazioni che necessitano dell'accesso. Se si utilizza AWS IAM Identity Center per gestire persone e applicazioni, si assegnano set di autorizzazioni a utenti o gruppi per definirne il livello di accesso. I set di autorizzazioni creano e assegnano automaticamente le policy IAM ai ruoli IAM associati alla persona o all'applicazione. Per ulteriori informazioni, consulta Set di autorizzazioni nella Guida per l'AWS IAM Identity Center utente.

Se non utilizzi IAM Identity Center, devi creare entità IAM (utenti o ruoli) per le persone o le applicazioni che necessitano di accesso. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in AWS Health. Dopo aver concesso le autorizzazioni, fornisci le credenziali all'utente o allo sviluppatore dell'applicazione. Utilizzeranno tali credenziali per accedere. AWSPer ulteriori informazioni sulla creazione di utenti, gruppi, policy e autorizzazioni IAM, consulta IAM Identities and Policies and permissions in IAM nella IAM User Guide.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse AWS Health

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Health supporta queste funzionalità, consulta. Come AWS Health 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.

Utilizzo di ruoli collegati ai servizi per AWS Health

AWS Health utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Health I ruoli collegati ai servizi sono predefiniti AWS Health e includono tutte le autorizzazioni necessarie al servizio per chiamare altri utenti al posto tuo. Servizi AWS

È possibile utilizzare un ruolo collegato al servizio da configurare per evitare di aggiungere manualmente le autorizzazioni AWS Health necessarie. AWS Health definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Health Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Autorizzazioni del ruolo collegato ai servizi per AWS Health

AWS Health ha due ruoli collegati ai servizi:

- AWSServiceRoleForHealth_Organizations— Questo ruolo si fida che AWS Health (`health.amazonaws.com`) assuma il ruolo a cui accedere Servizi AWS al posto tuo. A questo ruolo è associata la politica `Health_OrganizationsServiceRolePolicy` AWS gestita.
- AWSServiceRoleForHealth_EventProcessor— Questo ruolo prevede che il AWS Health service principal (`event-processor.health.amazonaws.com`) assuma il ruolo al posto tuo. A questo ruolo è associata la politica `AWSHealth_EventProcessorServiceRolePolicy` AWS gestita. Il responsabile del servizio utilizza il ruolo per creare una regola EventBridge gestita da Amazon per

il rilevamento e la risposta agli AWS incidenti. Questa regola è l'infrastruttura necessaria Account AWS per fornire informazioni sulla modifica dello stato di allarme dal tuo account a AWS Health.

Per ulteriori informazioni sulle politiche AWS gestite, vedereAWS politiche gestite per AWS Health.

Creazione di un ruolo collegato ai servizi per AWS Health

Non è necessario creare il ruolo AWSServiceRoleForHealth_Organizations collegato al servizio. Quando richiami l'EnableHealthServiceAccessForOrganizationoperazione, AWS Health crea questo ruolo collegato al servizio nell'account per te.

È necessario creare manualmente il ruolo AWSServiceRoleForHealth_EventProcessor collegato al servizio nel proprio account. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Modifica di un ruolo collegato ai servizi per AWS Health

AWS Health non ti consente di modificare il ruolo collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. 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 AWS Health

Per eliminare il AWSServiceRoleForHealth_Organizations ruolo, devi prima chiamare l'DisableHealthServiceAccessForOrganizationoperazione. Puoi quindi eliminare il ruolo tramite la console IAM, l'API IAM o AWS Command Line Interface (AWS CLI).

Per eliminare il AWSServiceRoleForHealth_EventProcessor ruolo, contatta Supporto AWS e chiedi che eliminino i tuoi carichi di lavoro da AWS Incident Detection and Response. Una volta completato questo processo, puoi eliminare uno dei ruoli tramite la console IAM, l'API IAM o. AWS CLI

Informazioni correlate

Per ulteriori informazioni, consulta Utilizzo di ruoli collegati a servizi nella Guida per l'utente di IAM .

AWS politiche gestite per AWS Health

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS Health dispone delle seguenti politiche gestite.

Indice

- Policy gestita da AWS : AWSHealth_EventProcessorServiceRolePolicy
- Policy gestita da AWS : Health_OrganizationsServiceRolePolicy
- AWS politica gestita: AWSHealthFullAccess
- AWS Health aggiornamenti alle politiche AWS gestite

Policy gestita da AWS : AWSHealth_EventProcessorServiceRolePolicy

AWS Health utilizza la politica AWSHealth_EventProcessorServiceRolePolicy AWS gestita. Questa policy gestita è attribuita al ruolo collegato ai servizi `AWSServiceRoleForHealth_EventProcessor`. La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health.

La policy gestita dispone delle seguenti autorizzazioni per consentire l'accesso AWS Health alla EventBridge regola Amazon per il rilevamento e la risposta agli AWS incidenti.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `events`— Descrive ed elimina EventBridge le regole e descrive e aggiorna gli obiettivi di tali regole.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Per un elenco delle modifiche alla politica, vedereAWS Health aggiornamenti alle politiche AWS gestite.

Policy gestita da AWS : Health_OrganizationsServiceRolePolicy

AWS Health utilizza la politica Health_OrganizationsServiceRolePolicy AWS gestita. Questa policy gestita è attribuita al ruolo collegato ai servizi `AWSServiceRoleForHealth_Organizations`.

La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health.

Questa politica concede le autorizzazioni che consentono di accedere AWS Health ai AWS Organizations dettagli richiesti per la visualizzazione Health Organizational.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations`— Descrive gli account in Organizations AWS Organizations e Servizi AWS che possono essere utilizzati.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

Per un elenco delle modifiche alla politica, vedereAWS Health aggiornamenti alle politiche AWS gestite.

AWS politica gestita: AWSHealthFullAccess

AWS Health utilizza la politica AWSHealthFullAccess AWS gestita. La policy concede alle entità (utenti o ruoli IAM) l'accesso alla AWS Health console. Per ulteriori informazioni, consulta Utilizzo della console di AWS Health.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations`— Abilita o disabilita la funzionalità di visualizzazione AWS Health organizzativa per tutti gli account di un' AWS organizzazione e visualizza le unità organizzative (OU) dell'account di gestione
- `health`— Accesso alle operazioni e alle notifiche dell' AWS Health API
- `iam`— Crea un ruolo IAM collegato al AWS Health servizio

```
{
    "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "OrganizationWriteAccess",
                "Effect": "Allow",
                "Action": [
                    "organizations:EnableAWSServiceAccess",
                    "organizations:DisableAWSServiceAccess"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "organizations:ServicePrincipal": "health.amazonaws.com"
                    }
                }
            },
            {
                "Sid": "HealthFullAccess",
                "Effect": "Allow",
                "Action": [
                    "health:*",
                    "organizations:DescribeAccount",
                    "organizations:ListAccounts",
                    "organizations:ListDelegatedAdministrators",
                    "organizations:ListParents"
                ],
                "Resource": "*"
            },
            {
```

```
                "Sid": "ServiceLinkAccess",
                "Effect": "Allow",
                "Action": "iam:CreateServiceLinkedRole",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "iam:AWSServiceName": "health.amazonaws.com"
                    }
                }
            }
        ]
}
```

Per un elenco delle modifiche alla politica, consultaAWS Health aggiornamenti alle politiche AWS gestite.

AWS Health aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Health da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti per AWS Health.

La tabella seguente descrive importanti aggiornamenti alle politiche AWS Health gestite dal 13 gennaio 2022.

AWS Health

Modifica	Descrizione	Data
AWS politica gestita: AWSHealthFullAccess - Aggiornamento a una policy esistente	AWS Health ha esteso la AWSHealth FullAccess politica AWS GovCloud (US) Regions alle regioni della Cina.	16 ottobre 2023
Policy gestita da AWS : Health_OrganizationsService	AWS Health ha aggiunto nuove AWS Organizations azioni per consentire al	19 luglio 2023

Modifica	Descrizione	Data
RolePolicy - Aggiornamento a una policy esistente	ruolo collegato al servizio di descrivere gli account e i AWS servizi con cui è possibile utilizzare. AWS Organizations	
Log delle modifiche pubblicato	Registro delle modifiche per le politiche AWS Health gestite.	13 gennaio 2023

Registrazione e monitoraggio AWS Health

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Health altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per osservare AWS Health, segnalare quando qualcosa non va e intraprendere azioni laddove opportuno:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon Elastic Compute Cloud EC2 (Amazon) e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon EventBridge offre un near-real-time flusso di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. EventBridge consente l'elaborazione automatizzata basata sugli eventi. Puoi scrivere le regole che controllano determinati eventi e attivano operazioni automatiche in altri servizi AWS quando tali eventi si verificano. Per ulteriori informazioni, consulta Monitoraggio degli eventi AWS Health con Amazon EventBridge.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon Simple Storage Service (Amazon S3) da te specificato. Puoi identificare quali utenti e account hanno effettuato la chiamata AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente di .

Per ulteriori informazioni, consulta Monitoraggio AWS Health.

Convalida della conformità per AWS Health

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 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)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty

può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Health

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. 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.

AWS Health gli eventi vengono archiviati e replicati su più zone di disponibilità. Questo approccio garantisce la possibilità di accedervi dalle AWS Health Dashboard operazioni dell' AWS Health API. È possibile visualizzare AWS Health gli eventi fino a 90 giorni dal momento in cui si verificano.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, vedere Infrastruttura AWS globale.

Sicurezza dell'infrastruttura nell' AWS Health

In quanto servizio gestito, AWS Health è protetto dalle procedure di sicurezza della rete AWS globale descritte nel white paper Amazon Web Services: Overview of Security Processes.

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

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Analisi della configurazione e delle vulnerabilità in AWS Health

La configurazione e i controlli IT sono una responsabilità condivisa tra voi AWS e voi, i nostri clienti. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Best practice relative alla sicurezza di AWS Health

Consulta le seguenti best practice per lavorare con AWS Health.

Concedi AWS Health agli utenti le autorizzazioni minime possibili

Seguire il principio del privilegio minimo utilizzando il set minimo di autorizzazioni della policy d'accesso per utenti e gruppi . Ad esempio, potresti consentire a un utente AWS Identity and Access Management (IAM) di accedere a. AWS Health Dashboard Tuttavia, potresti non consentire allo stesso utente di abilitare o disabilitare l'accesso ad AWS Organizations.

Per ulteriori informazioni, consulta AWS Health esempi di politiche basate sull'identità.

Visualizza il AWS Health Dashboard

Controlla AWS Health Dashboard spesso per identificare gli eventi che potrebbero influire sul tuo account o sulle tue applicazioni. Ad esempio, potresti ricevere una notifica di evento sulle tue risorse, come un'istanza Amazon Elastic Compute Cloud (Amazon EC2) che deve essere aggiornata.

Per ulteriori informazioni, consulta Guida introduttiva alla AWS Health dashboard.

Integrazione AWS Health con Amazon Chime o Slack

Puoi integrarti AWS Health con i tuoi strumenti di chat. Questa integrazione consente a te e al tuo team di ricevere notifiche sugli AWS Health eventi in tempo reale. Per ulteriori informazioni, consulta la sezione AWS Health Strumenti in GitHub.

Monitora gli AWS Health eventi

Puoi integrarti AWS Health con Amazon CloudWatch Events, in modo da poter creare regole per eventi specifici. Quando CloudWatch Events rileva un evento che corrisponde alla tua regola, ricevi una notifica e puoi quindi agire. CloudWatch Gli eventi sono specifici della regione, quindi è necessario configurare questo servizio nella regione in cui risiede l'applicazione o l'infrastruttura.

In alcuni casi, non è possibile determinare la regione per l' AWS Health evento. Se si verifica tale situazione, l'evento viene visualizzato per impostazione predefinita nella regione Stati Uniti orientali (Virginia settentrionale). Puoi configurare CloudWatch gli eventi in questa regione per assicurarti di monitorarli.

Per ulteriori informazioni, consulta Monitoraggio degli eventi AWS Health con Amazon EventBridge.

Aggregazione di AWS Health eventi tra account

Per impostazione predefinita, puoi utilizzare AWS Health per visualizzare gli AWS Health eventi di un singolo AWS account. Se lo utilizzi AWS Organizations, puoi anche visualizzare AWS Health gli eventi centralmente in tutta l'organizzazione. Questa funzione consente di accedere alle stesse informazioni delle operazioni con account singolo. Puoi utilizzare i filtri per visualizzare gli eventi in AWS regioni, account e servizi specifici.

È possibile aggregare gli eventi per identificare gli account dell'organizzazione interessati da un evento operativo o ricevere notifiche in caso di vulnerabilità di sicurezza. È quindi possibile utilizzare queste informazioni per gestire e automatizzare in modo proattivo gli eventi di manutenzione delle risorse in tutta l'organizzazione. Utilizza questa funzionalità per rimanere informato sulle modifiche imminenti ai AWS servizi che potrebbero richiedere aggiornamenti o modifiche al codice.

È consigliabile utilizzare la funzionalità Amministratore delegato per delegare l'accesso alla visualizzazione AWS Health organizzativa a un account membro. Ciò semplifica l'accesso dei team operativi AWS Health agli eventi dell'organizzazione. La funzionalità Amministratore delegato ti consente di mantenere limitato il tuo account di gestione, fornendo al contempo ai team la visibilità di cui hanno bisogno per agire sugli AWS Health eventi.

> **Important**
>
> - AWS Health gli eventi inviati per gli account dell'organizzazione verranno visualizzati nella visualizzazione organizzativa finché l'evento è disponibile, fino a 90 giorni, anche se uno o più di tali account lasciano l'organizzazione.
> - Gli eventi organizzativi sono disponibili per 90 giorni prima di essere eliminati. Questa quota non può essere aumentata.

Prerequisiti

Prima di utilizzare la visualizzazione organizzativa, è necessario:

- Essere parte di un'organizzazione con tutte le funzionalità abilitate.
- Accedi all'account di gestione come utente AWS Identity and Access Management (IAM) o assumi un ruolo IAM.

Puoi anche accedere come utente root (scelta non consigliata) nell'account di gestione della tua organizzazione. Per ulteriori informazioni, consulta Lock away your AWS account root user access keys nella IAM User Guide.

- Se accedi come utente IAM, utilizza una policy IAM che conceda l'accesso alle azioni AWS Health and Organizations, come la AWSHealthFullAccesspolicy. Per ulteriori informazioni, consulta AWS Health esempi di politiche basate sull'identità.

Argomenti

- Abilitazione della visualizzazione organizzativa
- Visualizzazione della vista organizzativa
- Disabilitazione della visualizzazione organizzativa
- Gestione delle viste degli amministratori delegati per un'organizzazione

Abilitazione della visualizzazione organizzativa

Puoi utilizzare la AWS Health console per ottenere una visualizzazione centralizzata degli eventi sanitari della tua AWS organizzazione.

La visualizzazione organizzativa è disponibile nella AWS Health console per tutti i Supporto AWS piani senza costi aggiuntivi.

> **Note**
>
> Se desideri consentire agli utenti di accedere a questa funzionalità nell'account di gestione, devono disporre di autorizzazioni come la AWSHealthFullAccesspolitica. Per ulteriori informazioni, consulta AWS Health esempi di politiche basate sull'identità.

Enabling organizational view (Console)

È possibile abilitare la visualizzazione organizzativa dalla AWS Health console. È necessario accedere all'account di gestione della propria AWS organizzazione.

Per visualizzare la AWS Health dashboard della tua organizzazione

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.

2. Nel riquadro di navigazione, sotto Lo stato della tua organizzazione, scegli Configurazioni.
3. Nella pagina Abilita visualizzazione organizzativa, scegli Abilita visualizzazione organizzativa.
4. (Facoltativo) Se desideri apportare modifiche alle tue AWS organizzazioni, ad esempio creare unità organizzative (OUs), scegli Gestisci AWS Organizations.

   Per ulteriori informazioni, consulta Nozioni di base su AWS Organizations nella Guida per l'utente di AWS Organizations .

> **Note**
>
> - Quando abiliti la visualizzazione AWS Health organizzativa, il processo iniziale di caricamento dell'account viene eseguito in background e il completamento potrebbe richiedere alcuni minuti. Puoi chiudere la AWS Health console e tornare più tardi, poiché non è necessario attendere il completamento del processo. Gli eventi sanitari storici (quelli creati prima dell'attivazione della funzionalità) potrebbero richiedere fino a 24 ore per essere visualizzati nella visualizzazione dell'organizzazione.
> - Se disponi di un piano Business, Enterprise On-Ramp o Enterprise Support, puoi chiamare l'operatore dell'DescribeHealthServiceStatusForOrganizationAPI per verificare lo stato del processo.
> - Quando abiliti questa funzionalità, il ruolo `AWSServiceRoleForHealth_Organizations` collegato al servizio con la policy `Health_OrganizationsServiceRolePolicy` AWS gestita viene applicato all'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health.

Enabling organizational view (CLI)

È possibile abilitare la visualizzazione organizzativa utilizzando l'operazione EnableHealthServiceAccessForOrganizationAPI.

È possibile utilizzare AWS Command Line Interface (AWS CLI) o il proprio codice per chiamare questa operazione.

> **Note**
>
> - È necessario disporre di un piano Business, Enterprise On-Ramp o Enterprise Support per chiamare l' AWS Health API.
> - È necessario utilizzare l'endpoint della regione Stati Uniti orientali (Virginia settentrionale).

Example

Il AWS CLI comando seguente abilita questa funzionalità dal tuo AWS account. È possibile utilizzare questo comando dall'account di gestione o da un account che può assumere il ruolo con le autorizzazioni richieste.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

I seguenti esempi di codice chiamano l'operazione EnableHealthServiceAccessForOrganizationAPI.

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

È possibile utilizzare l' AWS SDK per la versione Java 2.0 per l'esempio seguente.

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationReques
```

```
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
 client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
 statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
 enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
 progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already
 in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
```

```
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
 e);
        }
    }
}
```

Per ulteriori informazioni, vedere Guida per sviluppatori SDK AWS for Java 2.0.

Quando si abilita questa funzionalità, il ruolo `AWSServiceRoleForHealth_Organizations` collegato al servizio con la politica `Health_OrganizationsServiceRolePolicy` AWS gestita viene applicato all'account di gestione dell'organizzazione.

> **Note**
>
> L'attivazione di questa funzionalità è un processo asincrono e richiederà tempo per essere completata. È possibile chiamare l'DescribeHealthServiceStatusForOrganizationoperazione per verificare lo stato del processo.

Visualizzazione della vista organizzativa

È possibile utilizzare la AWS Health console per ottenere una visualizzazione centralizzata degli eventi sanitari AWS dell'organizzazione.

La visualizzazione organizzativa è disponibile nella AWS Health console per tutti i Supporto AWS piani senza costi aggiuntivi.

> **Note**
>
> Se desideri consentire agli utenti di accedere a questa funzionalità nell'account di gestione, devono disporre di autorizzazioni come AWSHealthFullAccesspolitica. Per ulteriori informazioni, consulta AWS Health esempi di politiche basate sull'identità.

Viewing organizational view events (Console)

Dopo aver abilitato la visualizzazione organizzativa, AWS Health visualizza gli eventi sanitari per tutti gli account dell'organizzazione.

Quando un account entra a far parte dell'organizzazione, AWS Health lo aggiunge automaticamente alla visualizzazione organizzativa. Quando un account lascia l'organizzazione, i nuovi eventi di tale account non vengono più registrati nella visualizzazione organizzativa. Tuttavia, gli eventi esistenti rimangono ed è comunque possibile interrogarli fino al limite di 90 giorni.

AWS conserva i dati relativi alla policy dell'account per 90 giorni dalla data effettiva di chiusura dell'account amministratore. Al termine del periodo di 90 giorni, elimina AWS definitivamente tutti i dati relativi alla politica dell'account.

- Per conservare i risultati per più di 90 giorni, puoi archiviare le policy. Puoi anche utilizzare un'azione personalizzata con una EventBridge regola per archiviare i risultati in un bucket S3.
- Finché AWS conserva i dati della politica, quando riapri l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati della politica di servizio per l'account.
- Per ulteriori informazioni, consulta Chiusura di un account.

> **Important**
>
> Per i clienti delle regioni: AWS GovCloud (US)
>
> - Prima di chiudere il tuo account, effettua il backup ed elimina le risorse dell'account. Dopo aver chiuso l'account, non avrai più accesso ad essi.

> **Note**
>
> Quando abiliti questa funzione, la AWS Health console può visualizzare gli eventi pubblici dalla AWS Health Dashboard — Service Health degli ultimi 7 giorni. Questi eventi pubblici non sono specifici degli account della tua organizzazione. Events from the AWS Health Dashboard — Service Health fornisce informazioni pubbliche sulla disponibilità regionale dei AWS servizi.

È possibile visualizzare gli eventi di visualizzazione organizzativa nelle pagine seguenti:.

Problemi aperti e recenti

È possibile utilizzare la scheda Problemi aperti e recenti per visualizzare gli eventi che potrebbero influire sull' AWS infrastruttura, ad esempio le modifiche Servizi AWS e le risorse che influiscono sull'organizzazione.

Per visualizzare gli eventi organizzativi, visualizza gli eventi.

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Nel riquadro di navigazione, sotto Lo stato della tua organizzazione, scegli Problemi aperti e recenti per visualizzare gli eventi segnalati di recente.
3. Scegli un evento. Nella scheda Dettagli, puoi visualizzare le seguenti informazioni sull'evento:

    - Nome evento
    - Stato
    - Regione/ Zona di disponibilità
    - Account interessati
    - Ora di inizio
    - Ora di fine
    - Categoria
    - Descrizione

Modifiche pianificate

Utilizza la scheda Modifiche pianificate per visualizzare gli eventi imminenti che potrebbero influire sulla tua organizzazione. Questi eventi possono includere attività di manutenzione programmate per i servizi.

Altre notifiche

Utilizza la scheda Notifiche per visualizzare tutte le altre notifiche e gli eventi in corso degli ultimi sette giorni che potrebbero influire sulla tua organizzazione. Ciò può includere eventi, come rotazioni dei certificati, notifiche di fatturazione e vulnerabilità di sicurezza.

Event Log (Log eventi)

Puoi anche utilizzare la scheda Registro eventi per visualizzare AWS Health gli eventi per la visualizzazione organizzativa. Il layout e il comportamento delle colonne sono simili alla scheda Problemi aperti e recenti, tranne per il fatto che la scheda Registro eventi include colonne e opzioni di filtro aggiuntive, come la categoria Evento, lo Stato e l'ora di inizio.

Per visualizzare gli eventi organizzativi, visualizza gli eventi nella scheda Registro eventi

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Nel riquadro di navigazione, sotto Lo stato della tua organizzazione, scegli Registro eventi.
3. In Registro eventi, scegli il nome dell'evento. Puoi esaminare le seguenti informazioni sull'evento:
   - Nome evento
   - Stato
   - Regione/ Zona di disponibilità
   - Account interessati
   - Ora di inizio
   - Ora di fine
   - Categoria
   - Descrizione

Viewing affected accounts and resources (Console)

Nella sezione Lo stato della tua organizzazione, puoi visualizzare gli account dell'organizzazione interessati dall'evento e tutte le risorse correlate. Ad esempio, se è imminente un evento per la manutenzione delle istanze Amazon Elastic Compute Cloud (Amazon EC2), gli account della tua organizzazione che dispongono di EC2 istanze Amazon possono apparire nella scheda Dettagli. Puoi identificare le risorse specifiche e quindi contattare il proprietario dell'account.

Per visualizzare gli account e le risorse interessati

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Nel riquadro di navigazione, sotto Lo stato della tua organizzazione, scegli una delle schede.
3. Scegli un evento che abbia un valore per gli account interessati.
4. Scegli la scheda Account interessati.
5. Scegli Mostra i dettagli dell'account per visualizzare le seguenti informazioni relative agli account:
   - ID account
   - Account name (Nome account)

- Email principale
- Unità organizzativa (UO)

6. Espandi l'account per visualizzare le risorse interessate.
7. Se sono presenti più di 10 risorse, scegli Visualizza tutte le risorse per visualizzarle.
8. Per filtrare in base all'ID dell'account per questo evento specifico, procedi come segue:

   a. Nella scheda Account interessati, scegli Aggiungi filtro, scegli ID account, quindi inserisci l'ID dell'account. Puoi inserire un solo ID account alla volta.

   b. Scegli Applica. L'account che hai inserito viene visualizzato nell'elenco.

Viewing organizational view events (CLI)

Dopo aver abilitato questa funzionalità, AWS Health inizia a registrare gli eventi che influiscono sugli account dell'organizzazione. Quando un account entra a far parte dell'organizzazione, AWS Health aggiunge automaticamente l'account alla visualizzazione organizzativa.

> **Note**
>
> AWS Health non registra gli eventi che si sono verificati nell'organizzazione prima di abilitare la visualizzazione organizzativa.

Quando un account lascia l'organizzazione, i nuovi eventi di tale account non vengono più registrati nella visualizzazione organizzativa. Tuttavia, gli eventi esistenti rimangono ed è comunque possibile interrogarli fino al limite di 90 giorni.

AWS conserva i dati delle policy per l'account per 90 giorni dalla data di entrata in vigore della chiusura dell'account amministratore. Al termine del periodo di 90 giorni, elimina AWS definitivamente tutti i dati relativi alla politica dell'account.

- Per conservare i risultati per più di 90 giorni, puoi archiviare le policy. Puoi anche utilizzare un'azione personalizzata con una EventBridge regola per archiviare i risultati in un bucket S3.
- Finché AWS conserva i dati della politica, quando riapri l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati della politica di servizio per l'account.
- Per ulteriori informazioni, consulta Chiusura di un account.

> **Important**
>
> Per i clienti delle regioni: AWS GovCloud (US)
>
> - Prima di chiudere il tuo account, effettua il backup ed elimina le risorse dell'account. Dopo aver chiuso l'account, non avrai più accesso ad essi.

È possibile utilizzare le operazioni AWS Health API per restituire eventi dal punto di vista organizzativo.

Example : descrivere gli eventi di visualizzazione organizzativa

Il AWS CLI comando seguente restituisce gli eventi sanitari per AWS gli account dell'organizzazione.

```
aws health describe-events-for-organization --region us-east-1
```

Disabilitazione della visualizzazione organizzativa

Se non desideri aggregare gli eventi per la tua organizzazione, puoi disattivare questa funzionalità dall'account di gestione oppure puoi disabilitare la visualizzazione organizzativa utilizzando l'operazione DisableHealthServiceAccessForOrganizationAPI.

Disabling organizational view events (Console)

AWS Health interrompe l'aggregazione degli eventi per tutti gli altri account dell'organizzazione. Puoi continuare a visualizzare gli eventi precedenti della tua organizzazione finché non vengono eliminati.

Per disabilitare la visualizzazione organizzativa

1. Apri la AWS Health dashboard a https://health.aws.amazon.com/health/casa.
2. Nel riquadro di navigazione, sotto Lo stato della tua organizzazione, scegli Configurazioni.
3. Nella pagina Abilita visualizzazione organizzativa, scegli Disabilita visualizzazione organizzativa.

Dopo aver disattivato questa funzionalità, AWS Health non aggrega più gli eventi della tua organizzazione. Tuttavia, il ruolo collegato al servizio rimane nell'account di gestione finché non lo elimini tramite la console AWS Identity and Access Management (IAM), l'API IAM o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Disabling organizational view events (CLI)

Example

Il AWS CLI comando seguente disabilita questa funzionalità dal tuo account.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> **Note**
>
> Puoi anche disabilitare la funzionalità organizzativa utilizzando l'operazione API Organizations Disable AWSService Access. Dopo aver richiamato questa operazione, AWS Health interrompe l'aggregazione degli eventi per tutti gli altri account dell'organizzazione. Se chiami le operazioni AWS Health API per la visualizzazione organizzativa, AWS Health restituisce un errore. AWS Health continua ad aggregare gli eventi sanitari per il tuo AWS account.

Dopo aver disabilitato questa funzione, AWS Health non aggrega più gli eventi della tua organizzazione. Tuttavia, il ruolo collegato al servizio rimane nell'account di gestione finché non lo elimini tramite la console AWS Identity and Access Management (IAM), l'API IAM o. AWS CLIPer ulteriori informazioni, consulta Eliminazione di un ruolo collegato al servizio nella Guida per l'utente IAM.

Gestione delle viste degli amministratori delegati per un'organizzazione

Con AWS Health, puoi sfruttare la funzionalità di amministratore delegato AWS Organizations che consente a un account diverso dall'account di gestione di visualizzare gli AWS Health eventi aggregati sulla AWS Health dashboard o in modo programmatico tramite l'API.AWS Health La funzionalità di amministratore delegato offre ai diversi team la flessibilità necessaria per visualizzare

e gestire gli eventi sanitari all'interno dell'organizzazione. È una best practice AWS di sicurezza delegare le responsabilità al di fuori dell'account di gestione, ove possibile.

Indice

- Registrazione di un amministratore delegato per la visualizzazione organizzativa
- Rimozione di un amministratore delegato dalla visualizzazione organizzativa

Registrazione di un amministratore delegato per la visualizzazione organizzativa

Dopo aver abilitato la visualizzazione organizzativa per l'organizzazione, è possibile registrare fino a cinque account membro nell'organizzazione come amministratore delegato. A tale scopo, richiamate l'operazione RegisterDelegatedAdministratorAPI. Dopo aver registrato gli account dei membri, questi sono delegati ad amministrare gli account e possono accedere alla visualizzazione AWS Health organizzativa dalla AWS Health Dashboard. Se l'account dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, gli amministratori delegati possono utilizzare l' AWS Health API per accedere alla visualizzazione organizzativa. AWS Health

Per creare un amministratore delegato, dall'account di gestione dell'organizzazione, chiamate il seguente comando (). AWS Command Line Interface AWS CLIÈ possibile utilizzare questo comando dall'account di gestione o da un account che può assumere il ruolo con le AWS Identity and Access Management autorizzazioni richieste. Nel comando di esempio seguente, sostituisci ACCOUNT_ID con l'ID dell'account membro che desideri registrare insieme al responsabile del AWS Health servizio «health.amazonaws.com».

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Dopo la registrazione di un amministratore delegato, avrai visibilità su tutti gli eventi che riguardano gli account dell'organizzazione. AWS Health Puoi visualizzare gli eventi cronologici degli ultimi 90 giorni o dalla prima attivazione della funzionalità di visualizzazione organizzativa, a seconda di quale dei due eventi sia più recente. Tieni presente che l'attivazione della funzionalità di amministratore delegato è un processo asincrono e il completamento richiede fino a un minuto.

Rimozione di un amministratore delegato dalla visualizzazione organizzativa

Per rimuovere l'accesso a un amministratore delegato, chiama l'operazione API. DeregisterDelegatedAdministrator

Dall'account di gestione della tua organizzazione, chiama il seguente AWS CLI comando per rimuovere un account membro come amministratore delegato. Nel comando di esempio seguente, sostituisci ACCOUNT_ID con l'ID dell'account membro che desideri rimuovere.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Monitoraggio degli eventi AWS Health con Amazon EventBridge

Puoi usare Amazon EventBridge per rilevare e reagire agli AWS Health eventi. Quindi, in base alle regole che EventBridge crei, richiama una o più azioni mirate quando un evento corrisponde ai valori specificati in una regola. A seconda del tipo di evento, è possibile acquisire informazioni sull'evento, avviare eventi aggiuntivi, inviare notifiche, intraprendere azioni correttive o eseguire altre azioni. Ad esempio, puoi utilizzarlo per AWS Health ricevere notifiche e-mail se disponi Account AWS di AWS risorse programmate per gli aggiornamenti, come le istanze di Amazon Elastic Compute Cloud (Amazon EC2).

> **Note**
>
> - AWS Health organizza eventi con il massimo impegno possibile. Non è sempre garantito che gli eventi vengano consegnati EventBridge.
> - Tutte EventBridge le regole che crei possono ricevere notifiche solo per le tue Account AWS. Per ricevere eventi organizzativi per altri account all'interno del tuo account AWS Organizations, vedi Aggregazione AWS Health degli eventi utilizzando la visualizzazione organizzativa e l'accesso delegato come amministratore.

Puoi scegliere tra più tipi di target EventBridge come parte del tuo AWS Health flusso di lavoro, tra cui:

- AWS Lambda funzioni
- Flusso di dati Amazon Kinesis
- Code di Amazon Simple Queue Service (Amazon SQS)
- Obiettivi incorporati (come le azioni di CloudWatch allarme)
- Argomenti su Amazon Simple Notification Service (Amazon SNS)

Ad esempio, puoi utilizzare una funzione Lambda per passare una notifica a un canale Slack quando si verifica un AWS Health evento. In alternativa, puoi usare Lambda e EventBridge inviare notifiche di testo o SMS personalizzate con Amazon SNS quando si AWS Health verifica un evento.

Per esempi di automazione e avvisi personalizzati che puoi creare in risposta agli AWS Health eventi, consulta la AWS Health sezione Strumenti in. GitHub

Argomenti

- Creazione di EventBridge regole per la copertura Regione AWS
- Monitoraggio degli eventi pubblici e specifici dell'account per AWS Health
- Installazione di un ruolo collegato al servizio per utilizzare AWS Incident Detection and Response
- Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge
- Aggregazione degli AWS Health eventi utilizzando la visualizzazione organizzativa e l'accesso amministrativo delegato
- Integrazione del monitoraggio e delle notifiche degli AWS Health eventi con JIRA e ServiceNow
- Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi in AWS Health
- Configurazione di Amazon Q Developer nelle applicazioni di chat per inviare notifiche sugli eventi in AWS Health
- Esecuzione automatica delle operazioni sulle EC2 istanze in risposta agli eventi in AWS Health
- Riferimento: Amazon EventBridge schema AWS Health degli eventi

Creazione di EventBridge regole per la copertura Regione AWS

Devi creare una EventBridge regola per ogni regione per cui desideri ricevere AWS Health eventi. Se non crei una regola, non riceverai eventi. Ad esempio, per ricevere eventi dalla regione Stati Uniti occidentali (Oregon), devi creare una regola per questa regione.

La configurazione di una regola aggiuntiva in una regione di backup aggiunge un ulteriore livello di resilienza ai flussi di lavoro, nel caso in cui la regola principale fosse influenzata da un evento in corso. Gli eventi pubblici per AWS Health vengono inviati contemporaneamente sia alla regione interessata che a una regione di backup. Per ulteriori informazioni, consulta Informazioni sugli eventi pubblici per AWS Health. Per tutte le regioni nella partizione AWS standard, puoi configurare una regola negli Stati Uniti occidentali (Oregon) come backup per continuare a ricevere eventi anche se la tua regione principale è interessata da un problema in corso. La regione di backup per la regione Stati Uniti occidentali (Oregon) è la regione Stati Uniti orientali (Virginia settentrionale).

Ad esempio, se stai monitorando eventi nella regione Europa (Francoforte) e tale regione è temporaneamente non disponibile, AWS Health invieremo l'evento anche nella regione Stati Uniti

occidentali (Oregon). Successivamente, la tua EventBridge regola di backup invia l'evento ai target che hai specificato. Per creare una regola di backup, segui la procedura seguente Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi in AWS Health e utilizza la regione Stati Uniti occidentali (Oregon).

Alcuni AWS Health eventi non sono specifici della regione. Gli eventi che non sono specifici di una regione sono chiamati eventi globali. Questi includono gli eventi inviati per AWS Identity and Access Management (IAM). Per ricevere eventi globali, è necessario creare una regola per la regione Stati Uniti orientali (Virginia settentrionale) per la regione principale e la regione Stati Uniti occidentali (Oregon) come regione di backup.

Per ricevere eventi globali nella regione AWS GovCloud (US), è necessario creare una regola nella regione AWS GovCloud (Stati Uniti occidentali).

Monitoraggio degli eventi pubblici e specifici dell'account per AWS Health

Quando crei una EventBridge regola per monitorare gli eventi AWS Health, la regola fornisce sia eventi specifici dell'account che eventi pubblici:

- Gli eventi specifici dell'account influiscono sul tuo account e sulle tue risorse, ad esempio un evento che ti informa di un aggiornamento richiesto di un' EC2 istanza Amazon o di altri eventi di modifica pianificati.
- Gli eventi pubblici vengono visualizzati nella AWS Health Dashboard — Stato del servizio. Gli eventi pubblici non sono specifici Account AWS e forniscono informazioni pubbliche sulla disponibilità regionale di un servizio.

> **Important**
>
> Per ricevere entrambi i tipi di eventi, la regola deve utilizzare il `"source": [ "aws.health"]` valore. I caratteri jolly, ad esempio `"source": [ "aws.health*"]` non corrispondono allo schema da monitorare per eventuali eventi.

Se stai monitorando eventi pubblici da un Regione AWS, ti consigliamo di creare una regola di backup. Gli eventi pubblici di AWS Health vengono inviati contemporaneamente sia alla regione interessata che a una regione di backup. Si consiglia di deduplicare AWS Health gli eventi utilizzando

eventARN e CommunicationID perché questi rimangono coerenti per AWS Health i messaggi inviati alla regione di backup.

È possibile identificare se un evento è pubblico o specifico dell'account in, utilizzando il parametro. EventBridge eventScopeCode Gli eventi possono avere o. `PUBLIC` `ACCOUNT_SPECIFIC` Puoi anche filtrare la tua regola in base a questo parametro.

Esempio: eventi pubblici per Amazon Elastic Compute Cloud

L'evento seguente mostra un problema operativo per Amazon EC2 nella regione Stati Uniti orientali (Virginia settentrionale).


```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "latestDescription": "We are investigating increased API Error rates and
 Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
            "language": "en_US"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"

    }
```

```
}
```

Installazione di un ruolo collegato al servizio per utilizzare AWS Incident Detection and Response

Se utilizzi AWS Incident Detection and Response per il tuo account, devi installare il ruolo `AWSServiceRoleForHealth_EventProcessor` collegato al servizio nel tuo account.

Questo ruolo si affida al responsabile del `event-processor.health.amazonaws.com` servizio per l'assunzione del ruolo. A questo ruolo è associata la politica `AWSHealth_EventProcessorServiceRolePolicy` AWS gestita. Questa politica elenca le autorizzazioni che il ruolo può eseguire, ad esempio chiamare altre persone Servizi AWS per conto tuo.

Questo ruolo crea quindi una regola EventBridge gestita da Amazon nel tuo account. La regola è denominata`AWSHealthEventProcessor-DO-NOT-DELETE`. Questa regola è l'infrastruttura necessaria per il tuo account in modo che EventBridge possa fornire informazioni sulla modifica dello stato di allarme dal tuo account a AWS Health.

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

- Utilizzo di ruoli collegati ai servizi per AWS Health
- Policy gestita da AWS : AWSHealth_EventProcessorServiceRolePolicy

Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge

AWS Health supporta l'impaginazione degli AWS Health eventi quando l'elenco `resources` o `affectedEntities` fa sì che la dimensione del messaggio superi il limite di 256 KB di dimensione EventBridge del messaggio.

AWS Health include tutti `resources` i `detail.affectedEntities` campi del messaggio. Se questo elenco di `detail.affectedEntities` valori `resources` e supera 256 KB, AWS Health divide l'evento sanitario in più pagine e pubblica queste pagine come singoli messaggi in. EventBridge Ogni pagina mantiene gli stessi `communicationId` valori `eventARN` e valori per

aiutare a ricombinare l'elenco `resources` o `detail.affectedEntities` dopo che tutte le pagine sono state ricevute.

Questi messaggi aggiuntivi potrebbero generare messaggi non necessari, ad esempio quando la EventBridge regola viene indirizzata a un'interfaccia leggibile dall'uomo come e-mail o chat. I clienti con notifiche leggibili dall'uomo possono aggiungere un filtro per il `detail.page` campo in modo che elabori solo la prima pagina, eliminando così i messaggi non necessari creati dalle pagine successive.

Nello schema, ogni CommunicationID include il numero di pagina sillabato dopo il CommunicationID, anche quando è presente solo 1 pagina. I campi `detail.page` `detail.totalPages` descrivono il numero di pagina corrente e il numero totale di pagine dell'evento. AWS Health Le informazioni contenute in ogni messaggio impaginato sono le stesse ad eccezione dell'elenco di `detail.affectedEntities` o. `resources` Questi elenchi possono essere ricostruiti dopo aver ricevuto tutte le pagine. Le pagine delle risorse e delle entità interessate sono indipendenti dall'ordine.

Aggregazione degli AWS Health eventi utilizzando la visualizzazione organizzativa e l'accesso amministrativo delegato

AWS Health supporta la visualizzazione organizzativa e l'accesso amministrativo delegato per AWS Health gli eventi pubblicati su Amazon EventBridge. Quando la visualizzazione organizzativa è attivata AWS Health, l'account di gestione o un account amministratore delegato riceve un unico feed di AWS Health eventi da tutti gli account dell'organizzazione in. AWS Organizations

Questa funzionalità è progettata per fornire una visualizzazione centralizzata per aiutare a gestire AWS Health gli eventi all'interno dell'organizzazione. La configurazione della visualizzazione organizzativa e di una EventBridge regola nell'account di gestione non disattiva EventBridge le regole per gli altri account dell'organizzazione.

Per ulteriori informazioni sull'attivazione della visualizzazione organizzativa e dell'accesso amministrativo delegato AWS Health, consulta Aggregazione degli AWS Health eventi.

Integrazione del monitoraggio e delle notifiche degli AWS Health eventi con JIRA e ServiceNow

È possibile integrare AWS Health gli eventi con JIRA e ServiceNow ricevere informazioni operative e sull'account, prepararsi per le modifiche pianificate e gestire gli eventi Health utilizzando il Service Management Connector (SMC). SMC Integration with AWS Health può utilizzare gli eventi Health

inviati EventBridge per creare, mappare e aggiornare automaticamente ticket e ServiceNow incidenti JIRA.

Puoi utilizzare la visualizzazione organizzativa e l'accesso delegato come amministratore per gestire facilmente gli eventi Health in tutta l'organizzazione all'interno di JIRA e ServiceNow incorporare AWS Health le informazioni direttamente nel flusso di lavoro del tuo team.

Per ulteriori informazioni sull' ServiceNow integrazione tramite SMC, vedere Integrazione in. AWS Health ServiceNow

Per ulteriori informazioni sull'integrazione di JIRA Management Cloud tramite SMC, vedere in JIRA.AWS Health

Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi in AWS Health

Puoi creare una EventBridge regola per ricevere notifiche in caso di AWS Health eventi nel tuo account. Prima di creare regole per gli eventi AWS Health, procedi come segue:

- Acquisisci familiarità con eventi, regole e obiettivi in. EventBridge Per ulteriori informazioni, consulta What is Amazon EventBridge? nella Amazon EventBridge User Guide e nelle novità EventBridge : monitora e rispondi alle modifiche alle tue AWS risorse.
- Creare la destinazione o le destinazioni da utilizzare nelle regole degli eventi.

Per creare una EventBridge regola per AWS Health

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina. Scegli la regione in cui desideri tenere traccia degli eventi. AWS Health
3. Nel pannello di navigazione, scegli Regole.
4. Scegli Crea regola.
5. Nella pagina Definisci dettagli della regola, inserisci un nome e una descrizione per la regola.
6. Mantiei i valori predefiniti di per Bus di eventi e Tipo di regola, quindi scegli Avanti.
7. Nella pagina Crea modello di evento, per Origine evento, scegli AWS eventi ed eventi EventBridge partner.
8. In Event pattern, per Event source, scegli Servizi AWS.

9. In Schema di eventi, per Servizio AWS, scegli Health.
10. Per Tipo di evento, scegli una delle seguenti opzioni.
    - Specific Health Abuse Events: crea una regola per AWS Health gli eventi che hanno la parola `Abuse` nel nome del tipo di evento.
    - Eventi Health specifici: crea una regola per gli eventi per uno specifico Servizio AWS, come Amazon EC2.
11. Puoi scegliere Qualsiasi servizio o Servizi specifici. Se hai scelto un servizio specifico, scegli una delle seguenti opzioni:
    - Scegliete Qualsiasi categoria di tipo di evento per creare una regola che si applica a tutte le categorie di tipi di evento.
    - Scegli le categorie di tipi di eventi specifici, quindi scegli un valore dall'elenco, ad esempio issue, AccountNotification o ScheduledChange.

    > **Tip**
    >
    > - Per monitorare tutti AWS Health gli eventi per un servizio specifico, ti consigliamo di scegliere Qualsiasi categoria di tipo di evento e Qualsiasi risorsa. In questo modo la regola monitora AWS Health tutti gli eventi, inclusi eventuali nuovi codici di tipo di evento, per il servizio specificato. Per una regola di esempio, consulta tutti EC2 gli eventi Amazon.
    > - Puoi creare una regola per monitorare più di una categoria di servizi o tipi di eventi. A tale scopo, è necessario aggiornare manualmente il modello di evento per la regola. Per ulteriori informazioni, consulta Creazione di una regola per più servizi e categorie.

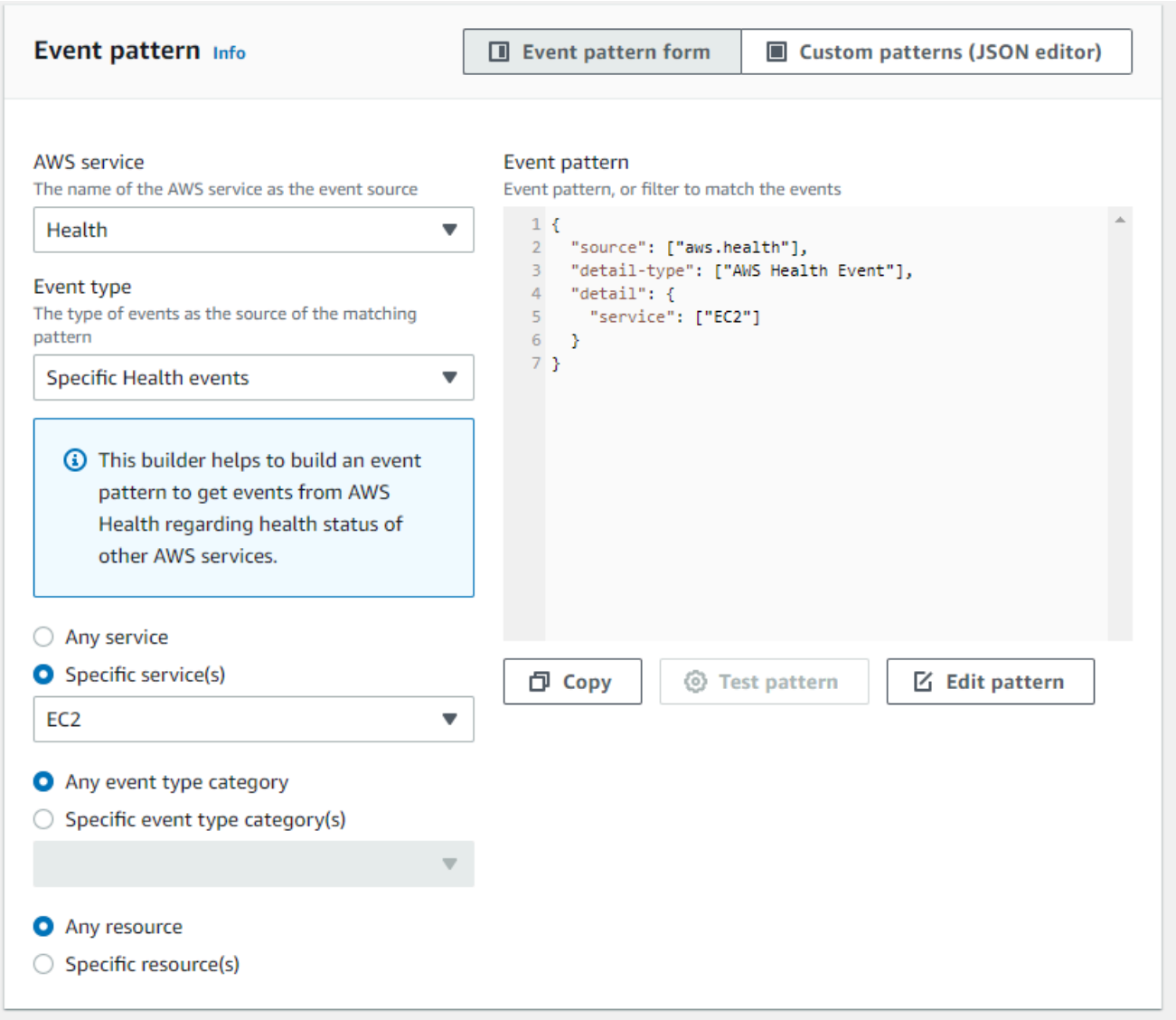
12. Se hai scelto una categoria specifica di servizi e tipi di eventi, scegli una delle seguenti opzioni per i codici dei tipi di evento.
    - Scegliete Qualsiasi codice del tipo di evento per creare una regola che si applica a tutti i codici dei tipi di evento.
    - Scegli uno o più codici di tipo di evento specifici, quindi scegli uno o più valori dall'elenco. Questo crea una regola che si applica solo a codici di tipi di eventi specifici. Ad esempio, se scegli **`AWS_EC2_INSTANCE_STOP_SCHEDULED`**e **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**, la regola si applica solo a questi eventi quando si verificano nel tuo account.
13. Scegli una delle seguenti opzioni per le risorse interessate.

- Scegli Qualsiasi risorsa per creare una regola valida per tutte le risorse.
- Scegli Risorse specifiche e inserisci IDs una o più risorse. Ad esempio, puoi specificare un ID di EC2 istanza Amazon, ad *i-EXAMPLEa1b2c3de4* esempio per monitorare gli eventi che riguardano solo questa risorsa.

14. Rivedi la configurazione delle regole in modo che soddisfi i requisiti di monitoraggio degli eventi.
15. Scegli Next (Successivo).
16. Nella pagina Seleziona obiettivi, scegli il tipo di oggetto che hai creato per questa regola, quindi configura le opzioni aggiuntive necessarie per quel tipo. Ad esempio, potresti inviare l'evento a una coda Amazon SQS o a un argomento Amazon SNS.
17. Scegli Next (Successivo).
18. (Facoltativo) Nella pagina Aggiungi tag, aggiungi tag alla chiave, quindi scegli Avanti.
    - Nota: attualmente i tag non vengono inviati dalla fonte aws.health in. EventBridge
19. Nella pagina Rivedi e crea, rivedi la configurazione della regola e fai in modo che soddisfi i requisiti di monitoraggio degli eventi.
20. Scegli Crea regola.

Example : regola per tutti gli EC2 eventi Amazon

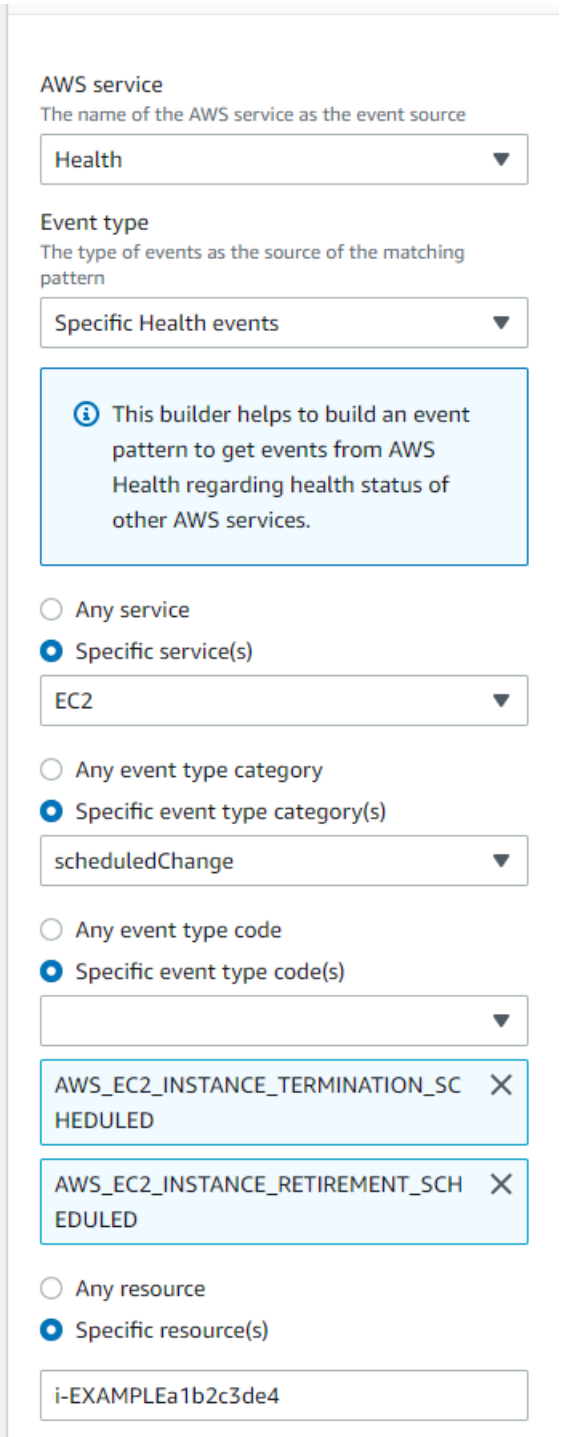
L'esempio seguente crea una regola in modo da EventBridge monitorare tutti gli EC2 eventi Amazon, incluse le categorie dei tipi di evento, i codici di evento e le risorse.



Example : regola per EC2 eventi Amazon specifici

L'esempio seguente crea una regola che EventBridge monitora quanto segue:

- Il EC2 servizio Amazon
- La categoria del tipo di evento ScheduledChange
- I codici dei tipi di evento per e `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- L'istanza con l'ID `i-EXAMPLEa1b2c3de4`



Creazione di una regola per più servizi e categorie

Gli esempi della procedura precedente mostrano come creare una regola per una singola categoria di servizi e tipi di eventi. È inoltre possibile creare una regola per più servizi e categorie di tipi di eventi. Ciò significa che non è necessario creare una regola separata per ogni servizio e categoria

che si desidera monitorare. A tale scopo, è necessario modificare lo schema degli eventi e quindi inserire le modifiche manualmente.

Puoi utilizzare una delle seguenti opzioni.

Per aggiungere servizi e categorie a una regola esistente

1. Nella EventBridge console, nella pagina Regole, scegli il nome della regola.
2. Nell'angolo in alto a destra, scegliere Edit (Modifica).
3. Scegli Next (Successivo).
4. Per Schema di evento, scegli Modifica modello, quindi inserisci le modifiche nel campo di testo.
5. Scegli Avanti fino a raggiungere la pagina di revisione e aggiornamento.
6. Scegli Aggiorna regola per salvare le modifiche.

Per aggiungere servizi e categorie per una nuova regola

1. Segui la procedura descritta Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi in AWS Health al passaggio 9.
2. Invece di scegliere un singolo servizio o categoria dagli elenchi, per Evento pattern, scegliete Modifica pattern.
3. Inserisci le modifiche nel campo di testo. Vedi il seguente pattern di esempio come modello per creare il tuo pattern di eventi.
4. Esamina lo schema dell'evento, quindi segui il resto della procedura Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi in AWS Health per creare la regola.

Usa l'API o AWS Command Line Interface (AWS CLI)

Per una regola nuova o esistente, utilizzate l'operazione PutRuleAPI o il `aws events put-rule` comando per aggiornare il modello di evento. Per un AWS CLI comando di esempio, vedete put-rule nel AWS CLI Command Reference.

Example Esempio: più servizi e categorie di tipi di eventi

Il seguente schema di eventi crea una regola per monitorare gli eventi per le `issue` categorie e tipo di `scheduledChange` evento per tre AWS servizi: Amazon EC2, Amazon EC2 Auto Scaling e Amazon VPC. `accountNotification`

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

Configurazione di Amazon Q Developer nelle applicazioni di chat per inviare notifiche sugli eventi in AWS Health

Puoi ricevere AWS Health eventi direttamente nei tuoi client di chat, come Slack e Amazon Chime. Puoi utilizzare questo evento per identificare problemi di AWS servizio recenti che potrebbero influire sulle tue AWS applicazioni e sull'infrastruttura. Quindi, puoi accedere alla tua AWS Health dashboard per saperne di più sull'aggiornamento. Ad esempio, se stai monitorando il tipo di `AWS_EC2_INSTANCE_STOP_SCHEDULED` evento nel tuo AWS account, l' AWS Health evento può apparire direttamente sul tuo canale Slack.

Prerequisiti

Prima di iniziare, devi avere quanto segue:

- Un client di chat configurato con Amazon Q Developer nelle applicazioni di chat. Puoi configurare Amazon Chime e Slack. Per ulteriori informazioni, consulta la sezione Introduzione ad Amazon Q Developer nelle applicazioni di chat nella Guida per l'amministratore delle applicazioni di chat di Amazon Q Developer.

- Un argomento di Amazon SNS che hai creato e al quale sei iscritto. Se hai già un argomento SNS, puoi utilizzarne uno esistente. Per ulteriori informazioni, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Per ricevere AWS Health eventi con Amazon Q Developer nelle applicazioni di chat

1. Segui la procedura descritta nel Configurazione di una EventBridge regola per l'invio di notifiche sugli eventi in AWS Health passaggio 13.

   a. Al termine della configurazione dello schema di eventi nel passaggio 13, aggiungi una virgola all'ultima riga dello schema e aggiungi la riga seguente per rimuovere i messaggi di chat non necessari dagli eventi impaginati AWS Health . Per informazioni, consulta Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge.

      ```
      "detail.page": ["1"]
      ```

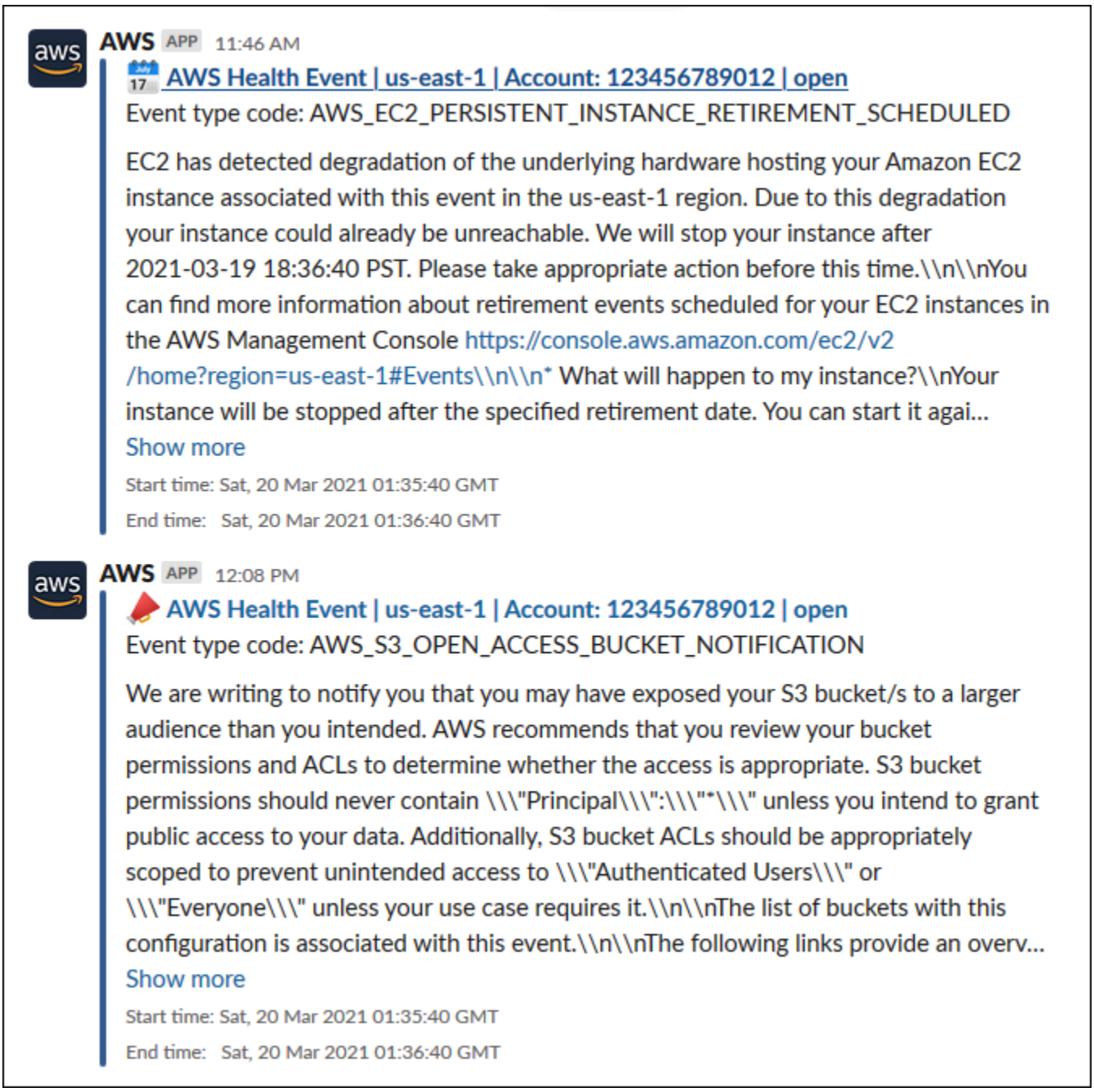
   b. Quando scegli l'obiettivo nel passaggio 14, scegli un argomento SNS. Utilizzerai lo stesso argomento SNS nella console delle applicazioni di chat di Amazon Q Developer.

   c. Completa il resto della procedura per creare la regola.
2. Accedi alla console delle applicazioni di chat di Amazon Q Developer.
3. Scegli il client di chat, ad esempio il nome del tuo canale Slack, quindi scegli Modifica.
4. Nella sezione Notifiche - opzionale, per Argomenti, scegli lo stesso argomento SNS specificato nel passaggio 1.
5. Seleziona Salva.

   Quando AWS Health invia un evento EventBridge che corrisponde alla tua regola, l' AWS Health evento verrà visualizzato nel tuo client di chat.
6. Scegli il nome dell'evento per visualizzare ulteriori informazioni nella tua AWS Health dashboard.

Example : AWS Health eventi inviati a Slack

Di seguito è riportato un esempio di due AWS Health eventi per Amazon EC2 e Amazon Simple Storage Service (Amazon S3) nella regione Stati Uniti orientali (Virginia settentrionale) che vengono visualizzati nel canale Slack.



Esecuzione automatica delle operazioni sulle EC2 istanze in risposta agli eventi in AWS Health

Puoi automatizzare le azioni che rispondono agli eventi pianificati per le tue EC2 istanze Amazon. Quando AWS Health invia un evento al tuo AWS account, la EventBridge regola può quindi richiamare obiettivi, come i documenti di AWS Systems Manager automazione, per automatizzare le azioni per tuo conto.

Ad esempio, quando è pianificato un evento di ritiro di un' EC2 istanza Amazon per un' EC2 istanza supportata da Amazon Elastic Block Store (Amazon EBS), AWS Health invierà il tipo di evento alla `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` tua dashboard. AWS Health Quando la regola rileva questo tipo di evento, puoi automatizzare l'arresto e l'avvio dell'istanza. In questo modo, non è necessario eseguire queste azioni manualmente.

> **Note**
>
> Per automatizzare le azioni per le tue EC2 istanze Amazon, le istanze devono essere gestite da Systems Manager.

Per ulteriori informazioni, consulta Automating Amazon EC2 with EventBridge nella Amazon EC2 User Guide.

Prerequisiti

È necessario creare una policy AWS Identity and Access Management (IAM), creare un ruolo IAM e aggiornare la policy di fiducia del ruolo prima di poter creare una regola.

Creazione di una policy IAM

Segui questa procedura per creare una policy gestita dal cliente per il tuo ruolo. Questa policy autorizza il ruolo a eseguire azioni per tuo conto. Questa procedura utilizza l'editor di policy JSON nella console IAM.

Per creare una policy IAM

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Policy.
3. Scegli Create Policy (Crea policy).
4. Scegliere la scheda JSON.
5. Copia il seguente codice JSON e sostituisci il codice JSON predefinito nell'editor.

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

```
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
  ]
}
```

a. Nel `Resource` parametro, per Amazon Resource Name (ARN), inserisci l'ID del tuo AWS account.

b. Puoi anche sostituire il nome del ruolo o utilizzare quello predefinito. Questo esempio usa *`AutomationEVRole`*.

6. Scegli Successivo: Tag.
7. (Facoltativo) Puoi aggiungere metadati alla policy collegando i tag come coppie chiave-valore.
8. Scegli Prossimo: Rivedi.
9. Nella pagina Rivedi la politica, inserisci un nome, ad *`AutomationEVRolePolicy`* esempio una descrizione facoltativa.
10. Consulta la pagina di riepilogo per vedere le autorizzazioni consentite dalla politica. Se sei soddisfatto della tua politica, scegli Crea politica.

Questa policy definisce le operazioni che questo ruolo può eseguire. Per ulteriori informazioni, consulta la pagina Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Creazione di un ruolo IAM

Dopo avere creato questa policy, devi creare un ruolo IAM e quindi collegare la policy a tale ruolo.

Per creare un ruolo per un AWS servizio

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio).
4. Scegli EC2il servizio a cui desideri consentire l'assunzione di questo ruolo.
5. Scegli Successivo: autorizzazioni.
6. Inserisci il nome della politica che hai creato, ad esempio*`AutomationEVRolePolicy`*, e quindi seleziona la casella di controllo accanto alla politica.
7. Scegli Successivo: Tag.
8. (Facoltativo) Puoi aggiungere metadati al ruolo collegando i tag come coppie chiave-valore.
9. Scegli Prossimo: Rivedi.
10. Per Nome ruolo, inserisci *`AutomationEVRole`*. Questo nome deve essere lo stesso nome che appare nell'ARN della policy IAM che hai creato.
11. (Facoltativo) In Role description (Descrizione ruolo), immettere una descrizione per il nuovo ruolo.
12. Rivedere il ruolo e scegliere Crea ruolo.

Per ulteriori informazioni, consulta Creating a role for an AWS service nella IAM User Guide.

Aggiorna la politica di fiducia

Infine, puoi aggiornare la politica di fiducia per il ruolo che hai creato. È necessario completare questa procedura per poter scegliere questo ruolo nella EventBridge console.

Per aggiornare la politica di attendibilità per il ruolo

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Nell'elenco dei ruoli del tuo AWS account, scegli il nome del ruolo che hai creato, ad esempio*AutomationEVRole*.
4. Selezionare la scheda Trust relationships (Relazioni di trust) e scegliere Edit trust relationship (Modifica relazione di trust).
5. Per Policy Document, copia il seguente codice JSON, rimuovi il criterio predefinito e incolla il codice JSON copiato al suo posto.

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

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

Per ulteriori informazioni, consulta Modifying a role trust policy (console) nella IAM User Guide.

Crea una regola per EventBridge

Segui questa procedura per creare una regola nella EventBridge console in modo da poter automatizzare l'arresto e l'avvio delle EC2 istanze il cui ritiro è programmato.

Per creare una regola EventBridge per le azioni automatizzate di Systems Manager

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel pannello di navigazione, in Events (Eventi), scegli Rules (Regole).
3. Nella pagina Crea regola, inserisci un nome e una descrizione per la regola.
4. In Define pattern (Definisci modello) scegliere Event pattern (Modello di evento), quindi selezionare Pre-defined pattern by service (Modello predefinito in base al servizio).
5. Per Service provider (Provider di servizi), selezionare AWS.
6. Per Nome del servizio, scegli Health.
7. Per Tipo di evento, scegli Specific Health events.
8. Scegli uno o più servizi specifici, quindi scegli EC2.
9. Scegli le categorie di tipi di eventi specifici, quindi scegli ScheduledChange.
10. Scegli i codici dei tipi di evento specifici, quindi scegli il codice del tipo di evento.

    Ad esempio, per le istanze EC2 supportate da Amazon EBS, scegli. **`AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED`** Per le EC2 istanze archiviate su istanze Amazon, scegli. **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**
11. Seleziona Qualsiasi risorsa.

    Il modello del tuo evento sarà simile al seguente esempio.

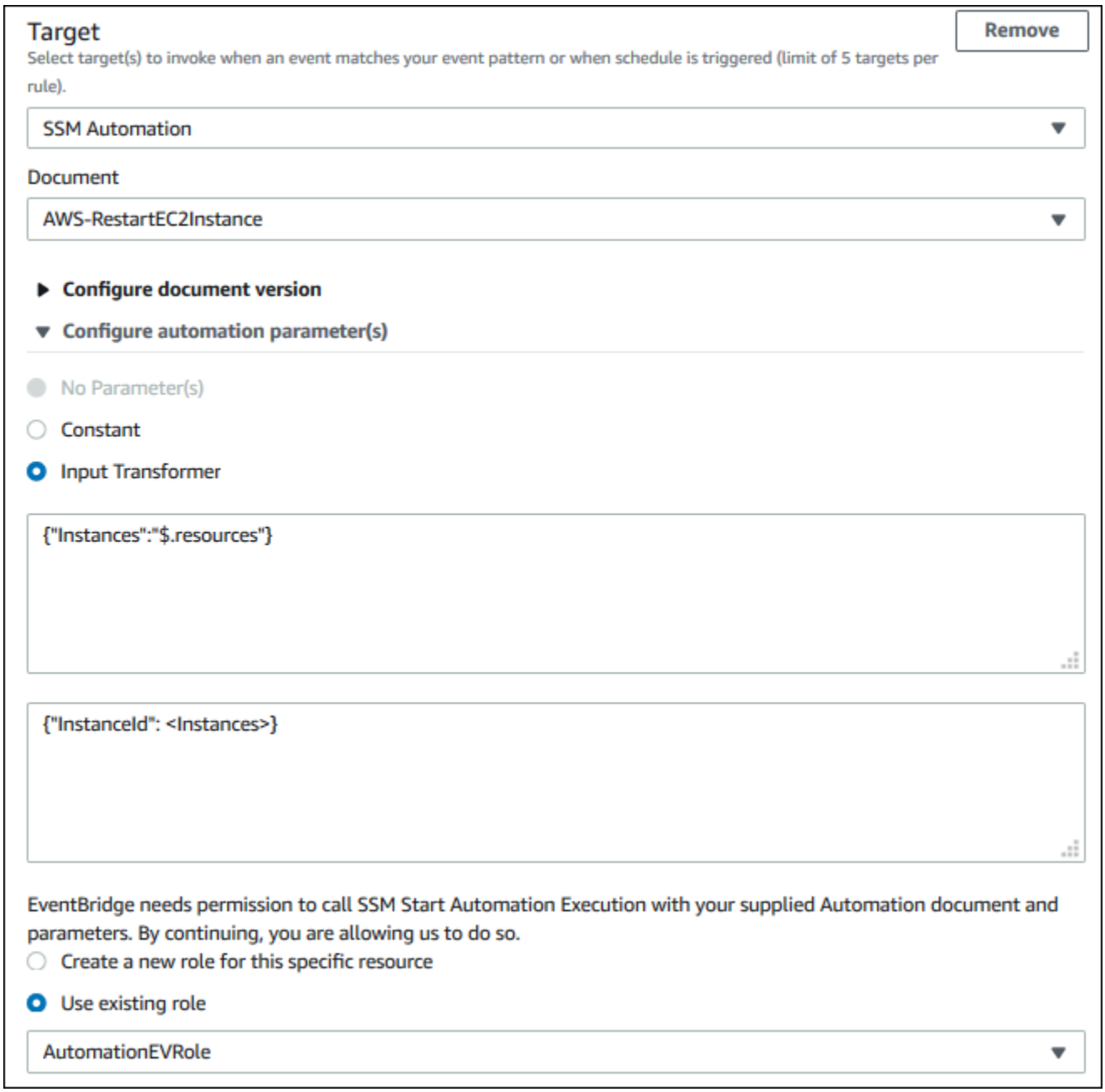
    Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
```

```
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. Aggiungere la destinazione del documento Systems Manager Automation. In Seleziona obiettivi, per Target, scegli SSM Automation.
13. Per Document (Documento), scegliere `AWS-RestartEC2Instance`.
14. Espandi i parametri di configurazione dell'automazione, quindi scegli Input Transformer.
15. Per il campo Input Path, inserisci**`{"Instances":"$.resources"}`**.
16. Per il secondo campo, immettere**`{"InstanceId": <Instances>}`**.
17. Scegli Usa il ruolo esistente, quindi scegli il ruolo IAM che hai creato, ad esempio*`AutomationEVRole`*.

    Il tuo obiettivo dovrebbe essere simile all'esempio seguente.



> **Note**
>
> Se non disponi di un ruolo IAM esistente con le autorizzazioni richieste EC2 e Systems Manager e la relazione di fiducia, il tuo ruolo non verrà visualizzato nell'elenco. Per ulteriori informazioni, consulta Prerequisiti.

18. Scegli Create (Crea) .

Se si verifica un evento nel tuo account che corrisponde alla tua regola, EventBridge invierà l'evento alla destinazione specificata.

Riferimento: Amazon EventBridge schema AWS Health degli eventi

Di seguito è riportato lo schema degli AWS Health eventi. Il contenuto del parametro details è riportato in una seconda tabella. I payload di esempio vengono forniti dopo le tabelle dello schema.

AWS Health schema degli eventi

AWS Health schema degli eventi

Parametro	Descrizione	Richiesto
versione	EventBridge versione, attualmente «0".	Sì
id	L'identificatore univoco dell' EventBridge evento.	Sì
tipo di dettaglio	Il tipo di dettaglio. Per AWS Health gli eventi, i valori supportati sono &AWS `Health Event` e `AWS Health Abuse Event`	Sì

Parametro	Descrizione	Richiesto
source (origine)	La fonte del bus degli eventi. Per AWS Health gli eventi, il valore supportato è `aws.health`	Sì

Parametro	Descrizione	Richiesto
account	L'ID dell'account a cui è stato inviato l'AWS Health evento. **Note** Per quanto riguarda l'organizzazione, si tratta di un account diverso dall'account interessato se è ricevuto nell'account di gestione o nell'account amministratore delegato.	Sì

Parametro	Descrizione	Richiesto
time	L'ora in cui è stata inviata la notifica a EventBridge. Formato:`yyyy-mm-ddThh:mm:ssZ` .	Sì

Parametro	Descrizione	Richiesto
Regione	Il Regione AWS destinatario a cui è stata recapitata la notifica. **Note** Questo campo non indica la regione interessata da questo AWS Health evento. Tali informazioni sono riportate in`detail.eventRegion`.	Sì

Parametro	Descrizione	Richiesto
resources	Descrive l'elenco delle eventuali risorse interessate all'interno di un account. Questo campo è vuoto se non ci sono risorse a cui si fa riferimento.	No
dettaglio	La sezione contenente i dettagli dell' AWS Health evento, come descritto nella tabella immediatamente successiva a questa.	Sì

Contenuto dello schema del parametro «details»

La tabella seguente documenta il contenuto del parametro detail nello schema degli AWS Health eventi.

AWS Health schema dell'evento: contenuto dettagliato del parametro

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
EventARN	L'identificatore univoco dell' AWS Health evento per la regione specifica, inclusi la regione e l'ID dell'evento. **Note** L'ARN di un evento non è esclusivo di una regione Account AWS o di una regione specifica.	Sì
service	Le Servizio AWS persone interessate dall' AWS Health evento. Ad esempio, Amazon EC2, Amazon Simple Storage Service, Amazon Redshift o Amazon Relational Database Service.	Sì
eventTypeCode	L'identificatore univoco per il tipo di evento. Ad esempio: `AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED` ed `AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED` . Gli eventi che includono `MAINTENANCE_SCHEDULED` vengono generalmente posticipati circa	Sì

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
	due settimane prima dell'orario di inizio. **Note** Tutti i nuovi eventi del ciclo di vita pianificati hanno lo stesso tipo di evento. `AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT`	
eventTypeCategory	Il codice della categoria dell'evento. I valori supportati includono`issue`, `accountNotification` `investigation` , e. `scheduledChange`	Sì
eventScopeCode	Indica se l' AWS Health evento è specifico dell'account o pubblico. I valori supportati sono `ACCOUNT_SPECIFIC` o `PUBLIC`.	Sì

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
ID di comunicazione	Un identificatore univoco per questa comunicazione relativa all'evento. AWS Health I messaggi con lo stesso ID di comunicazione potrebbero essere messaggi di backup o pagine di un singolo AWS Health evento. Questo identificatore può essere utilizzato con l'ID dell'account per aiutare a deduplicare i messaggi. Con il supporto per la paginazione AWS Health degli eventi, l'ID di comunicazione include il numero di pagina per mantenere l'ID di comunicazione univoco tra le pagine, ad esempio 12345678910-1. Per ulteriori informazioni, consulta Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge.	Sì
startTime	L'ora di inizio dell'evento, nel formato. AWS Health `DoW, DD, MMM, YYYY, HH:MM:SS TZ` L'orario di inizio può essere futuro per gli eventi programmati.	Sì

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
endTime	L'ora di fine dell' AWS Health evento, nel formato:`DoW, DD MMM YYYY HH:MM:SS TZ`. L'ora di fine non può essere fornita per gli eventi programmati per un periodo futuro.	No
lastUpdatedTime	L'ora dell'ultimo aggiornamento dell' AWS Health evento, nel formato`DoW, DD MMM YYYY HH:MM:SS TZ`.	Sì
Codice di stato	Lo stato dell'evento. AWS Health I valori supportati includono `open`, `closed`, `upcoming`.	Sì
EventRegion	La regione interessata descritta da questo AWS Health evento.	Sì

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
Descrizione dell'evento	Una sezione che descrive l' AWS Health evento. Ciò include campi per la lingua e il testo per descrivere l'evento. • lingua: il codice per la lingua utilizzata nell' AWS Health evento. Questo è in genere determinato dalla regione in cui viene pubblicato l'evento. Ad esempio, nella `us-east-1` regione, questo è in genere`en_US`. • LatestDescription: descrive l' AWS Health evento così come viene renderizzato dall' AWS Health API e in genere appare nella dashboard. AWS Health **Note** Per gli eventi pubblici, contiene solo l'ultimo aggiornamento e non l'intera cronologia dell'evento.	Sì

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
Metadati dell'evento	Metadati aggiuntivi dell'evento che possono essere forniti per l'evento. AWS Health • <metadata key 1>— Stringhe di coppie chiave-valore di metadati: «keystring1": «keyvalue1" Le coppie chiave-valore per i metadati degli eventi sono determinate dal servizio che ha inviato l'evento. AWS Health	No
Entità interessate	Un array che descrive il valore delle risorse e lo stato delle risorse interessate all'interno dell'evento. AWS Health • EntityValue: l'ID della risorsa/entità. • lastUpdatedTime: l'ora in cui lo stato di questa risorsa/entità è stato aggiornato l'ultima volta, nel formato. `DoW, DD MMM YYYY HH:MM:SS TZ` • status: lo stato della risorsa/entità interessata. I valori supportati includono `IMPAIRED`,,`UNIMPAIRED` , `PENDING` e. `RESOLVED` `UNKNOWN`	No

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
pagina	La pagina rappresentata da questo messaggio. Per ulteriori informazioni, consulta Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge. **Note** L'impaginazione avviene solo sulle risorse. Se il limite di dimensione di 256 KB viene superato per un altro motivo, la comunicazione avrà esito negativo.	Sì
Pagine totali	Il numero totale di pagine di questo evento sulla salute. Per ulteriori informazioni, consulta Visualizzazione di elenchi di eventi suddivisi in pagine su AWS Health EventBridge. È possibile utilizzare questo valore per determinare se sono state ricevute tutte le pagine di una comunicazione multipagina per un account.	Sì

contenuto del parametro 'dettaglio'	Descrizione	Richiesto
Account interessato	L'ID dell'account interessato. Questo valore può essere diverso dal valore nel `account` campo se questo evento sanitario viene inviato a un account che fa parte di un AWS Organizations e viene ricevuto nell'account di gestione o nell'account amministratore delegato.	Sì

Public Health Event - Problema EC2 operativo di Amazon


```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T09:01:22Z",
    "region": "af-south-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:af-south-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-d0179ed6d68f",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
        "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "statusCode": "open",
        "eventRegion": "af-south-1",
        "eventDescription": [{
```

```
            "language": "en_US",
            "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
        }],
        "affectedEntities": [],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

AWS Health Evento specifico dell'account - Problema dell'API Elastic Load Balancing

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-10T06:27:57Z",
    "region": "ap-southeast-2",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
        "service": "ELASTICLOADBALANCING",
        "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "ap-southeast-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "page": "1",
```

```
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

AWS Health Evento specifico dell'account: prestazioni ridotte di Amazon EC2 Instance Store Drive

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-03T06:27:57Z",
    "region": "us-west-2",
    "resources": [
        "i-abcd1111"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "affectedEntities": [{
            "entityValue": "i-abcd1111"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
```

```
}
```

Monitoraggio AWS Health

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Health altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per osservare AWS Health, segnalare quando qualcosa non va e intraprendere azioni laddove opportuno:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

  Puoi utilizzare Amazon EventBridge per ricevere notifiche sugli AWS Health eventi che potrebbero influire sui tuoi servizi e risorse. Ad esempio, se AWS Health pubblica un evento sulle tue EC2 istanze Amazon, puoi utilizzare queste notifiche per intervenire e aggiornare o sostituire le tue risorse secondo necessità. Per ulteriori informazioni, consulta Monitoraggio degli eventi AWS Health con Amazon EventBridge.
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente di .

Argomenti

- Registrazione delle chiamate AWS Health API con AWS CloudTrail

Registrazione delle chiamate AWS Health API con AWS CloudTrail

AWS Health è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in AWS Health. CloudTrail acquisisce le chiamate API AWS Health come eventi. Le chiamate acquisite includono chiamate dalla AWS Health console e chiamate di codice alle operazioni AWS Health API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Health Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella

cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata inviata AWS Health, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

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

AWS Health informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in AWS Health, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di AWS Health, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

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

Tutte le operazioni AWS Health API vengono registrate CloudTrail e documentate nell'AWS Health API Reference. Ad esempio, le chiamate alle `DescribeAffectedEntities` operazioni `DescribeEventsDescribeEventDetails`, e generano voci nei file di CloudTrail registro.

AWS Health supporta la registrazione delle seguenti azioni come eventi nei file di CloudTrail registro:

- Se la richiesta è stata effettuata con credenziali root o IAM
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.

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

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Puoi archiviare i tuoi file di log nel tuo bucket Amazon S3 per tutto il tempo che desideri. Puoi anche definire regole del ciclo di vita di Amazon S3 per archiviare o eliminare file di log automaticamente. Per impostazione predefinita, i file di log sono crittografati mediante la crittografia lato server (SSE) di Amazon S3.

Per ricevere una notifica al momento della consegna dei file di log, puoi CloudTrail configurare la pubblicazione di notifiche Amazon SNS quando vengono consegnati nuovi file di log. Per ulteriori informazioni, consulta l'argomento relativo alla configurazione delle notifiche Amazon SNS per CloudTrail.

Puoi anche aggregare i file di AWS Health log di più AWS regioni e più AWS account in un unico bucket Amazon S3.

Per ulteriori informazioni, consulta le pagine relative alla ricezione di file di log di CloudTrail da più regioni e ricezione di file di log di CloudTrail da più account.

Esempio: AWS Health voci dei file di registro

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

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'DescribeEntityAggregatesoperazione.

```
{
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
```

```
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

Cronologia dei documenti per AWS Health

La tabella seguente descrive la documentazione per questa versione di AWS Health.

- Versione API: 04-08-2016

La tabella seguente descrive importanti aggiornamenti alla AWS Health documentazione, a partire dal 28 agosto 2020. Puoi ora iscriverti a un feed RSS per ricevere notifiche sugli aggiornamenti.

Modifica	Descrizione	Data
Sezione aggiornata: Abilitazione della visualizzazione organizzativa	Sono state aggiunte informazioni alla sezione Note che indicano che aggrega AWS Health automaticamente tutti gli eventi sanitari storici dell'organizzazione quando si abilita la visualizzazione organizzativa. Gli eventi storici potrebbero richiedere fino a 24 ore per essere visualizzati nella visualizzazione organizzativa. Per ulteriori informazioni, consulta Attivazione della visualizzazione organizzativa	27 giugno 2025
Sezione aggiornata: aggregazione degli AWS Health eventi tra gli account	Nota rimossa che AWS Health non mostra gli eventi che si sono verificati prima dell'attivazione della visualizzazione organizzativa. Per ulteriori informazioni, consulta Aggregazione di AWS Health eventi tra account	27 giugno 2025
WorkDocs obsoleta	Sono stati rimossi i riferimenti agli eventi obsoleti del ciclo di	19 giugno 2025

	vita WorkDocs pianificato per. AWS Health	
È stata aggiunta una nota per la cronologia della migrazione delle notifiche AWS gestite	È stata aggiunta una nota relativa alle date chiave per la migrazione delle e-mail alle notifiche AWS gestite in Notifiche all'utente AWS. Per ulteriori informazioni, consulta Gestire AWS Health le notifiche in Notifiche all'utente AWS.	28 aprile 2025
Eventi del ciclo di vita pianificati aggiornati	Eventi del ciclo di vita pianificati aggiornati per indicare che AWS Health gli eventi rimangono aperti per 4 anni anziché 90 giorni per le risorse non risolte. Per ulteriori informazioni, consulta la sezione Cosa devo aspettarmi quando ricevo una notifica di un evento relativo al ciclo di vita pianificato? sezione in Eventi del ciclo di vita pianificati per. AWS Health	18 aprile 2025

È stata aggiornata la descrizione dell'elenco delle risorse interessate per gli eventi del ciclo di vita pianificati	L'elenco delle risorse interessate per gli eventi del ciclo di vita pianificati viene in genere aggiornato una volta ogni 24 ore, ma potrebbero essere necessarie fino a 72 ore per riflettere lo stato attuale delle risorse. Per ulteriori informazioni, consulta la sezione Dettagli dell'evento in Visualizzazione degli eventi dell'account nella dashboard. AWS Health	7 aprile 2025
Aggiunta una FAQ per la gestione delle AWS Health notifiche in Notifiche all'utente AWS	Per ulteriori informazioni, consulta Gestire le notifiche nelle Notifiche all'utente AWS domande frequenti.	18 febbraio 2025
Sono state aggiunte informazioni relative alle richieste IPv6 - only agli endpoint.	Per ulteriori informazioni, consulta Scelta degli endpoint per le AWS Health richieste API.	28 gennaio 2025
Gestisci le AWS Health notifiche in Notifiche all'utente AWS	Per ulteriori informazioni, consulta Gestire le notifiche in Notifiche all'utente AWS.	16 gennaio 2025
JSON corretto nel monitoraggio AWS Health degli eventi con Amazon EventBridge	Per ulteriori informazioni, consulta Monitoraggio AWS Health degli eventi con Amazon EventBridge.	3 settembre 2024
Informazioni aggiornate sul download delle risorse interessate	Per ulteriori informazioni, consulta Visualizzazione delle risorse interessate.	27 luglio 2024

È stata rimossa la privacy del traffico Internet dalla documentazione della sezione Sicurezza AWS Health	Per ulteriori informazioni, consulta Sicurezza in AWS Health.	27 marzo 2024
Aggiornamento della AWS Health dashboard: stato del servizio ed eventi del ciclo di vita pianificato per la documentazione. AWS Health	Per ulteriori informazioni, consulta AWS Health Dashboard: stato del servizio ed eventi pianificati del ciclo di vita per. AWS Health	15 febbraio 2024
È stato rimosso un bullet point duplicato in Creazione EventBridge di una regola per AWS Health	È stato rimosso un bullet point duplicato in Creazione di EventBridge una regola per. AWS Health	4 dicembre 2023
È stata aggiunta documentazione per gli eventi del ciclo di vita pianificato	Per ulteriori informazioni, vedere Planned Lifecycle Events for. AWS Health	31 ottobre 2023
Documentazione per `AWSHealthFullAccess` aggiornata	È ora possibile utilizzare la politica `AWSHealthFullAccess` gestita in AWS GovCloud (US) Regions. Vedi le politiche AWS gestite per AWS Health.	16 ottobre 2023
È stata aggiunta la documentazione per la configurazione delle notifiche AWS utente in AWS Health.	Ora puoi configurare le notifiche AWS utente in AWS Health. Per ulteriori informazioni, consulta Configurare le notifiche AWS utente per AWS Health.	30 agosto 2023

È stata aggiunta la documentazione per la funzionalità di amministratore delegato alla sezione Aggregazione AWS Health degli eventi.	Per ulteriori informazioni, consulta Visualizzazione organizzativa dell'amministratore delegato.	27 luglio 2023
Aggiornamento della politica SLR	Aggiornamento della politica AWS gestita: OrganizationsServiceRolePolicy Health_. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Health.	19 luglio 2023
AWS Health lo schema ora supporta i metadati degli eventi	Ora puoi ricevere i metadati degli eventi dagli AWS Health eventi. Per ulteriori informazioni, consulta Monitoraggio AWS Health degli eventi con Amazon EventBridge.	20 giugno 2023
Documentazione aggiornata per Amazon EventBridge	Ora puoi utilizzare una EventBridge regola Amazon per monitorare sia gli eventi specifici dell'account che quelli pubblici. Per ulteriori informazioni, consulta Monitoraggio AWS Health degli eventi con Amazon EventBridge.	2 maggio 2023
È stata aggiunta documentazione per le politiche AWS gestite	È stata aggiunta documentazione per le politiche AWS gestite per AWS Health e l'utilizzo dei ruoli collegati ai servizi per. AWS Health	18 gennaio 2023

È stata aggiunta la documentazione sull'impostazione del fuso orario	Utilizza la nuova funzionalità del fuso orario per visualizzare la AWS Health Dashboard nel fuso orario locale o in UTC. Per ulteriori informazioni, vedi Guida introduttiva alla AWS Health Dashboard — Stato dell'account e AWS Health Dashboard — Stato del servizio.	21 settembre 2022
Documentazione aggiornata	È stata aggiunta documentazione per AWS Health Aware. Per ulteriori informazioni, vedere AWS Health Aware.	25 maggio 2022
Documentazione aggiornata	The Service Health Dashboard and the AWS Personal Health Dashboard sono stati rinominati Dashboard. AWS Health Per ulteriori informazioni, vedi Guida introduttiva alla AWS Health dashboard - Stato dell'account e AWS Health Dashboard - Stato del servizio.	28 febbraio 2022
Documentazione aggiornata per Amazon EventBridge	Nuovo argomento per AWS Health utilizzare Amazon per EventBridge monitorare e gli eventi Health. Per ulteriori informazioni, consulta Monitoraggio AWS Health degli eventi con Amazon EventBridge.	3 febbraio 2022

Documentazione aggiornata	Se disponi di un piano Enterprise On-Ramp Support, puoi utilizzare l' AWS Health API.	24 novembre 2021
Documentazione aggiunta	Nuovo argomento per AWS Health i concetti. Per ulteriori informazioni, vedere Concetti per AWS Health.	29 luglio 2021
Documentazione aggiornata per CloudWatch gli eventi	È stata aggiunta una sezione su come creare una regola per più servizi e categorie di tipi di eventi. Per ulteriori informazi oni, vedere Creazione di una regola per più servizi e categorie.	7 maggio 2021
Documentazione aggiornata per CloudWatch gli eventi	È stata aggiornata la sezione per automatizzare AWS Systems Manager le azioni per le regole di Amazon CloudWatch Events. Per ulteriori informazioni, consulta Automazione delle azioni per le EC2 istanze Amazon.	28 Aprile 2021
Documentazione aggiornata per gli eventi CloudWatch	È stata aggiunta una sezione per ricevere AWS Health eventi nel client di chat. Per ulteriori informazioni, consulta Ricezione di AWS Health eventi con Amazon Q Developer nelle applicazioni di chat.	16 marzo 2021

Documentazione aggiornata	I seguenti argomenti sono stati aggiornati: • È stato aggiornato l'argomento Aggregazione AWS Health degli eventi • Riorganizzato e aggiornato l'argomento Monitor for AWS Health events with Amazon CloudWatch Events • È stata aggiornata la sezione Condizioni basate su risorse e azioni	29 gennaio 2021
È stata aggiunta la AWS Health dashboard per la visualizzazione organizzativa nella console AWS Health	È possibile utilizzare la AWS Health console per abilitare la funzionalità di visualizzazione organizzativa. È quindi possibile visualizzare gli eventi sanitari relativi agli account dei membri AWS della propria organizzazione.	14 dicembre 2020
Demo degli endpoint ad alta disponibilità	È possibile utilizzare il codice di esempio per determinare l'endpoint regionale attivo e la AWS regione di firma per. AWS Health	22 ottobre 2020
Aggiornamenti alla Guida per l'AWS Health utente	L'organizzazione si aggiorna e ha aggiunto un feed RSS in modo da poter sottoscrivere gli ultimi aggiornamenti della AWS Health documentazione.	28 agosto 2020

Aggiornamenti precedenti

Modifica	Descrizione	Data
Aggiornato l'argomento della vista organizzativa per includere esempi.	Consultare Aggregazione di AWS Health eventi tra account.	3 giugno 2020
Sicurezza e AWS Health	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di AWS Health. Consultare Sicurezza in AWS Health.	5 maggio 2020
Aggiunta una nuova sezione per spiegare come utilizzare la visualizzazione organizzativa per gli eventi aggregati tra tutti gli account in AWS Organizat ions.	Consultare Aggregazione di AWS Health eventi tra account.	18 dicembre 2019
È stata aggiunta una nuova sezione «Condizioni basate su risorse e azioni» per spiegare le restrizioni sugli eventi fornite dall'API. AWS Health	Consultare Gestione delle identità e degli accessi per l' AWS Health.	2 agosto 2018
È stata aggiunta una nota sulla visibilità delle informazi oni. AWS Health	Consultare Gestione delle identità e degli accessi per l' AWS Health.	16 agosto 2017
Release del servizio.	AWS Health rilasciato.	1° dicembre 2016

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.