aws

Guida per l'utente

AWS Health

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Health: Guida per l’utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l’immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è AWS Health? 1
Concetti per AWS Health 2
AWS Health evento 2
Account-specific evento 3
Evento pubblico 3
AWS Health Pannello di controllo 3
AWS Health Dashboard — Stato del servizio 4
Codice del tipo di evento 4
Categorie di tipi di eventi 4
Stato dell'evento 6
Azionabilità 6
Personaggi 7
Entità interessate 7
AWS Health eventi su Amazon EventBridge 8
AWS Health "Hello, World!" 8
Visualizzazione organizzativa 8
Notifiche AWS agli utenti 9
Nozioni di base 10
Registrati per un Account AWS 10
Visualizza gli eventi dell'account in AWS Health Dashboard 11
Problemi aperti e recenti 11
Modifiche pianificate 13
Altre notifiche 13
Log degli eventi 13
Dettagli dell'evento 14
Tipi di eventi 16
Visualizzazione del calendario 17
Visualizzazione delle risorse interessate 18
Impostazioni del fuso orario 19
Lo stato della tua organizzazione 19
Avvisi per AWS Health eventi 20
Configurazione di Amazon EventBridge 21
Gestisci le notifiche in Notifiche AWS agli utenti 21
Configura il tuo AWS abbonamento alle notifiche gestite per AWS Health eventi 22

AWS Domande frequenti sulle notifiche gestite ... 23
AWS Health Pannello di controllo ... 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 ... 31
Accesso agli eventi pianificati del ciclo di vita ... 32
Catalogo delle versioni per AWS Health ... 33
Cos'è il catalogo delle versioni? ... 33
Cosa puoi fare con il catalogo delle versioni ... 34
Come accedere al catalogo delle versioni ... 34
Dettagli disponibili nel catalogo delle versioni ... 35
Top-level immissione della versione ... 35
Oggetto evento del ciclo di vita ... 35
Impact-risk tag ... 36
Come recuperare le informazioni del catalogo delle versioni con l'API ... 36
Come visualizzare il catalogo delle versioni nel Dashboard Health ... 37
Integrazione con altri sistemi tramite l'API AWS Health ... 39
Firma AWS Health Richieste API ... 40
Scelta degli endpoint per AWS Health Richieste API ... 40
Demo: recupero programmatico dei dati degli ultimi sette giorni degli eventi ... 42
Demo: recupero degli ultimi sette giorni di AWS Health dati sugli eventi utilizzando Java ... 42
Demo: recupero degli ultimi sette giorni di AWS Health dati sugli eventi usando Python ... 45
Tutorial: Utilizzo del AWS Health API con esempi in Java ... 48
Fase 1: inizializzare le credenziali ... 48
Fase 2: Inizializzare un AWS Health Client API ... 49
Fase 3: Utilizzo AWS Health Operazioni API per ottenere informazioni sugli eventi ... 49
Sicurezza ... 53
Protezione dei dati ... 54
Crittografia dei dati ... 55
Gestione dell'identità e degli accessi ... 55
Destinatari ... 56
Autenticazione con identità ... 56
Gestione dell'accesso tramite policy ... 57
In che modo AWS Health funziona con IAM ... 59

Identity-based esempi di politiche 65
Risoluzione dei problemi 78
Uso di ruoli collegati ai servizi 81
AWS politiche gestite per AWS Health 83
Registrazione e monitoraggio AWS Health 90
Convalida della conformità 90
Resilienza 91
Sicurezza dell'infrastruttura 91
Analisi della configurazione e delle vulnerabilità 92
Best practice di sicurezza 92
Grant AWS Health autorizzazioni minime possibili per gli utenti 92
Visualizza il Dashboard Health 92
Integra AWS Health con Amazon Chime o Slack 92
Monitor per AWS Health eventi 92
Aggregazione di eventi AWS Health 94
Prerequisiti 94
Abilitazione della visualizzazione organizzativa 95
Visualizzazione della vista organizzativa 99
Disabilitazione della visualizzazione organizzativa 104
Gestione delle viste degli amministratori delegati per un'organizzazione 105
Registrazione di un account amministratore delegato 106
Rimozione di un account amministratore delegato 107
Monitoraggio degli eventi sanitari con EventBridge 108
Creazione di EventBridge regole per Regione AWS copertura 109
Configurazione ad alta disponibilità (opzionale) 110
Integrazione semplificata 110
Eventi globali 110
Monitoraggio di eventi pubblici e specifici per account per AWS Health 111
Regole di backup per AWS Health eventi 111
Visualizzazione di elenchi suddivisi in pagine di AWS Health eventi in corso EventBridge 112
Aggregazione AWS Health eventi che utilizzano la visualizzazione organizzativa e l'accesso amministratore delegato 113
Integrazione AWS Health monitoraggio e notifiche degli eventi con JIRA e ServiceNow 113
Configurazione di una EventBridge regola per inviare notifiche sugli eventi 114
Utilizzando l'API o AWS Command Line Interface 114

Configurazione di Amazon Q Developer nelle applicazioni di chat per inviare notifiche sugli eventi 116
Prerequisiti 117
Esecuzione automatica delle operazioni sulle istanze EC2 in risposta agli eventi 119
Prerequisiti 119
Crea una regola per EventBridge 123
Riferimento: AWS Health eventi Amazon EventBridge schema 126
AWS Health schema evento 126
Evento sulla salute pubblica - Problema operativo di Amazon EC2 141
Account-specific AWS Health Evento - Problema con l'API Elastic Load Balancing 142
Account-specific AWS Health Evento: evento di backup per Amazon EC2 Instance Store Drive con prestazioni ridotte 143
Account-specific AWS Health Evento: ritiro dell'istanza Amazon EC2 144
Account-specific AWS Health Evento - Evento sul ciclo di vita pianificato Lambda 145
Monitoraggio AWS Health 147
Registrazione dei log AWS Health Chiamate API con AWS CloudTrail 147
AWS Health informazioni in CloudTrail 148
Esempio: AWS Health voci del file di log 149
Domande frequenti sui protocolli supportati 151
Quali sono i AWS Protocolli CBOR JSON e Smithy RPC v2, e in cosa differiscono? 151
Come posso iniziare a usare il protocollo CBOR Smithy RPC v2? 151
Quali sono i rischi dell'abilitazione del protocollo Smithy RPC v2 CBOR? 152
Cosa succede se la mia soluzione non supporta Smithy RPC v2 CBOR? 152
What AWS Le regioni supportano il protocollo Smithy RPC v2 CBOR? 152
Quali miglioramenti della latenza posso aspettarmi dall'aggiornamento alle versioni SDK che supportano Smithy RPC v2 CBOR? 153
Sarà il AWS Il protocollo JSON sarà obsoleto? 153
Dove posso trovare ulteriori informazioni su Smithy RPC v2 CBOR? 153
Cronologia dei documenti 154
Aggiornamenti precedenti 168
..... clxix

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, chiamata 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l' AWS Health API per l'integrazione con sistemi interni e di terze parti. Se utilizzi un piano Regione AWS che non offre uno di questi Supporto AWS piani o se non sei passato a uno di questi piani, puoi utilizzare l' AWS Health API con un piano Business On-Ramp, Enterprise o Enterprise Support. Per ulteriori informazioni, consulta la documentazione di riferimento dell'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 puoi utilizzare il servizio per mantenere l'integrità delle tue applicazioni, servizi e risorse nel tuo Account AWS.

Argomenti

- AWS Health evento
- AWS Health Pannello di controllo
- Codice del tipo di evento
- Categorie di tipi di eventi
- Stato dell'evento
- Azionabilità
- Personaggi
- Entità interessate
- AWS Health eventi su Amazon EventBridge
- AWS Health "Hello, World!"
- Visualizzazione organizzativa
- Notifiche AWS agli utenti

AWS Health evento

AWS Health gli eventi, noti anche come eventi sanitari, 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 può inviare un evento se AWS Identity and Access Management (IAM) prevede di deprecare una policy gestita o AWS Config prevede di deprecare una regola gestita. AWS Health invia anche eventi in caso di problemi di disponibilità del servizio in un. Regione AWSÈ possibile rivedere la descrizione dell'evento per comprendere il problema, identificare le risorse interessate e intraprendere le azioni consigliate.

Esistono due tipi di eventi sulla salute:

Indice

- Account-specific evento
- Evento pubblico

Account-specific evento

Account-specific gli eventi sono locali per il tuo account Account AWS o per un account AWS della tua organizzazione. 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 sul nome delle risorse interessate.

Puoi trovare eventi specifici dell'account dalla tua AWS Health dashboard, dall'AWS Health API o utilizzare Amazon EventBridge o le notifiche AWS degli utenti per ricevere notifiche .

Evento pubblico

Gli eventi pubblici sono eventi di servizio segnalati che non sono specifici di un account. Ad esempio, in caso di problemi 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 intervenire su di esse.

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

> **Important**
>
> Gli eventi pubblici non sono disponibili tramite notifiche AWS gestite in Notifiche AWS agli utenti. Per ricevere eventi pubblici, devi creare una EventBridge regola Amazon o una User-configured notifica (UCN) all'interno Notifiche AWS agli utenti. Per ulteriori informazioni, consulta Monitoraggio degli eventi in AWS Health con Amazon EventBridge e Gestire le notifiche in Notifiche AWS agli utenti.

Se hai un account, consultaPer iniziare con il tuo AWS Health Dashboard.

Se non disponi di un account, consulta AWS Health Pannello di controllo.

AWS Health Pannello di controllo

Se ne hai uno 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, ad esempio un imminente problema di manutenzione di un servizio in una regione. Puoi anche utilizzare la AWS Health Dashboard per conoscere gli eventi che potrebbero interessarti direttamente, ad esempio una risorsa obsoleta nel tuo account.

Puoi accedere a per visualizzare la tua AWS Health dashboard Console di gestione AWS all'indirizzo. https://health.aws.amazon.com/health/home

Per ulteriori informazioni, consulta Per iniziare con il tuo AWS Health Dashboard.

AWS Health Dashboard — Stato del servizio

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

Per ulteriori informazioni, consulta AWS Health Pannello di controllo.

Codice del tipo di evento

I codici del tipo di evento visualizzati in un evento Health includono il servizio interessato e il tipo di evento. Ad esempio, se ricevi un evento sanitario con il codice del tipo di `AWS_EC2_SYSTEM_MAINTENANCE_EVENT` evento, significa che il servizio sta programmando 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 eventi

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 il `AWS_RDS_MAINTENANCE_SCHEDULED` codice. In questo esempio, la categoria è pianificata. È possibile utilizzare queste informazioni per comprendere le categorie di eventi ad alto livello.

È consigliabile monitorare tutte le categorie di tipi di eventi. Nota che ogni categoria viene visualizzata per diversi tipi di eventi. Puoi anche utilizzare l'operazione DescribeEventTypes API 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 dell'utente. Questi eventi potrebbero essere informativi o richiedere un'azione urgente da parte dell'utente. 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 dei tipi 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 sui AWS servizi o sulle risorse. Gli eventi più comuni in questa categoria includono comunicazioni su problemi operativi che causano il degrado del servizio o problemi localizzati a livello di risorse per la sensibilizzazione dell'utente.

Di seguito sono riportati alcuni esempi di codici di tipo 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 risorse di Amazon Elastic Block Store (Amazon EBS).
- `AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT`— Questo evento indica che il tuo account potrebbe essere sospeso se non intraprendi alcuna azione.

Modifica programmata

Questi eventi forniscono informazioni sulle modifiche imminenti ai tuoi servizi e alle tue risorse. Questi eventi includono eventi pianificati del ciclo di vita, ad esempio notifiche di fine supporto e aggiornamenti automatici per diverse versioni. Alcuni eventi potrebbero suggerire 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 di 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'istanza Amazon EC2 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 evento di fine del supporto per una delle sue versioni, che richiede l'intervento del cliente.

> **Tip**
>
> Se utilizzi l' AWS Health API o la AWS Command Line Interface (AWS CLI) per restituire i dettagli dell'evento, l'`Event`oggetto contiene il campo con il valore. `eventScopeCode` `ACCOUNT_SPECIFIC` Per ulteriori informazioni, consulta la documentazione di riferimento dell'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 sulla salute nel AWS Health dashboard o nell' AWS Health API per un massimo di 90 giorni.

Azionabilità

L'azionabilità è un campo che ti aiuta a dare priorità agli eventi sanitari in base al fatto che sia richiesta un'azione da parte tua. Gli eventi sanitari includono uno stato di fattibilità che indica se è necessario intervenire per mitigare i rischi per AWS le risorse o se l'evento è di natura informativa.

Il campo di azionabilità può contenere uno dei seguenti valori:

- `ACTION_REQUIRED`: gli eventi con questo stato richiedono un'azione da parte tua per mitigare il potenziale impatto legato alla disponibilità, alla fatturazione o alla sicurezza delle tue risorse. AWS

- `ACTION_MAY_BE_REQUIRED`: gli eventi con questo stato indicano le modifiche che richiedono un'azione, in base all'implementazione, alle dipendenze e ai flussi di lavoro specifici. Questi eventi richiedono una revisione per determinare se è necessaria un'azione.
- `INFORMATIONAL`: gli eventi con questo stato forniscono una visibilità continua delle informazioni operative sui AWS servizi che utilizzi. Non è prevista alcuna azione immediata.

> **Note**
>
> Gli eventi relativi allo stato di salute relativi ai problemi di servizio non includono un'etichetta di fattibilità, poiché la necessità di azioni di ripristino dipende dalla specifica architettura dell'applicazione.

Personaggi

Il campo personas fornisce un elenco di contatti che consente di indirizzare le informazioni pertinenti ai team appropriati all'interno dell'organizzazione. Ogni evento Health può includere una o più delle seguenti persone:

- `OPERATIONS`: Per eventi legati alle attività operative e alla disponibilità del servizio.
- `SECURITY`: per eventi legati a considerazioni sulla sicurezza.
- `BILLING`: Per eventi con potenziali implicazioni in termini di costi.

Ad esempio, quando AWS invia un evento sulla fine del supporto standard che viene convertito in supporto esteso, l'evento include anche `BILLING` nell'elenco delle persone per `OPERATIONS` garantire che le informazioni raggiungano i team responsabili della gestione dei costi.

Entità interessate

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

AWS Health eventi su Amazon EventBridge

Puoi configurare EventBridge le regole di Amazon per i tuoi account per automatizzare le azioni dopo la ricezione dell' AWS Health evento appropriato da parte di un account. Queste possono essere azioni generiche, come l'invio di tutti i messaggi relativi agli eventi del ciclo di vita pianificati 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 in AWS Health con Amazon EventBridge.

AWS Health "Hello, World!"

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

- Ottieni informazioni sugli eventi che potrebbero influire sui tuoi AWS servizi e sulle tue 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 eventi e codici di tipo di evento

Per ulteriori informazioni, consulta la documentazione di riferimento dell'API di AWS Health.

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

Visualizzazione organizzativa

Puoi utilizzare questa funzionalità per aggregare tutti gli eventi relativi allo stato di salute dei tuoi AWS account AWS Organizations in un'unica visualizzazione 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. Puoi abilitare questa

funzionalità dalla AWS Health console o dall'API. Per ulteriori informazioni, consulta Aggregazione AWS Health eventi tra gli account.

Notifiche AWS agli utenti

AWS Health si integra con Notifiche AWS agli utenti in modo da poter ricevere e controllare facilmente le notifiche sugli eventi che riguardano l'utente Account AWS e i servizi. Notifiche agli utenti offre notifiche gestite per AWS Health gli eventi per impostazione predefinita. Puoi configurare questi abbonamenti per controllare la frequenza con cui ricevi i 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 agli utenti in. Console di gestione AWS Per ulteriori informazioni, consulta Manage (Gestione) AWS Health notifiche in Notifiche AWS agli utenti

Per iniziare con il tuo AWS Health Dashboard

Puoi usare il tuo AWS Health Dashboard per saperne di più AWS Health eventi. Questi eventi possono influire sul tuo Servizi AWS o Account AWS. Dopo aver effettuato l'accesso al tuo account, AWS Health La 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.
- Gli 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 disponi di un Account AWS, puoi usare AWS Health Pannello di controllo per informazioni sulla disponibilità generale del servizio.
> Se hai un account, ti consigliamo di accedere al tuo AWS Health Dashboard per ottenere informazioni più approfondite sugli eventi e sulle modifiche imminenti che potrebbero influire sui tuoi servizi e sulle tue risorse.

Argomenti

- Registrati per un Account AWS
- Visualizzazione degli eventi del tuo account nel AWS Health Dashboard
- Configurazione di Amazon EventBridge
- Manage (Gestione) AWS Health notifiche in Notifiche AWS agli utenti

Registrati per un Account AWS

Per iniziare con AWS, hai bisogno di un Account AWS. Ci sono due modi per iscriversi AWS.
Se desideri il controllo completo sulla configurazione dell'account e su dove sono archiviati i tuoi contenuti, o se hai carichi di lavoro regolamentati come HIPAA o FedRAMP, usa Iscriviti a AWS

(avanzato). Se sei un nuovo utente e desideri utilizzare un login che possiedi già AWS e crea un AWS ambiente con impostazioni preconfigurate in select Regioni AWS, usa Iscriviti per AWS.

Visualizzazione degli eventi del tuo account nel AWS Health Dashboard

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

Per visualizzare gli eventi dell'account nel tuo AWS Health Dashboard

1. Apri il tuo AWS Health Dashboard all'indirizzo https://health.aws.amazon.com/health/home.
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 programmate — Visualizza i prossimi eventi che potrebbero influire sui tuoi servizi e sulle tue 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 degli eventi — Visualizza tutti gli eventi degli ultimi 90 giorni.

Problemi aperti e recenti

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

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

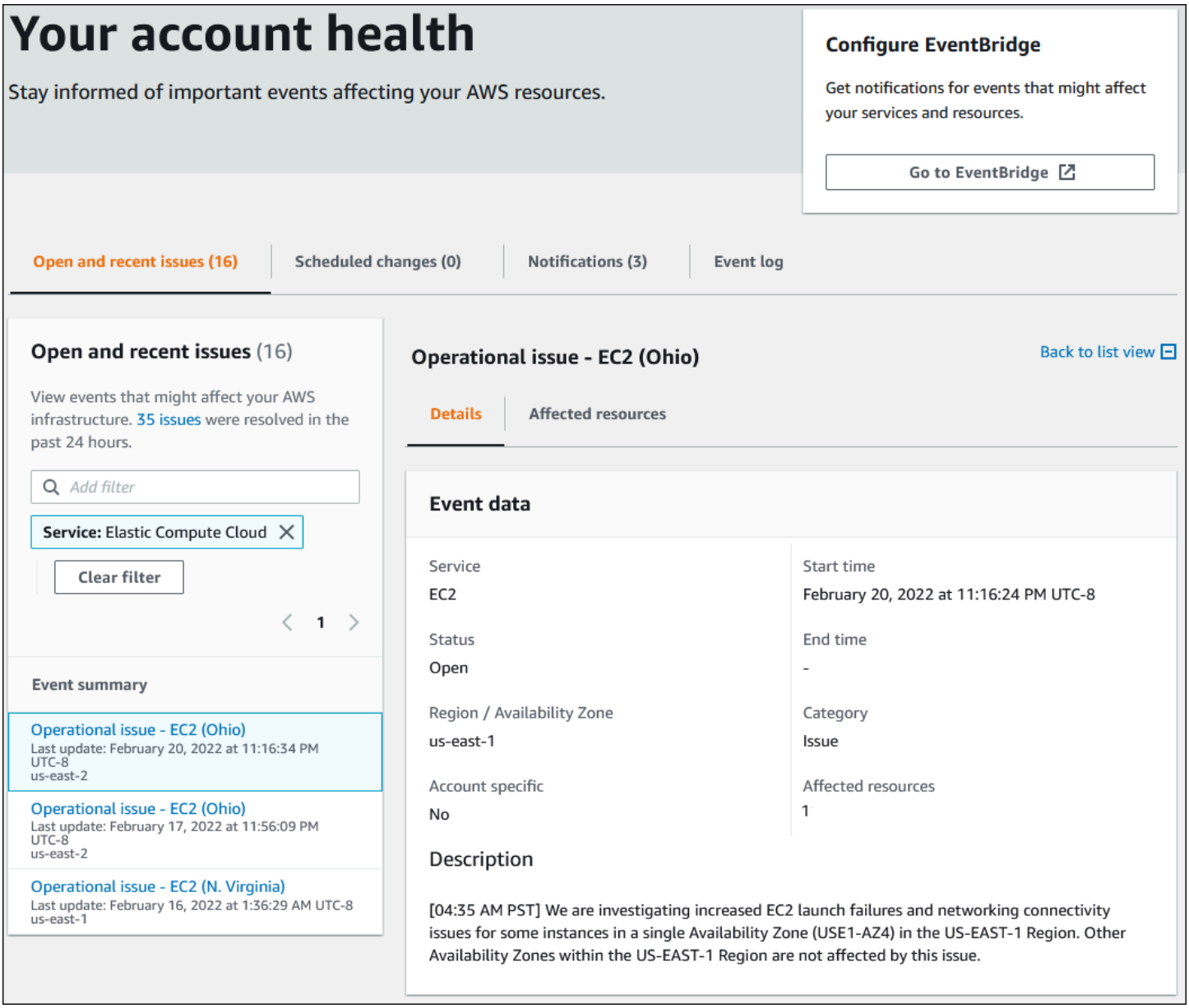
È possibile filtrare gli eventi visualizzati in qualsiasi scheda scegliendo le opzioni dall'elenco dei filtri. Ad esempio, puoi restringere i risultati per Zona di disponibilità, Regione, ora di fine dell'evento o ora dell'ultimo aggiornamento, Servizio AWS e così via.

Per vedere tutti gli eventi, anziché quelli recenti che appaiono nella dashboard, scegli Log degli eventi scheda.

> **Note**
>
> Al momento, non puoi eliminare le notifiche per gli eventi che appaiono nel tuo AWS Health Dashboard. Dopo un Servizio AWS risolve un evento, la notifica viene rimossa dalla visualizzazione del pannello di controllo.

Example: Evento relativo a problemi operativi per Amazon Elastic Compute Cloud (Amazon EC2)

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



Modifiche pianificate

Usa il Modifiche pianificate scheda per visualizzare i prossimi eventi che potrebbero influire sul tuo account. Questi eventi possono includere attività di manutenzione programmata per i servizi ed eventi del ciclo di vita pianificati che richiedono un'azione per essere risolti. Per facilitare la pianificazione di queste attività, viene fornita una visualizzazione del calendario in cui è possibile mappare le modifiche pianificate in un calendario mensile. I filtri sono disponibili. Per ulteriori informazioni sugli eventi del ciclo di vita pianificati, vedere Eventi del ciclo di vita pianificati per AWS Health.

Altre notifiche

Usa il Notifiche scheda 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 di certificati, notifiche di fatturazione e vulnerabilità di sicurezza.

Log degli eventi

Usa il Registro eventi scheda per visualizzare tutto AWS Health eventi. La tabella di registro include colonne aggiuntive in modo da poter filtrare per Stato e Ora di inizio.

Quando scegli un evento nel Registro degli eventi tavolo, il Dettagli viene visualizzato un riquadro con le informazioni sull'evento e l'elenco delle risorse interessate. Per ulteriori informazioni, consulta Dettagli dell'evento.

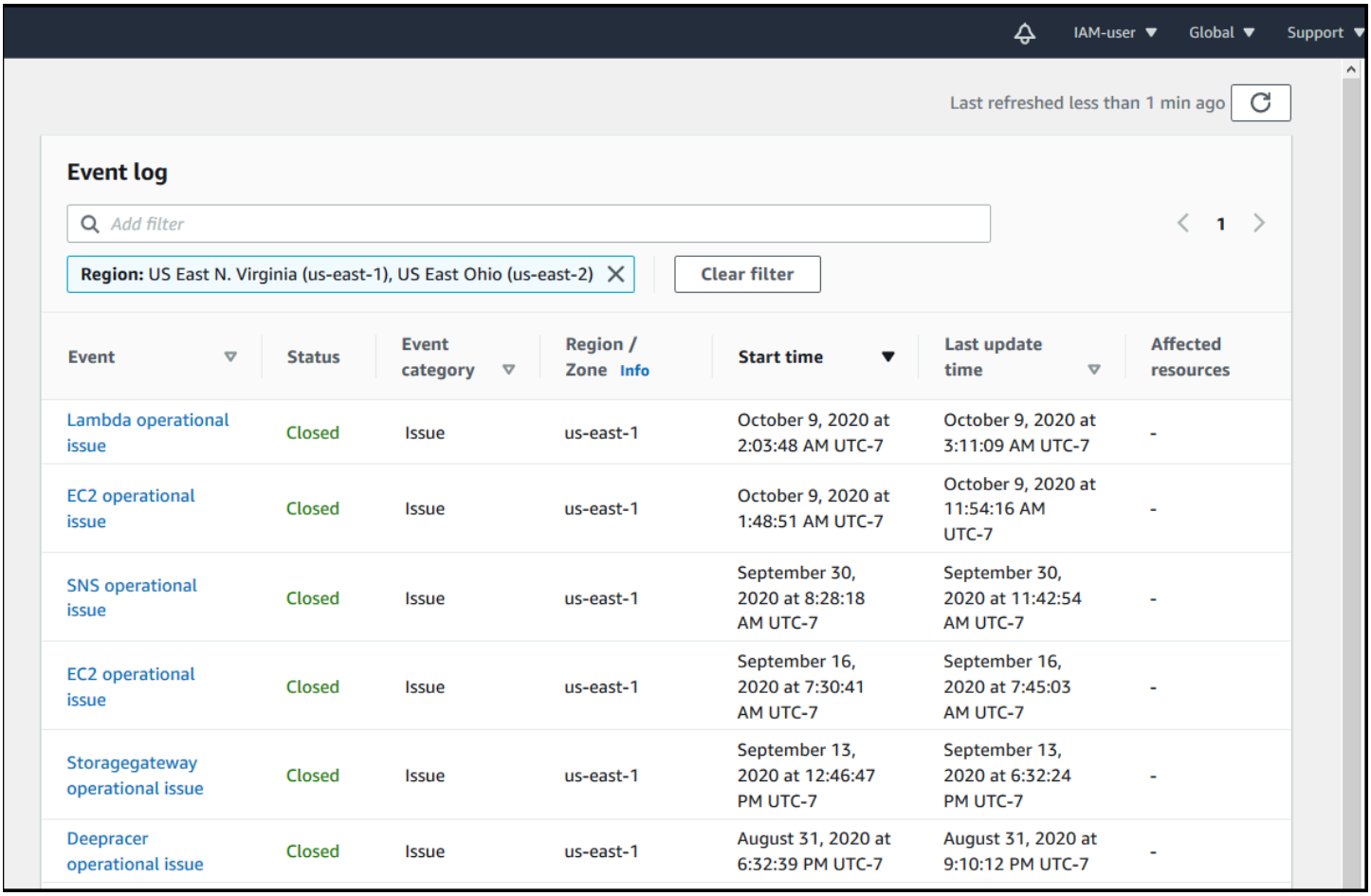
Puoi scegliere le seguenti opzioni di filtro per restringere i risultati:

- Zona di disponibilità
- Ora di fine
- Event
- Evento ARN
- Categoria dell'evento
- Ora dell'ultimo aggiornamento
- Region
- ID della risorsa/ARN
- Servizio
- Ora di inizio

- Stato

Example: Registro degli eventi

L'immagine seguente mostra gli eventi recenti nelle 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. Il Dettagli la scheda 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

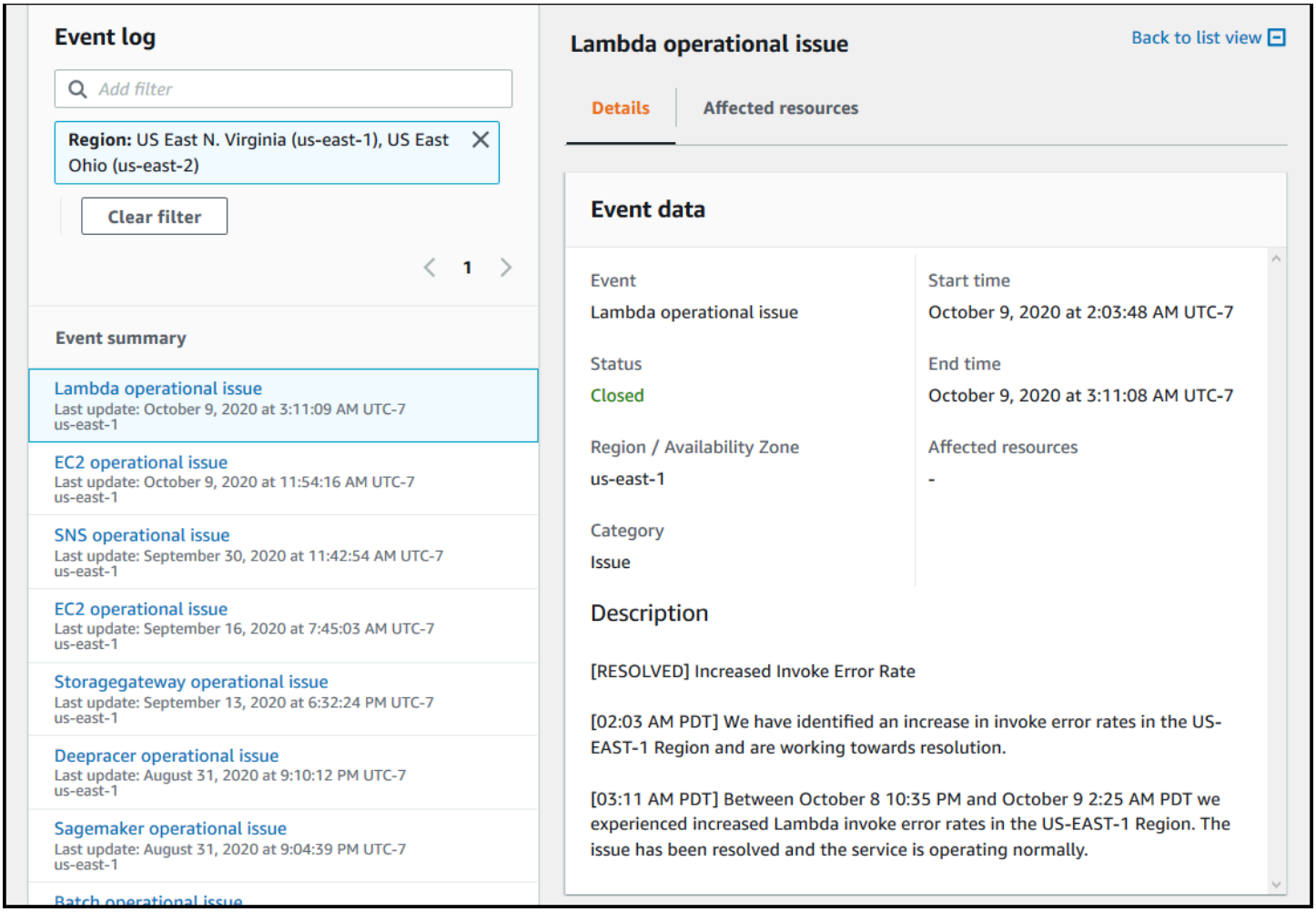
Il Risorse interessate la scheda mostra le seguenti informazioni su qualsiasi AWS risorse interessate dall'evento:

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

Puoi filtrare gli elementi che appaiono 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 esempio di evento per Lambda.



Tipi di eventi

Esistono due tipi di AWS Health eventi:

- Eventi pubblici sono eventi di servizio non specifici di un account. Ad esempio, se c'è 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.
- Account-specific gli eventi sono specifici del tuo account o di un account della tua organizzazione. Ad esempio, se c'è un problema con un'istanza Amazon EC2 in un Regione AWS che usi, AWS Health fornisce informazioni sull'evento e l'elenco delle istanze Amazon EC2 interessate.

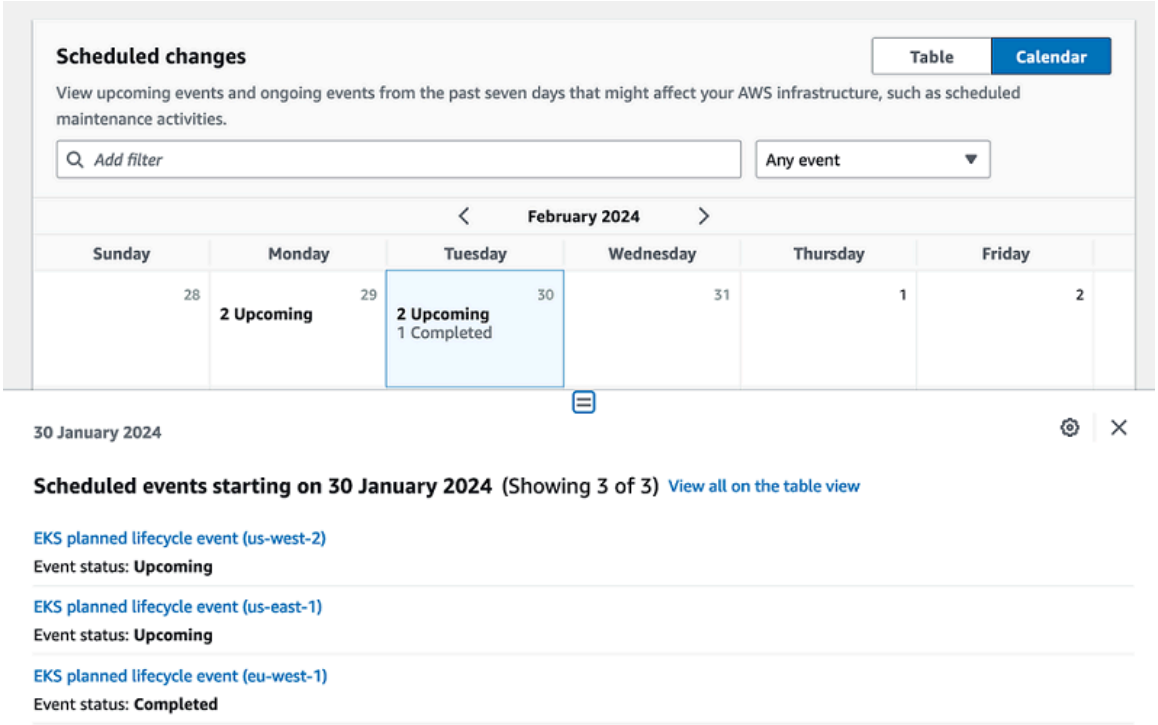
Puoi utilizzare le seguenti opzioni per identificare se un evento è pubblico o specifico dell'account:

- Nel AWS Health Dashboard, scegli Risorse interessate scheda 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 Per iniziare con il tuo AWS Health Dashboard.
- Usa il AWS Health API per restituire `eventScopeCode` parametro. Gli eventi possono avere il valore `PUBLIC`, `ACCOUNT_SPECIFIC` o `NONE`. Per ulteriori informazioni, vedere DescribeEventDetails operazione in AWS Health Riferimento API.

Visualizzazione del calendario

Visualizzazione del calendario è disponibile in modifiche programmate scheda al progetto AWS Health eventi in un calendario mensile. Questa visualizzazione consente di visualizzare le modifiche pianificate fino a 3 mesi nel passato e un anno nel futuro.

AWS Health gli eventi vengono visualizzati per data. Seleziona una data per visualizzare un pannello laterale che contiene ulteriori dettagli sul AWS Health evento. Prossime e in corso gli eventi sono visualizzati in nero. Completato gli eventi sono visualizzati in grigio. Se ci sono più di due eventi in una data, viene visualizzato solo il numero di eventi in nero e grigio. 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. Nel pannello laterale sono presenti dei breadcrumb per passare a una visualizzazione precedente.



Visualizzazione delle risorse interessate

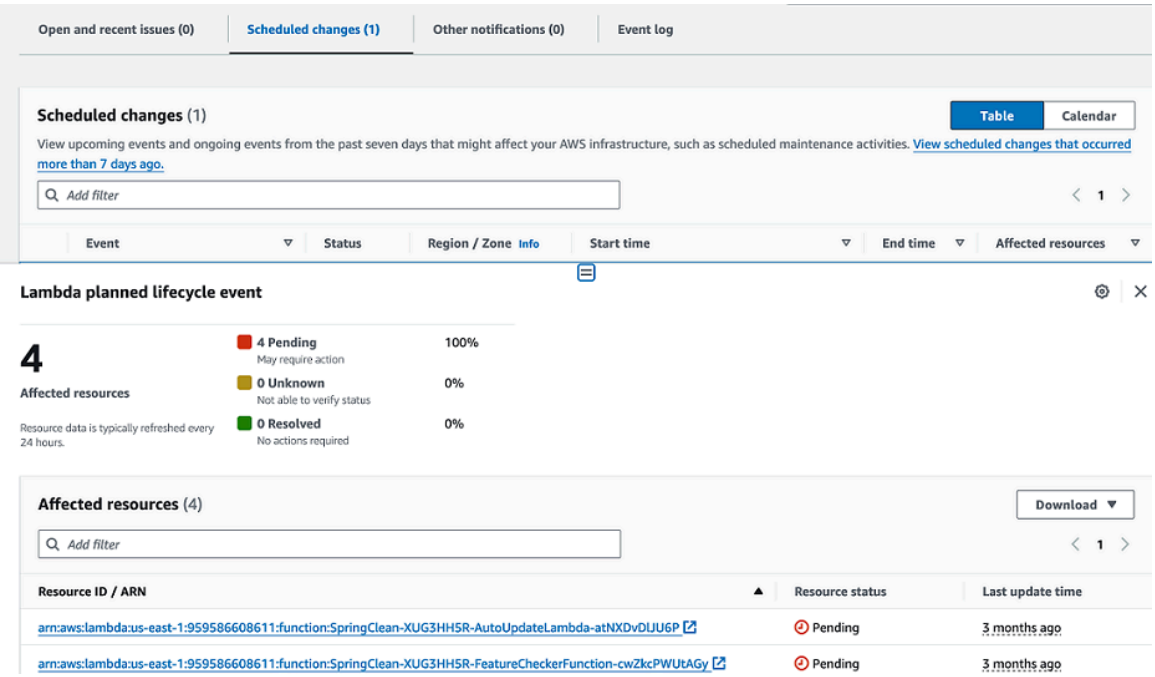
AWS Health gli eventi potrebbero specificare le risorse precise interessate. È possibile visualizzare le risorse interessate in Risorse interessate scheda del AWS Health evento. Per visualizzare lo stato, seleziona AWS Health evento. Lo stato viene visualizzato nella scheda delle risorse interessate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

Account-level AWS Health gli eventi visualizzano un riepilogo degli stati delle risorse interessate nella parte superiore del Risorse interessate scheda. Un elenco delle risorse interessate viene visualizzato in una tabella insieme allo stato corrispondente. Gli eventi del ciclo di vita pianificati sono un esempio di tipi di eventi che utilizzano il campo relativo allo stato della risorsa. Per saperne di più sugli eventi del ciclo di vita pianificati, vedi Eventi del ciclo di vita pianificati per AWS Health.

Quando si accede alla visualizzazione dell'organizzazione, AWS Health gli eventi visualizzano un riepilogo dello stato di tutte le risorse interessate per tutti gli account inclusi. Dopo il riepilogo è riportato un elenco degli account interessati e il numero di risorse in sospeso per quell'account. Seleziona il numero di account o il numero di risorse in sospeso per visualizzare il riepilogo della visualizzazione dell'account. Il riepilogo della visualizzazione dell'account contiene delle briciole per tornare all'elenco organizzativo degli account interessati. Un riepilogo degli stati delle risorse interessate viene visualizzato nella parte superiore del pannello diviso.

Puoi 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 negli account elencati. Passa al livello di account nella visualizzazione organizzativa per includere solo le risorse per quell'account nel file scaricato. Ogni risorsa interessata nel file scaricato include Account AWS ID, eventArn, nome dell'entità, entityArn, stato e ora dell'ultimo aggiornamento della risorsa. Se i filtri sono attivati, il file scaricato include solo i risultati filtrati.

È possibile scaricare un solo file alla volta. I file vengono scaricati automaticamente nella cartella di download predefinita del browser e hanno un nome di file predefinito basato su Regione AWS, il titolo dell'evento, la data di inizio dell'evento e la data di download.



Impostazioni del fuso orario

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

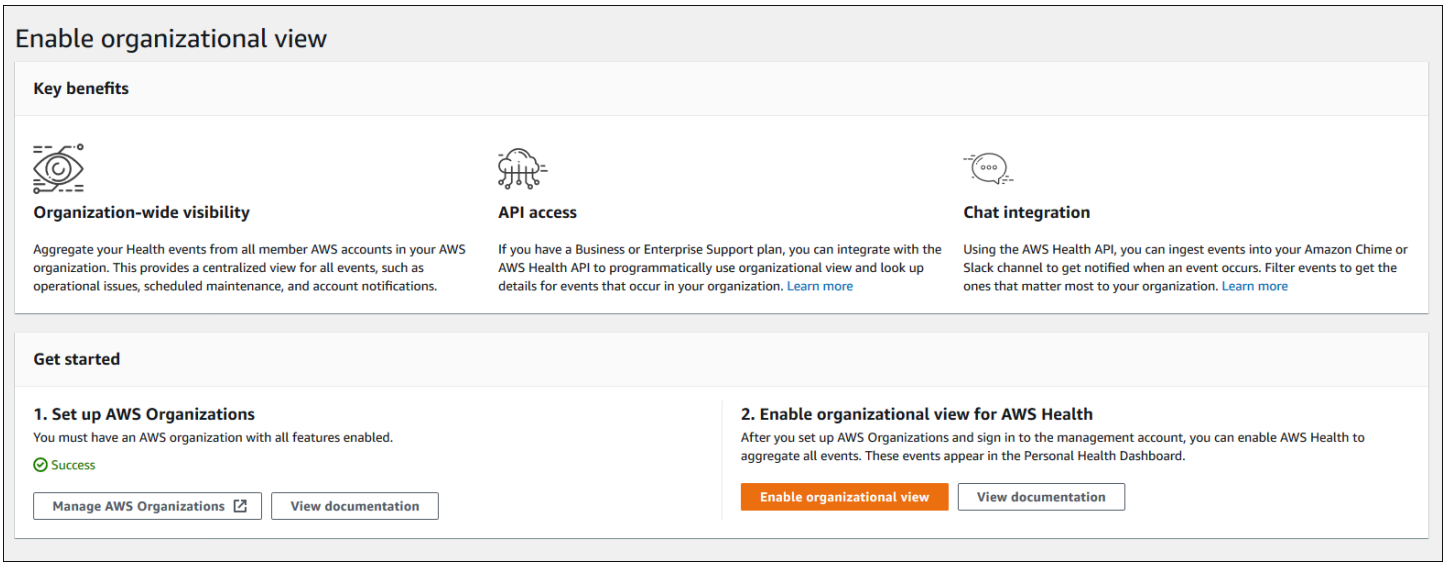
Per aggiornare le impostazioni del fuso orario

1. Apri il tuo AWS Health Dashboard all'indirizzo https://health.aws.amazon.com/health/home.
2. Nella parte inferiore della pagina, scegli Preferenze relative ai cookie.
3. Seleziona Consentito per cookie funzionali. Quindi scegli Salva le preferenze.
4. Nel pannello di navigazione del tuo AWS Health Dashboard, scegli Impostazioni del fuso orario.
5. Seleziona un fuso orario per il tuo AWS Health Sessioni del dashboard. Selezionare quindi Save changes (Salva modifiche).

Lo stato della tua organizzazione

AWS Health si integra con 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 AWS Health eventi tra gli account.



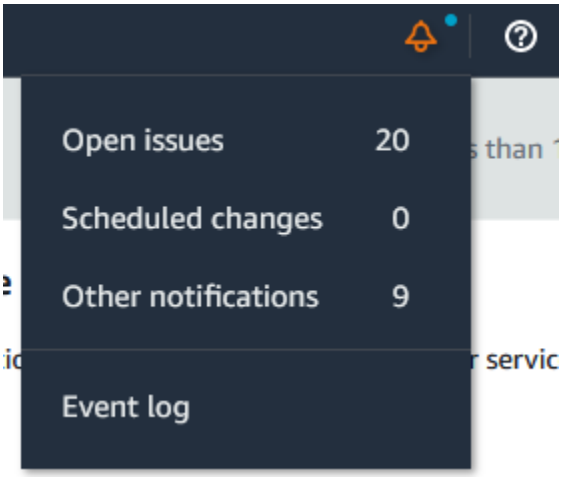
Avvisi per AWS Health eventi

I tuoi AWS Health La dashboard ha un'icona a forma di campana nella barra di navigazione della console con un menu di avviso. Questa funzione mostra il numero di recenti AWS Health eventi che appaiono nella dashboard in ogni categoria. Questa icona a forma di campana appare in diversi 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 al tuo 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

Usa EventBridge per rilevare e reagire alle modifiche per AWS Health eventi. È possibile monitorare specifici AWS Health eventi che si verificano nel tuo account e quindi imposta regole in modo che AWS Health ti avvisa, o intraprendi un'azione, quando gli eventi cambiano.

Usa EventBridge con AWS Health

1. Apri il tuo AWS Health Dashboard all'indirizzo https://health.aws.amazon.com/health/home.
2. Per accedere al EventBridge console per creare una regola, effettuate una delle seguenti operazioni:
   - Dal pannello di navigazione, in Integrazioni sanitarie, scegli Amazon EventBridge.
   - Sotto Configura EventBridge, scegli Vai a EventBridge.
3. Segui questa procedura per creare regole e monitorare gli eventi. Consulta Monitoraggio degli eventi in AWS Health con Amazon EventBridge.

Manage (Gestione) AWS Health notifiche in Notifiche AWS agli utenti

> **Important**
>
> Gli eventi pubblici non sono disponibili tramite notifiche AWS gestite in Notifiche AWS agli utenti. Per ricevere eventi pubblici, devi creare una EventBridge regola Amazon o una User-configured notifica (UCN) all'interno Notifiche AWS agli utenti. Per ulteriori informazioni, consulta Monitoraggio degli eventi in AWS Health con Amazon EventBridge e Gestire le notifiche in Notifiche AWS agli utenti.

AWS le notifiche gestite in ti Notifiche AWS agli utenti consentono di ricevere e gestire notifiche sugli eventi che riguardano l'utente Account AWS e i servizi. Quando utilizzi le notifiche AWS gestite in Notifiche AWS agli utenti, puoi specificare quali categorie di AWS Health eventi ricevere, configurare la visualizzazione organizzativa per le e-mail e ricevere notifiche consolidate anziché più email simili.

Puoi scegliere i seguenti canali aggiuntivi tramite Notifiche AWS agli utenti cui ricevere i tuoi AWS Health eventi:

- Email
- 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, inclusi gli ID delle risorse interessate, 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 Dashboard Health
>
> 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 AWS abbonamento alle notifiche gestite per AWS Health eventi

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

1. Apri Notifiche agli utenti in Console di gestione AWS.
2. Nel riquadro di navigazione, scegli gli abbonamenti alle notifiche AWS gestite.
3. 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 AWS agli utenti.

> **Note**
>
> AWS Health invio di e-mail migrato alle notifiche AWS gestite in Notifiche AWS agli utenti. Dal 15 dicembre 2025, ricevi e-mail da notifiche AWS gestite. Per ulteriori informazioni, vedi Cosa è cambiato nella migrazione alle notifiche AWS gestite? nelAWS notifiche gestite in AWS Domande frequenti sulle notifiche agli utenti.

AWS notifiche gestite in AWS Domande frequenti sulle notifiche agli utenti

Cosa è cambiato nella migrazione a AWS notifiche gestite?

Per impostazione predefinita, le e-mail relative alle notifiche gestite vengono inviate ai contatti esistenti dell'account (indirizzi email root, operativi, di fatturazione e di sicurezza). Le email che ricevi dalle notifiche AWS gestite provengono da `health@aws.com` anziché `no-reply-aws@amazon.com` e il formato delle email cambia. Se in precedenza hai impostato regole e-mail per le AWS Health notifiche, ad esempio l'instradamento di un'e-mail in base all'ID mittente o lo scraping del contenuto dell'e-mail, devi aggiornare questa configurazione in modo che corrisponda al nuovo formato 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 email 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 quelli dei membri.

Per abilitare l'aggregazione, devi aver AWS Organizations configurato e concesso un accesso affidabile tra il tuo account di gestione e il Notifiche AWS agli utenti servizio.

Per ulteriori informazioni, consulta Aggregazione delle notifiche AWS gestite in. Notifiche AWS agli utenti

Devo abilitare AWS Organizations accesso affidabile con Notifiche AWS agli utenti per ricevere email aggregate da AWS notifiche gestite?

Sì, AWS Organizations è richiesto un accesso affidabile con Notifiche AWS agli utenti from.

Qual è la differenza tra abilitare un accesso affidabile tramite AWS Organizations con AWS Health e con Notifiche AWS agli utenti?

La fiducia organizzativa e i relativi privilegi di amministratore delegato vengono assegnati dal servizio e fungono da barriera contro le autorizzazioni eccessivamente estese. L'accesso affidabile per AWS Health consente la visualizzazione organizzativa delle AWS Health API Dashboard Health, degli AWS Health eventi inviati tramite Amazon e delle configurazioni di notifica in. EventBridge Notifiche agli utenti L'accesso affidabile per Notifiche AWS agli utenti abilita le notifiche aggregate all'interno AWS delle notifiche gestite. Poiché l'accesso affidabile non è condiviso, la configurazione degli amministratori delegati deve essere aggiunta separatamente per ogni servizio.

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

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

Cosa fare AWS le categorie di notifiche gestite corrispondono a AWS Health schema?

Le notifiche relative alle operazioni sanitarie, alla sicurezza e alla fatturazione corrispondono alle notifiche AWS Health dell'account e alle modifiche pianificate relative rispettivamente alle operazioni, alla sicurezza e alla persona di fatturazione. AWS Health gli eventi con più di un tag personale vengono inviati tramite le categorie Sicurezza e Fatturazione. Account-specific i problemi includono eventi relativi allo stato di salute della categoria tematica specifici di un Account AWS.

Gli eventi di servizio pubblico non sono disponibili tramite notifiche AWS gestite.

AWS Health Pannello di controllo

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 Per iniziare con il tuo AWS Health Dashboard.

Per visualizzare il AWS Health Dashboard: stato del servizio

1. Accedi alla pagina https://health.aws.amazon.com/health/status.

   > **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

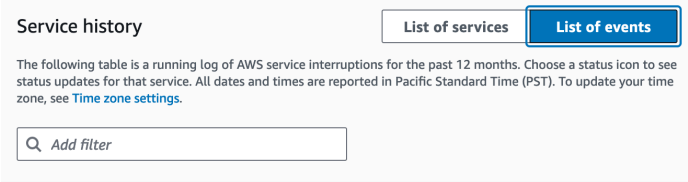
> **Note**
>
> Puoi visualizzare gli eventi nel tuo fuso orario locale o in UTC. Per ulteriori informazioni, consulta Impostazioni del fuso orario.

3. 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.

4. Accanto a un evento di servizio in corso, scegli l'icona di stato ( ) per visualizzare ulteriori informazioni sull'evento.

5. (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.

6. (Facoltativo) Puoi visualizzare gli eventi nel tuo fuso orario locale o UTC. Per ulteriori informazioni, consulta Impostazioni del fuso orario.

7. (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 Per iniziare con il tuo AWS Health Dashboard.

> **Note**
>
> Sebbene sia disponibile un feed RSS per gli eventi sanitari, il formato è soggetto a modifiche. Pertanto, lo scraping del feed RSS potrebbe non fornire tutti i dati pertinenti. Per importare in modo programmatico i dati sugli eventi sanitari, consigliamo l'integrazione con Amazon. EventBridge Per ulteriori informazioni, consulta Monitoraggio degli eventi in AWS Health con Amazon EventBridge.

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.

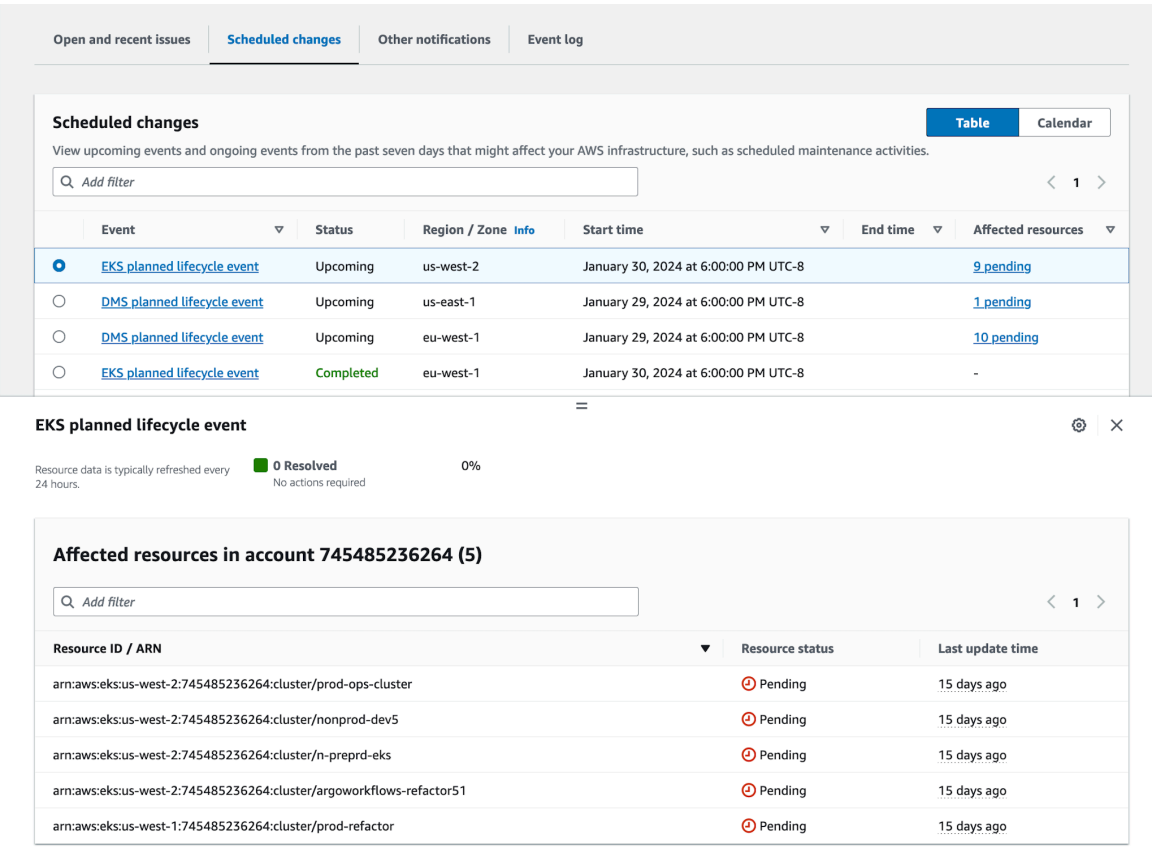
Ora di fine dell'evento: l'ora di fine dell'evento è la data in cui termina la modifica per tutte le AWS risorse. Tieni presente che l'ora di fine non è sempre specificata. È importante considerare l'ora di inizio come la data di modifica.

> **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.



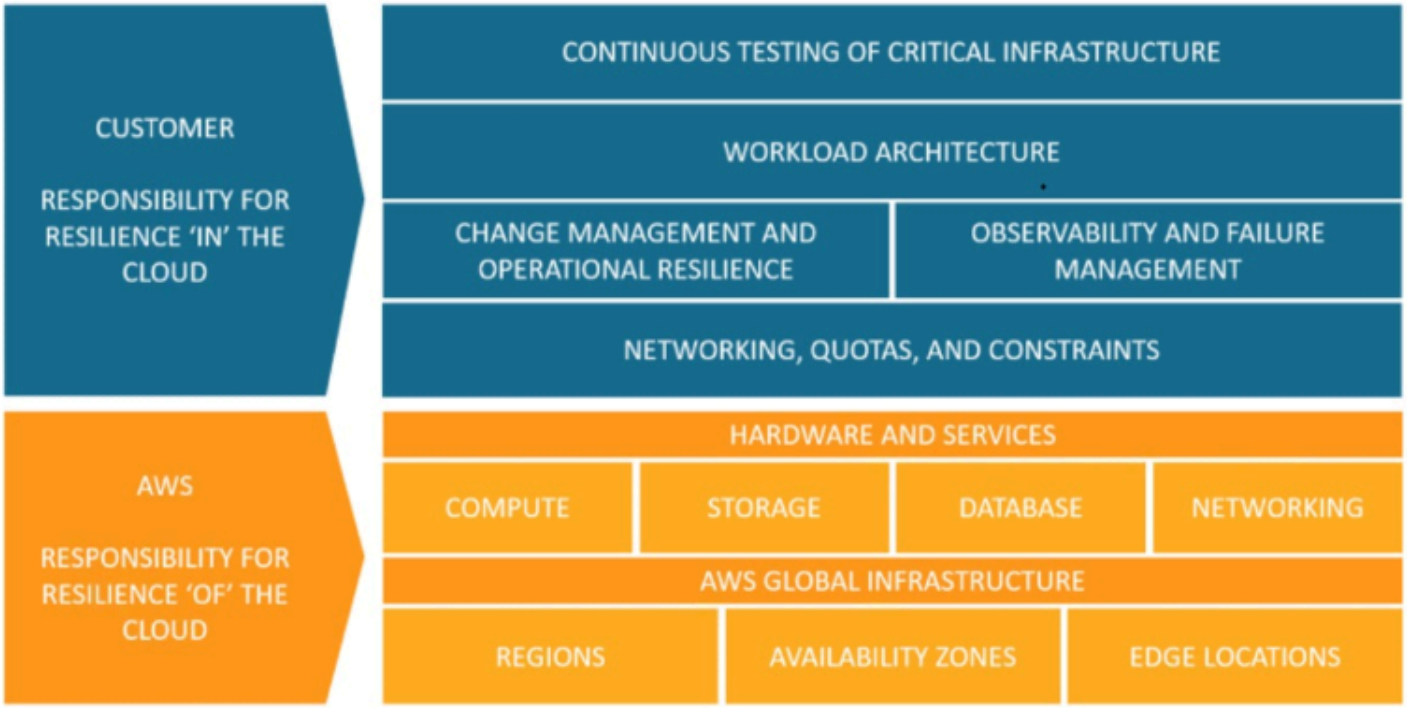
Una volta trascorsa la data pianificata dell'evento:

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

Catalogo delle versioni per AWS Health

Scopri il catalogo delle versioni per AWS Health, che fornisce una panoramica completa delle versioni supportate e delle relative tempistiche.

Argomenti

- Cos'è il catalogo delle versioni?
- Cosa puoi fare con il catalogo delle versioni
- Come accedere al catalogo delle versioni
- Dettagli disponibili nel catalogo delle versioni
- Come recuperare le informazioni del catalogo delle versioni con l'API
- Come visualizzare il catalogo delle versioni nel Dashboard Health

Cos'è il catalogo delle versioni?

Se si eseguono applicazioni su AWS, è necessario rimanere aggiornati sulle versioni del software per mantenere una solida postura operativa e di sicurezza. AWS Health invia già dati specifici per account e risorse Eventi del ciclo di vita pianificati per AWS Health con largo anticipo rispetto ai traguardi della fine del supporto della versione principale. Il catalogo delle versioni aggiunge una panoramica a livello di servizio delle versioni supportate e delle relative tempistiche. È possibile utilizzare questa visualizzazione per creare pianificazioni di aggiornamento e controlli di governance e per passare a versioni supportate più recenti prima di ricevere un evento del ciclo di vita pianificato specifico per l'account.

L'API del ciclo di vita delle versioni aggrega queste informazioni in un unico schema coerente. Con una chiamata API autenticata, puoi richiedere la tempistica di supporto di una versione specifica di un AWS componente di servizio, ad esempio un AWS Lambda runtime del linguaggio, una versione del motore Amazon Relational Database Service (Amazon RDS) o una versione Kubernetes di Amazon Elastic Kubernetes Service (Amazon EKS).

Usa questi dati per creare dashboard di aggiornamento, avvisare sulle versioni che si avvicinano alla fine del supporto e automatizzare i controlli di conformità per le versioni in esecuzione. Puoi anche ridurre il debito tecnico passando a versioni più recenti supportate prima di ricevere un evento del ciclo di vita pianificato specifico per l'account.

Cosa puoi fare con il catalogo delle versioni

L'API del ciclo di vita delle versioni ti offre l'accesso programmatico per capire dove sono AWS il componente di servizio rientra nella relativa timeline di supporto. I casi d'uso più comuni includono:

- Gestione delle vulnerabilità e della conformità — Identifica il software che ha raggiunto la fine del ciclo di vita e che non riceve più patch di sicurezza (ad esempio, Python 3.9 ha raggiunto la fine del ciclo di vita nell'ottobre 2025) e inserisci i dati di fine vita nelle dashboard di conformità per gli audit PCI DSS, SOC 2 e FedRAMP.
- Verifica dell'inventario dell'infrastruttura e della flotta — Cross-reference il tuo database di gestione della configurazione (CMDB) o l'inventario delle risorse per contrassegnare i motori di database non supportati (Amazon RDS PostgreSQL, MySQL) o i runtime Lambda (Node.js, Java, .NET). Ciò è particolarmente utile per AWS-servizi gestiti, perché il catalogo tiene traccia di Amazon EKS, Amazon Aurora (Aurora) MySQL e PostgreSQL, Amazon RDS, Amazon OpenSearch Servizio, Amazon ElastiCache, tempi di esecuzione Lambda e altro ancora.
- Pianificazione proattiva degli aggiornamenti — Crea tempistiche e programmi di migrazione e genera tabelle di marcia che mostrino quando ciascuna dipendenza esce dal supporto rispetto alle sue fasi di sviluppo attive.
- CI/CD automazione delle pipeline — Integra l'API nelle tue pipeline per far fallire le build o generare avvisi quando un progetto dipende da un runtime o da un framework che è prossimo alla fine del ciclo di vita. Puoi anche mantenere automaticamente una matrice di test (ad esempio, esegui il test su tutte le versioni di Python supportate attivamente) senza codificare gli elenchi delle versioni.
- Strumenti e dashboard per sviluppatori — Potenzia i dashboard operativi interni che mostrano lo stato di supporto di ogni componente utilizzato in un carico di lavoro specifico.
- AWS monitoraggio del ciclo di vita del servizio — Traccia AWS-versioni di servizi gestiti, come Amazon EKS e Lambda, e preparati agli aggiornamenti forzati prima che si verifichino.

Come accedere al catalogo delle versioni

È possibile visualizzare il catalogo delle versioni in due modi:

- Dashboard Health — Visualizza le versioni supportate e le relative tempistiche del ciclo di vita direttamente nella console.
- AWS Health API — Clienti su AWS L'assistenza può chiamare il `DescribeServiceLifecycle` API per integrare i dati del ciclo di vita nei loro flussi di lavoro operativi.

Vedi il AWS Health Riferimento API per tutti i dettagli.

Dettagli disponibili nel catalogo delle versioni

Ogni versione in una risposta fornisce una panoramica e una cronologia delle varie fasi del ciclo di vita.

Top-level immissione della versione

Campo	Description
`service`	La AWS servizio a cui appartiene la versione, ad esempio `LAMBDA`, `RDS`, o `EKS`.
`title`	Il nome leggibile dall'uomo della versione, ad esempio `Python 3.14 Lambda Runtime`.
`version`	L'identificatore di versione specifico del servizio che trasmetti nelle query, ad esempio `python3.14` .
`lifecycleEvents`	Un elenco degli eventi del ciclo di vita per questa versione, in ordine cronologico. Ogni evento indica una data significativa, ad esempio un rilascio, la fine del supporto standard o la fine del ciclo di vita, e include tag di rischio di impatto che indicano le conseguenze del superamento di tale data. Leggi gli eventi per comprendere la cronologia completa dal rilascio alla fine del supporto.

Oggetto evento del ciclo di vita

Campo	Description
`lifecycleEventType`	Il tipo di pietra miliare, ad esempio, `END_OF_SUPPORT` , `BLOCK_RESOURCE_CREATE` , o `BLOCK_RESOURCE_UPDATE` .
`date`	La data in cui la pietra miliare ha effetto.
`description`	Una spiegazione leggibile dall'uomo di ciò che accade in questa data.

Campo	Description
`impactRisks`	Uno o più tag di rischio di impatto, ad esempio `END_OF_SUPPORT` , `BILLING`, o `AVAILABILITY` , che indicano cosa smette di funzionare allo scadere della data.
`regions`	Le Regioni a cui si applica l'evento. Un valore di `["all"]` indica tutte le regioni.

> **Note**
>
> I valori mostrati per `lifecycleEventType` e `impactRisks` sono quelli visibili in questo esempio. Vedi il AWS Health Riferimento API per l'elenco completo dei valori possibili.

Impact-risk tag

Ogni evento elenca uno o più tag di rischio di impatto in modo da poterne valutare la gravità. `AVAILABILITY` gli impatti sono i più urgenti, perché la risorsa diventa non disponibile dopo tale data.

Tag	Significato
`END_OF_SUPPORT`	La versione non riceve più patch o aggiornamenti di sicurezza.
`BILLING`	Continuare a utilizzare questa versione potrebbe comportare costi aggiuntivi, ad esempio costi di supporto esteso.
`AVAILABILITY`	La risorsa diventa non disponibile dopo la scadenza della data. Questo è l'impatto più urgente.

Come recuperare le informazioni del catalogo delle versioni con l'API

Interroga le informazioni sul ciclo di vita utilizzando AWS Command Line Interface (AWS CLI).

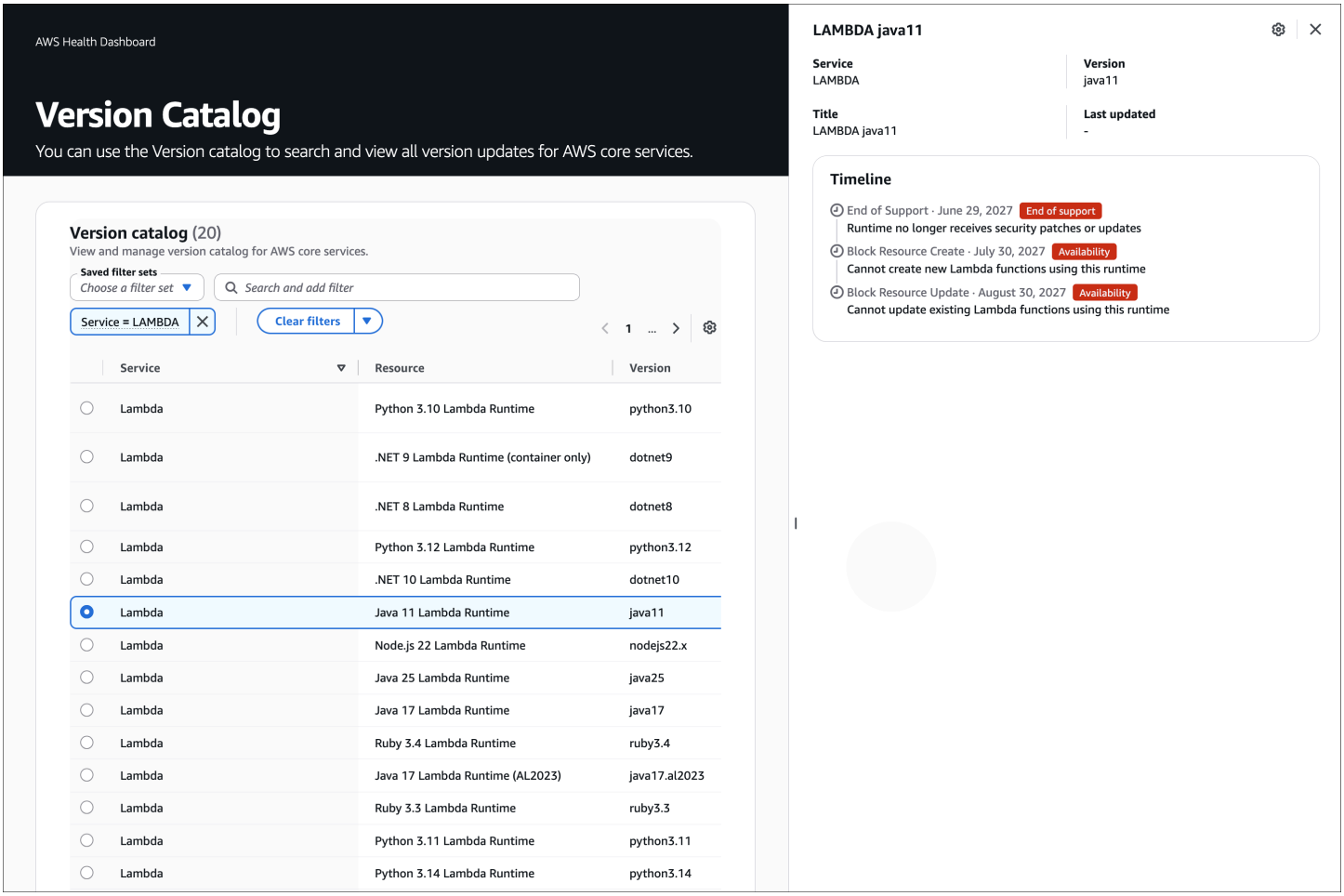
```
aws health describe-service-lifecycle
```

L'esempio seguente mostra una voce di versione tratta da `DescribeServiceLifecycle` API.


```
{
  "service": "LAMBDA",
  "title": "Python 3.14 Lambda Runtime",
  "version": "python3.14",
  "lifecycleEvents": [
    {
      "lifecycleEventType": "END_OF_SUPPORT",
      "date": 1877472000.0,
      "description": "Runtime no longer receives security patches or updates",
      "impactRisks": ["END_OF_SUPPORT"],
      "regions": ["all"]
    },
    {
      "lifecycleEventType": "BLOCK_RESOURCE_CREATE",
      "date": 1880150400.0,
      "description": "Cannot create new Lambda functions using this runtime",
      "impactRisks": ["AVAILABILITY"],
      "regions": ["all"]
    },
    {
      "lifecycleEventType": "BLOCK_RESOURCE_UPDATE",
      "date": 1882828800.0,
      "description": "Cannot update existing Lambda functions using this runtime",
      "impactRisks": ["AVAILABILITY"],
      "regions": ["all"]
    }
  ]
}
```


Come visualizzare il catalogo delle versioni nel Dashboard Health

Quanto segue mostra la funzionalità del catalogo delle versioni in Dashboard Health.


AWS Health Dashboard
Version Catalog
You can use the Version catalog to search and view all version updates for AWS core services.
Version catalog (20)
View and manage version catalog for AWS core services.
Saved filter sets
Choose a filter set
Search and add filter
Service = LAMBDA
Clear filters
1 ...
Service
Resource
Version
Lambda Python 3.10 Lambda Runtime python3.10
Lambda .NET 9 Lambda Runtime (container only) dotnet9
Lambda .NET 8 Lambda Runtime dotnet8
Lambda Python 3.12 Lambda Runtime python3.12
Lambda .NET 10 Lambda Runtime dotnet10
Lambda Java 11 Lambda Runtime java11
Lambda Node.js 22 Lambda Runtime nodejs22.x
Lambda Java 25 Lambda Runtime java25
Lambda Java 17 Lambda Runtime java17
Lambda Ruby 3.4 Lambda Runtime ruby3.4
Lambda Java 17 Lambda Runtime (AL2023) java17.al2023
Lambda Ruby 3.3 Lambda Runtime ruby3.3
Lambda Python 3.11 Lambda Runtime python3.11
Lambda Python 3.14 Lambda Runtime python3.14
LAMBDA java11
Service
LAMBDA
Version
java11
Title
LAMBDA java11
Last updated
-
Timeline
End of Support · June 29, 2027 End of support
Runtime no longer receives security patches or updates
Block Resource Create · July 30, 2027 Availability
Cannot create new Lambda functions using this runtime
Block Resource Update · August 30, 2027 Availability
Cannot update existing Lambda functions using this runtime

Integrazione AWS Health con altri sistemi che utilizzano AWS Health "Hello, World!"

AWS Health è un servizio web RESTful 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations di Supporto AWSper utilizzare l' AWS Health API. Se utilizzi un piano Regione AWS che non offre uno di questi Supporto AWS piani o se non sei passato a uno di questi piani, puoi utilizzare l' AWS Health API con un piano Business On-Ramp, Enterprise o Enterprise Support. Se chiami l' AWS Health API da un utente Account AWS che non è iscritto a uno di questi piani, ricevi un `SubscriptionRequiredException` errore.

Puoi utilizzare gli AWS SDK 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 Console di gestione AWS che è possibile utilizzare per visualizzare e cercare eventi ed entità interessate. Per informazioni, consulta Per iniziare con il tuo AWS Health Dashboard.

Argomenti

- Firma AWS Health Richieste API
- Scelta degli endpoint per AWS Health Richieste API
- Demo: recupero degli ultimi sette giorni di AWS Health dati sugli eventi a livello di codice
- Tutorial: Utilizzo del AWS Health API con esempi in Java

Firma AWS Health Richieste API

Quando utilizzi gli AWS SDK o il AWS Command Line Interface (AWS CLI) per effettuare richieste AWS, questi strumenti firmano automaticamente le richieste per te con la chiave di accesso che specifichi al momento della configurazione degli strumenti. Ad esempio, se utilizzi la AWS SDK per Java precedente demo dell'endpoint ad alta disponibilità, non devi 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 utilizzi gli AWS SDK 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 AWS Health Richieste 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 Richieste API.

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

La tabella seguente rappresenta la configurazione predefinita.

Description	Regione di firma	Endpoint	Protocollo
Attivo	us-east-1	health.us-east-1.amazonaws.com (IPv4-only) health.us-east-1.api.aws (IPv4 e IPv6 supportati)	HTTPS
Passivo	us-east-2	health.us-east-2.amazonaws.com (IPv4-only) health.us-east-2.api.aws (IPv4 e IPv6 supportati)	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 degli ultimi sette giorni di AWS Health dati sugli eventi a livello di codice

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 degli ultimi sette giorni di AWS Health dati sugli eventi utilizzando Java
- Demo: recupero degli ultimi sette giorni di AWS Health dati sugli eventi usando Python

Demo: recupero degli ultimi sette giorni di AWS Health dati sugli eventi utilizzando 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: AWS Health output 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 degli ultimi sette giorni di AWS Health dati sugli eventi usando 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: AWS Health output 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 del 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'istanza AWSCredentials:

```
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: Inizializzare un AWS Health Client API

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: Utilizzo AWS Health Operazioni 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

Sicurezza nel cloud presso AWS è la massima priorità. Come 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 AWS e tu. 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 in esecuzione AWS servizi in AWS Cloud. AWS ti fornisce anche servizi che puoi utilizzare in sicurezza. Third-party i revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito del AWS Programmi di conformità. Per saperne di più sui programmi di conformità applicabili a AWS Health, vedi AWS Servizi rientranti nell'ambito del programma di conformità.
- Sicurezza nel cloud — La tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la sensibilità dei tuoi dati, i requisiti della tua azienda e le leggi e i regolamenti applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'uso AWS Health. Nei seguenti argomenti viene illustrato come configurare AWS Health per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a usarne altri AWS servizi che ti aiutano a monitorare e proteggere i tuoi AWS Health risorse.

Argomenti

- Protezione dei dati in AWS Health
- Gestione delle identità e degli accessi per AWS Health
- Registrazione e monitoraggio AWS Health
- Convalida della conformità per AWS Health
- Resilienza in AWS Health
- Sicurezza dell'infrastruttura in AWS Health
- Analisi della configurazione e delle vulnerabilità in AWS Health
- Le migliori pratiche di sicurezza per AWS Health

Protezione dei dati in AWS Health

Il AWS modello di responsabilità condivisa si applica alla protezione dei dati in. 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, vedere Domande frequenti sulla privacy dei datiTermini. Per ulteriori informazioni sulla protezione dei dati in Europa, consulta il Centro generale sulla protezione dei dati (GDPR).

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS con cui comunicare AWS 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'uso CloudTrail percorsi da catturare AWS attività, vedi Lavorare con CloudTrail sentieri nel AWS CloudTrail Guida per l'utente.
- Usare AWS soluzioni di 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 sono necessari moduli crittografici convalidati FIPS 140-3 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

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

Crittografia dei dati

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

La crittografia dei dati si riferisce alla protezione dei dati durante il transito (durante il trasferimento dal servizio all'utente) AWS account) e a riposo (mentre è archiviato in 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 di clienti negli eventi.

Crittografia dei dati a riposo

Tutti i dati archiviati da AWS Health è crittografato a riposo.

Crittografia dei dati in transito

Tutti i dati inviati da e verso AWS Health è crittografato durante il transito.

Gestione delle chiavi

AWS Health non supporta le chiavi di crittografia gestite dal cliente per i dati crittografati in AWS Cloud.

Gestione delle identità e degli accessi per AWS Health

AWS Identity and Access Management (IAM) è un Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso a AWS risorse. Gli amministratori IAM controllano chi può esserlo autenticate (effettuato l'accesso) e autorizzati (dispongono delle autorizzazioni) da utilizzare AWS Health risorse. IAM è un Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso tramite policy
- In che modo AWS Health funziona con IAM

- AWS Health esempi di policy basate sull'identità
- Risoluzione dei problemi AWS Health identità e accesso
- Utilizzo di ruoli collegati ai servizi per AWS Health
- AWS politiche gestite per AWS Health

Destinatari

Come si usa AWS Identity and Access Management (IAM) si differenzia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi AWS Health identità e accesso)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta In che modo AWS Health funziona con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta AWS Health esempi di policy basate sull'identità)

Autenticazione con identità

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

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

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

AWS Utente root dell'account

Quando crei un Account AWS, si inizia con un'identità di accesso denominata Account AWS utente root che ha accesso completo a tutti Servizi AWS e risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, vedere Richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzo di credenziali temporanee nel Guida per l'utente IAM.

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

Ruoli IAM

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

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Sei tu a controllare l'accesso in AWS creando politiche e allegandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un principale effettua una richiesta. La maggior parte delle politiche sono archiviate in AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

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

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

Identity-based norme

Identity-based le policy sono documenti relativi alle politiche di autorizzazione JSON che si allegano a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporato direttamente in un'unica identità) o politiche gestite (politiche autonome associate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Resource-based norme

Resource-based le policy sono documenti di policy JSON che alleghi a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Resource-based le policy sono policy in linea che si trovano in quel servizio. Non puoi usare AWS policy gestite da 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 solo a un utente IAM di accedere a eventi Amazon EC2 specifici nel AWS Health Dashboard.

Per ulteriori informazioni, consulta Resources.

Liste di controllo accessi

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

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

AWS Health non supporta gli ACL.

Altri tipi di policy

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

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta Policy di controllo delle risorse (RCP) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

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

In che modo AWS Health funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Health, dovresti capire quali funzionalità IAM possono essere utilizzate con AWS Health. Per avere una visione di alto livello di come AWS Health e altro AWS i servizi funzionano con IAM, vedi AWS Servizi che funzionano con IAM nel Guida per l'utente IAM.

Argomenti

- AWS Health policy basate sull'identità
- AWS Health policy basate sulle risorse
- Autorizzazione basata su AWS Health tag

- AWS Health Ruoli IAM

AWS Health policy basate sull'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.

Operazioni

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

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Azioni politiche in AWS Health usa il seguente prefisso prima dell'azione: `health:`. Ad esempio, per concedere a qualcuno il permesso di visualizzare informazioni dettagliate su eventi specifici con DescribeEventDetails Operazione API, includi `heath:DescribeEventDetails` azione nella politica.

Le dichiarazioni politiche devono includere un `Action` o `NotAction` elemento. AWS Health definisce il proprio insieme 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, vedi Azioni definite da AWS Health nel Guida per l'utente IAM.

Resources

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

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

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

Un AWS Health l'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 tutto AWS Health eventi per Amazon EC2 che appartengono a un account specifico, utilizza il carattere jolly (*).

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

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARN) e AWS Namespace dei servizi.

Alcuni AWS Health le 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, DescribeEvents l'operazione restituisce informazioni sugli eventi che soddisfano un criterio di filtro specificato. Ciò significa che un utente IAM deve disporre delle autorizzazioni per visualizzare questo evento.

Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

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

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

Per visualizzare un elenco di AWS Health tipi di risorse e relativi ARN, vedi Risorse definite da AWS Health nel Guida per l'utente IAM. 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 usare AWS Policy JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per vedere tutto AWS chiavi di condizione globali, vedere AWS chiavi di contesto relative alle condizioni globali nel 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 vedere tutto AWS chiavi di condizione globali, vedere AWS Chiavi di contesto delle condizioni globali nel Guida per l'utente IAM.

Il DescribeAffectedEntities e DescribeEventDetails Le operazioni API supportano `health:eventTypeCode` e `health:service` chiavi di condizione.

Per visualizzare un elenco di AWS Health chiavi di condizione, vedere Chiavi di condizione per AWS Health nel Guida per l'utente IAM. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite da AWS Health.

Esempi

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

AWS Health policy basate sulle risorse

Resource-based le policy sono documenti di policy JSON che specificano quali azioni può eseguire un preponente specificato su AWS Health risorsa e in quali condizioni. AWS Health supporta politiche di autorizzazione basate sulle risorse per gli eventi sanitari. Resource-based le politiche consentono di concedere l'autorizzazione di utilizzo ad altri account in base alla risorsa. È inoltre possibile utilizzare una politica basata sulle risorse per consentire un AWS servizio per accedere al tuo AWS Health eventi.

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'entità principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi AWS account, è inoltre necessario concedere all'entità principale il permesso di 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, vedere In che modo i ruoli IAM differiscono da Resource-based Politiche nel Guida per l'utente IAM.

AWS Health supporta solo politiche basate sulle risorse per DescribeAffectedEntities e DescribeEventDetails Operazioni API. È possibile specificare queste azioni in una policy per definire quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire azioni su AWS Health evento.

Esempi

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

Autorizzazione basata su AWS Health tag

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 con 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. Si ottengono credenziali di sicurezza temporanee chiamando AWS STS Operazioni API come AssumeRole o GetFederationToken.

AWS Health supporta l'utilizzo di credenziali temporanee.

Service-linked ruoli

Service-linked ruoli permettere AWS servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. Service-linked i ruoli appaiono nel tuo 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`. Allegato al ruolo c'è il Health_OrganizationsServiceRolePolicy AWS politica gestita. La AWS la politica gestita consente AWS Health di accedere a eventi sanitari da altri AWS account dell'organizzazione.

È possibile utilizzare EnableHealthServiceAccessForOrganization operazione per creare il ruolo collegato al servizio nell'account. Tuttavia, se si desidera disattivare questa funzionalità, è necessario prima chiamare il DisableHealthServiceAccessForOrganization operazione. È quindi possibile 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 AWS Health eventi tra gli account.

Ruoli dei servizi

Questa funzionalità 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 policy 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 Console di gestione AWS, AWS CLI, o AWS API. 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 di AWS Health console
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Accedere al AWS Health Dashboard e AWS Health "Hello, World!"
- Condizioni basate su risorse e operazioni

Best practice delle policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare AWS Health risorse nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con AWS politiche gestite e passaggio alle autorizzazioni con privilegi minimi — Per iniziare a concedere le autorizzazioni agli utenti e ai carichi di lavoro, utilizza AWS politiche gestite che concedono autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo AWS politiche gestite dal cliente specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo

definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e suggerimenti utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA) — Se hai uno scenario che richiede utenti IAM o un utente root Account AWS, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Utilizzo di AWS Health console

Per accedere a AWS Health console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi a AWS Health risorse nel 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 il AWS Health console, puoi allegare quanto segue AWS politica gestita, AWSHealthFullAccess.

Il `AWSHealthFullAccess` la politica concede a un'entità il pieno accesso a quanto segue:

- Abilita o disabilita il AWS Health funzionalità di visualizzazione organizzativa per tutti gli account in un AWS organizzazione
- La AWS Health Dashboard nel AWS Health plancia
- AWS Health Operazioni e notifiche API
- Visualizza le informazioni sugli account che fanno parte del tuo AWS organizzazione
- Visualizza le unità organizzative (OU) dell'account di gestione

Example: AWSHealthFullAccess

JSON

```
{
    "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 `Health_OrganizationsServiceRolePolicy` AWS politica gestita, in modo che AWS Health puoi visualizzare gli eventi per altri account della tua organizzazione. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health.

Non è necessario consentire le autorizzazioni minime della console agli utenti che effettuano chiamate solo verso AWS CLI o il 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 collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando AWS CLI o AWS API.

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

Accedere al AWS Health Dashboard e AWS Health "Hello, World!"

Il AWS Health La dashboard è disponibile per tutti AWS account. I AWS Health L'API è disponibile solo per gli account con AWS Supporto aziendale+, AWS Supporto aziendale, o AWS Piano operativo unificato. 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 a AWS Health Dashboard e AWS Health API.

Per impostazione predefinita, gli utenti IAM non hanno accesso a AWS Health Dashboard o AWS Health API. Consenti agli utenti l'accesso ai tuoi account AWS Health informazioni 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 visualizzarlo 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 di tutti AWS servizi sull'account, che possono includere, a titolo esemplificativo ma non esaustivo, AWS ID di risorse come ID di istanza Amazon EC2, indirizzi IP delle istanze EC2 e notifiche di sicurezza generali.
> Ad esempio, se una policy IAM concede l'accesso solo a AWS Health Dashboard e AWS Health API, quindi l'utente o il ruolo a cui si applica la policy può accedere a tutte le informazioni pubblicate su AWS servizi e risorse correlate, anche se altre politiche IAM non consentono tale accesso.

Puoi utilizzare due gruppi di API per AWS Health.

- Account individuali: puoi utilizzare operazioni come DescribeEvents e DescribeEventDetails per ottenere informazioni su AWS Health eventi per il tuo account.
- Account organizzativo: puoi utilizzare operazioni come DescribeEventsForOrganization e DescribeEventDetailsForOrganization per ottenere informazioni su AWS Health eventi per gli account che fanno parte della tua organizzazione.

Per ulteriori informazioni sulle operazioni API disponibili, consulta AWS Health Riferimento alle API.

Singole operazioni

È possibile impostare `Action` elemento di una policy IAM per `health:Describe*`. Ciò consente l'accesso a AWS Health Dashboard e AWS Health. AWS Health supporta il controllo degli accessi agli eventi in base a `eventTypeCode` e servizio.

Descrivere l'accesso

Questa dichiarazione politica garantisce l'accesso a AWS Health Dashboard e qualsiasi `Describe*` AWS Health Operazioni API. Ad esempio, un utente IAM con questa policy può accedere a AWS Health Dashboard nel Console di gestione AWS e chiama il AWS Health `DescribeEvents` operazione API.

Example: Descrivere l'accesso

JSON

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

Negare l'accesso

Questa dichiarazione politica nega l'accesso a AWS Health Dashboard e AWS Health API. Un utente IAM con questa policy non può visualizzare AWS Health Dashboard nel Console di gestione AWS e non puoi chiamare nessuno dei AWS Health Operazioni API.

Example: Negare l'accesso

JSON

```
{
  "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 al AWS Health e AWS Organizations azioni.

Le `Action` l'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 API, consulta Azioni definite da AWS Health API e notifiche nel Guida per l'utente IAM.

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

Consentire l'accesso a AWS Health visualizzazione organizzativa

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

Example: Consenti AWS Health accesso alla vista organizzativa

JSON

```
{
    "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 a AWS Health visualizzazione organizzativa

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

Example: Rifiuta AWS Health accesso alla vista organizzativa

JSON

```
{
```

```
    "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 AWS Health-dichiarazione politica specifica a tale politica.

Condizioni basate su risorse e operazioni

AWS Health supporti condizioni IAM per DescribeAffectedEntities e DescribeEventDetails Operazioni API. È possibile utilizzare condizioni basate su risorse e azioni per limitare gli eventi che AWS Health L'API invia a un utente, un gruppo o un ruolo.

A tale scopo, aggiorna il `Condition` blocca la policy IAM o imposta il `Resource` elemento. Puoi usare Condizioni delle stringhe per limitare l'accesso in base a determinati AWS Health campi di eventi.

È possibile utilizzare i seguenti campi quando si specifica un AWS Health evento nella tua polizza:

- `eventTypeCode`
- `service`

> **Note**
>
> - Il DescribeAffectedEntities e DescribeEventDetails Le operazioni API supportano le autorizzazioni a livello di risorsa. Ad esempio, puoi creare una policy per consentire o negare specifiche AWS Health eventi.
> - Le DescribeAffectedEntitiesForOrganization e DescribeEventDetailsForOrganization Le operazioni API non supportano le autorizzazioni a livello di risorsa.
> - Per ulteriori informazioni, consulta Azioni, risorse e chiavi di condizione per AWS Health API e notifiche nel Riferimento all'autorizzazione al servizio.

Example: Action-based condizione

Questa dichiarazione politica garantisce l'accesso a AWS Health Dashboard e AWS Health `Describe*` Operazioni API, ma nega l'accesso a qualsiasi AWS Health eventi relativi ad Amazon EC2.

JSON

```
{
    "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: Resource-based condizione

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

JSON

```
{
  "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: eventoTypeCode condizione

Questa dichiarazione politica garantisce l'accesso a AWS Health Dashboard e AWS Health `Describe*` Operazioni API, ma nega l'accesso a qualsiasi AWS Health eventi con `eventTypeCode` che corrisponde `AWS_EC2_*`.

JSON

```
{
    "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 il DescribeAffectedEntities e DescribeEventDetails operazioni e non sono autorizzati ad accedere a AWS Health evento, il `AccessDeniedException` viene visualizzato un errore. Per ulteriori informazioni, consulta Risoluzione dei problemi AWS Health identità e accesso.

Risoluzione dei problemi AWS Health identità e accesso

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

Argomenti

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

Non sono autorizzato a eseguire un'azione in AWS Health

Se Console di gestione AWS indica 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.

Il `AccessDeniedException` l'errore appare quando un utente non dispone dell'autorizzazione all'uso AWS Health Dashboard o AWS Health Operazioni API.

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

Le AWS Health L'API richiede un AWS Supporto aziendale+, AWS Supporto aziendale, o AWS Piano operativo unificato di Supporto AWS. Se chiami il AWS Health API da un account che non dispone

di un AWS Supporto aziendale+, AWS Supporto aziendale, o AWS Piano operativo unificato, viene restituito il seguente codice di errore: `SubscriptionRequiredException`.

Non sono autorizzato a esibirmi: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 trasmettere il ruolo al servizio.

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

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

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è 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, è necessario concedere l'autorizzazione alle persone o alle applicazioni che devono accedere. Se stai usando Centro identità AWS IAM per gestire persone e applicazioni, si assegnano set di autorizzazioni a utenti o gruppi per definire il loro livello di accesso. I set di autorizzazioni creano e assegnano automaticamente politiche IAM ai ruoli IAM associati alla persona o all'applicazione. Per ulteriori informazioni, consulta Set di autorizzazioni nel Centro identità AWS IAM Guida per l'utente.

Se non utilizzi IAM Identity Center, devi creare entità IAM (utenti o ruoli) per le persone o le applicazioni che necessitano dell'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 AWS. Per saperne di più sulla creazione di utenti, gruppi, policy e autorizzazioni IAM, consulta Identità IAM e Politiche e autorizzazioni in IAM nel Guida per l'utente IAM.

Voglio permettere a persone esterne alla mia AWS account per accedere al mio AWS Health risorse

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

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Health supporta queste funzionalità, vedi In che modo AWS Health funziona con IAM.
- Per sapere come fornire l'accesso alle tue risorse in tutto il mondo Account AWS che possiedi, vedi Fornire l'accesso a un utente IAM in un altro Account AWS che possiedi nel Guida per l'utente IAM.
- Per sapere come fornire l'accesso alle tue risorse a terze parti Account AWS, vedi Fornire l'accesso a Account AWS di proprietà di terzi nel Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per AWS Health

AWS Health utilizza AWS Identity and Access Management (SONO) ruoli collegati ai servizi. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a AWS Health. Service-linked i ruoli sono predefiniti da AWS Health e includono tutte le autorizzazioni richieste dal servizio per chiamare altri Servizi AWS per te.

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

Service-linked autorizzazioni di ruolo per AWS Health

AWS Health ha tre ruoli collegati ai servizi:

- AWSServiceRoleForHealth_Organizations — Questo ruolo si affida a AWS Health (`health.amazonaws.com`) per assumere il ruolo di accesso Servizi AWS per te. Allegato a questo ruolo c'è il `Health_OrganizationsServiceRolePolicy` AWS politica gestita.
- AWSServiceRoleForHealth_EventProcessor — Questo ruolo si fida del AWS Health responsabile del servizio (`event-processor.health.amazonaws.com`) per assumere il ruolo al posto tuo. Allegato a questo ruolo c'è il `AWSHealth_EventProcessorServiceRolePolicy` AWS politica gestita. Il responsabile del servizio utilizza il ruolo per creare un Amazon EventBridge regola gestita per AWS Rilevamento e risposta agli incidenti. Questa regola è l'infrastruttura richiesta nel tuo

Account AWS per inviare informazioni sulla modifica dello stato di allarme dal tuo account a AWS Health.

- AWSServiceRoleForTagsHealth — Questo ruolo si affida a AWS Health responsabile del servizio (`tags.health.amazonaws.com`) per assumere il ruolo al posto tuo. Allegato a questo ruolo c'è il TagsHealthServiceRolePolicy AWS politica gestita. Il responsabile del servizio utilizza il ruolo per leggere i tag sulle risorse del tuo account tramite AWS Resource Groups Tagging API, in modo che AWS Health puoi mostrare il tuo AWS Health eventi per tag di risorsa.

Per ulteriori informazioni su AWS politiche gestite, vedere AWS politiche gestite per AWS Health.

Creazione di un ruolo collegato ai servizi per AWS Health

Non è necessario creare il AWSServiceRoleForHealth_Organizations ruolo collegato al servizio. Quando chiami il EnableHealthServiceAccessForOrganization operazione, AWS Health crea questo ruolo collegato al servizio nell'account per te.

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

Non è necessario creare il AWSServiceRoleForTagsHealth ruolo collegato al servizio. Quando attivi la funzionalità dei tag per il tuo account, AWS Health crea il ruolo nel tuo account per te. Quando attivi la funzionalità dei tag per la tua organizzazione dall'account di gestione dell'organizzazione, AWS Health crea il ruolo nell'account di gestione e in ogni account membro dell'organizzazione. AWS Health crea anche il ruolo in qualsiasi account che entra a far parte dell'organizzazione dopo aver attivato la funzionalità.

Modifica di un ruolo collegato ai servizi per AWS Health

AWS Health non 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 al servizio 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 il DisableHealthServiceAccessForOrganization operazione. È quindi possibile eliminare il ruolo tramite la console IAM, l'API IAM o AWS Command Line Interface (AWS CLI).

Per eliminare AWSServiceRoleForHealth_EventProcessor ruolo, contatto Supporto AWS e chiedi loro di alleggerire i tuoi carichi di lavoro da AWS Rilevamento e risposta agli incidenti. Al termine di questo processo, puoi eliminare entrambi i ruoli tramite la console IAM, l'API IAM o AWS CLI.

Per eliminare AWSServiceRoleForTagsHealth ruolo, devi prima disattivare la funzionalità dei tag per l'account. Se l'account appartiene a un'organizzazione in cui la funzionalità dei tag è attivata, anche l'account di gestione dell'organizzazione deve disattivare la funzionalità dei tag per l'organizzazione. Se si tenta di eliminare il ruolo mentre la funzionalità dei tag è ancora abilitata per l'account o la relativa organizzazione, l'eliminazione non riesce e IAM segnala che il ruolo è utilizzato da AWS Health. Dopo aver disabilitato la funzionalità, puoi eliminare il ruolo 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

Un AWS una politica gestita è una politica autonoma creata e amministrata da AWS. AWS le policy 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 AWS le policy gestite potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti AWS clienti da utilizzare. Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

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

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

AWS Health dispone delle seguenti politiche gestite.

Indice

- AWS politica gestita: AWSHealth_EventProcessorServiceRolePolicy
- AWS politica gestita: Health_OrganizationsServiceRolePolicy
- AWS politica gestita: TagsHealthServiceRolePolicy
- AWS politica gestita: AWSHealthFullAccess
- AWS Health aggiornamenti a AWS policy gestite

AWS politica gestita: AWSHealth_EventProcessorServiceRolePolicy

AWS Health utilizza il AWSHealth_EventProcessorServiceRolePolicy AWS politica 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 per te. 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 da consentire AWS Health per accedere ad Amazon EventBridge regola per AWS Rilevamento e risposta agli incidenti.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

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

JSON

```
{
    "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, vedere AWS Health aggiornamenti a AWS policy gestite.

AWS politica gestita: Health_OrganizationsServiceRolePolicy

AWS Health utilizza il Health_OrganizationsServiceRolePolicy AWS politica 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 per te. 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 autorizzazioni che consentono AWS Health per accedere è richiesto AWS Organizations dettagli per la visualizzazione dell'organizzazione sanitaria.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations` — Descrive gli account in AWS Organizations e il Servizi AWS che può essere utilizzato con le organizzazioni.

JSON

```
{
    "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, consulta AWS Health aggiornamenti a AWS policy gestite.

AWS politica gestita: TagsHealthServiceRolePolicy

AWS Health utilizza il TagsHealthServiceRolePolicy AWS politica gestita. Questa policy gestita è attribuita al ruolo collegato ai servizi `AWSServiceRoleForTagsHealth`. La policy consente al ruolo collegato al servizio di completare le azioni per te. 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 autorizzazioni di sola lettura che consentono AWS Health per leggere i tag sulle risorse del tuo account. AWS Health utilizza questi tag in modo da poter visualizzare e filtrare i tuoi AWS Health eventi per tag di risorsa. Con questa politica, AWS Health non può creare, modificare o rimuovere tag e non può accedere alle risorse stesse.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `tag` — Recupera le risorse nel tuo account e i tag ad esse allegati tramite AWS Resource Groups Tagging API.

Per vedere le autorizzazioni per questa policy, consulta TagsHealthServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

Per un elenco delle modifiche alla politica, consulta AWS Health aggiornamenti a AWS policy gestite.

AWS politica gestita: AWSHealthFullAccess

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

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations` — Attivare o disattivare il AWS Health funzionalità di visualizzazione organizzativa per tutti gli account in un AWS organizzazione e visualizza le unità organizzative (OU) dell'account di gestione
- `health` — Accesso al AWS Health Operazioni e notifiche API
- `iam` — Crea un ruolo IAM collegato a AWS Health servizio

JSON

```
{
    "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, vedere AWS Health aggiornamenti a AWS policy gestite.

AWS Health aggiornamenti a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti di AWS politiche gestite per AWS Health da quando questo servizio ha iniziato a tracciare 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 gli aggiornamenti importanti di AWS Health politiche gestite dal 13 gennaio 2022.

AWS Health

Modifica	Descrizione	Data
AWS politica gestita: TagsHealthServiceRolePolicy: nuova policy	AWS Health ha aggiunto una nuova politica gestita allegata al `AWSServiceRoleForTagsHealth` ruolo collegato al servizio. La policy garantisce l'accesso in sola lettura a AWS Resource Groups Tagging API in modo che AWS Health puoi leggere i tag sulle risorse del tuo account. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health.	30 ottobre 2026
AWS politica gestita: AWSHealthFullAccess - Aggiornamento a una policy esistente	AWS Health ha ampliato il AWSHealthFullAccess politica per AWS GovCloud (US) Regions e le regioni della Cina.	16 ottobre 2023
AWS politica gestita: Health_OrganizationsServiceRolePolicy - Aggiornamento a una policy esistente	AWS Health ne ha aggiunti di nuovi AWS Organizations azioni per consentire al ruolo collegato al servizio di descrivere gli account e AWS servizi che possono essere utilizzati con AWS Organizations.	19 luglio 2023
Log delle modifiche pubblicato	Registro delle modifiche per AWS Health politiche gestite.	13 gennaio 2023

Registrazione e monitoraggio AWS Health

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni di AWS Health e il tuo altro AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio da monitorare AWS Health, segnala quando qualcosa non va e intraprendi le azioni appropriate:

- Amazon CloudWatch monitora il tuo AWS le risorse e le applicazioni su cui esegui AWS in tempo reale. È possibile raccogliere e tenere traccia dei parametri, 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 avere CloudWatch monitora l'utilizzo della CPU o altre metriche delle tue istanze Amazon Elastic Compute Cloud (Amazon EC2) e avvia automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch Guida per l'utente.
- Amazon EventBridge fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche in 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 in AWS Health con Amazon EventBridge.
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto dell'utente AWS account e invia i file di registro a un bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e la data in cui sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente di AWS CloudTrail.

Per ulteriori informazioni, consulta Monitoraggio AWS Health.

Convalida della conformità per AWS Health

Il nostro nuovo AWS l'esperienza di iscrizione non è progettata per carichi di lavoro regolamentati. Se stai usando il nostro nuovo AWS esperienza di registrazione, ma desideri utilizzarla AWS per carichi di lavoro regolamentati, puoi iscriviti a AWS (avanzato) o attivare funzionalità avanzate per il tuo AWS ambiente.

Per sapere se un Servizio AWS rientra nell'ambito di specifici programmi di conformità, vedere Servizi AWS nell'ambito del programma di conformità e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta AWS Programmi di conformità.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, vedere Scaricamento dei report in AWS Artifact.

La tua responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità dell'utente in materia di conformità durante l'utilizzo Servizi AWS, vedi AWS Documentazione sulla sicurezza.

Resilienza in AWS Health

Le AWS l'infrastruttura globale è costruita intorno AWS Regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate a reti a bassa latenza, alta produttività 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 in più zone di disponibilità. Questo approccio garantisce che sia possibile accedervi da Dashboard Health o il AWS Health operazioni API. È possibile visualizzare AWS Health eventi fino a 90 giorni dalla data in cui si sono verificati.

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

Sicurezza dell'infrastruttura in AWS Health

Come servizio gestito, AWS Health è protetto da AWS procedure globali di sicurezza della rete descritte nella Amazon Web Services: panoramica dei processi di sicurezza white paper.

Tu usi AWS chiamate API 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 clienti devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECCHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare Servizio di token di sicurezza AWS (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 AWS e tu, nostro cliente. Per ulteriori informazioni, consulta la AWS modello di responsabilità condivisa.

Le migliori pratiche di sicurezza per AWS Health

Consulta le seguenti best practice per lavorare con AWS Health.

Grant AWS Health autorizzazioni minime possibili per gli utenti

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

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

Visualizza il Dashboard Health

Controlla il tuo Dashboard Health spesso per identificare 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 Per iniziare con il tuo AWS Health Dashboard.

Integra AWS Health con Amazon Chime o Slack

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

Monitor per AWS Health eventi

Puoi integrare AWS Health con Amazon CloudWatch Eventi, 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 Eventi Gli eventi sono Region-specific, quindi è necessario configurare questo servizio nella regione in cui risiede l'applicazione o l'infrastruttura.

In alcuni casi, la regione di AWS Health l'evento non può essere determinato. Se si verifica tale situazione, l'evento viene visualizzato per impostazione predefinita nella regione Stati Uniti orientali (Virginia settentrionale). Puoi configurare CloudWatch Eventi in questa regione per assicurarti di monitorare questi eventi.

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

Aggregazione AWS Health eventi tra gli account

Per impostazione predefinita, puoi AWS Health utilizzarlo per visualizzare gli AWS Health eventi di un singolo AWS account. Se lo usi 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.

Puoi aggregare gli eventi per identificare gli account della tua 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 imminenti modifiche 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 agli AWS Health eventi dell'organizzazione. La funzione Amministratore delegato consente di mantenere limitato l'account di gestione, fornendo al contempo ai team la visibilità di cui hanno bisogno per intervenire sugli AWS Health eventi.

> **Important**
>
> - AWS Health gli eventi inviati per gli account dell'organizzazione verranno visualizzati nella visualizzazione dell'organizzazione finché l'evento è disponibile, fino a 90 giorni, anche se uno o più di questi 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, devi:

- 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 (opzione non consigliata) nell'account di gestione della tua organizzazione. Per maggiori informazioni, consulta Bloccare le chiavi di accesso utente root del tuo AWS account nella IAM User Guide.

- Se accedi come utente IAM, utilizza una policy IAM che conceda l'accesso alle azioni AWS Health e alle organizzazioni, come la AWSHealthFullAccess policy. Per ulteriori informazioni, consulta AWS Health esempi di policy 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 nella 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 AWSHealthFullAccess policy. Per ulteriori informazioni, consulta AWS Health esempi di policy basate sull'identità.

Enabling organizational view (Console)

Puoi abilitare la visualizzazione organizzativa dalla AWS Health console. Devi accedere all'account di gestione della tua AWS organizzazione.

Per visualizzare AWS Health Dashboard per la tua organizzazione

1. Apri la tua AWS Health dashboard all'indirizzo https://health.aws.amazon.com/health/home.

2. Nel pannello di navigazione, in 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 la creazione di unità organizzative (OU), 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 potrebbe richiedere diversi minuti per essere completato. Puoi chiudere la AWS Health console e tornare più tardi, poiché non devi attendere il completamento del processo. La cronologia degli eventi sanitari (quelli creati prima dell'attivazione della funzionalità) potrebbe richiedere fino a 24 ore per essere visualizzati nella visualizzazione organizzativa.
> - Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi chiamare l'operazione DescribeHealthServiceStatusForOrganization API 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 EnableHealthServiceAccessForOrganization API.

Puoi usare AWS Command Line Interface (AWS CLI) o il tuo codice per chiamare questa operazione.

> **Note**
>
> - È necessario disporre di un piano di supporto Business On-Ramp, Enterprise o Enterprise 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 EnableHealthServiceAccessForOrganization API.

Python

```
import boto3

client = boto3.client('health', region_name='us-east-1')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

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

```
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 policy `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

Puoi utilizzare la AWS Health console per ottenere una visualizzazione centralizzata degli eventi sanitari nella 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 AWSHealthFullAccess policy. Per ulteriori informazioni, consulta AWS Health esempi di policy basate sull'identità.

Viewing organizational view events (Console)

Dopo aver abilitato la visualizzazione organizzativa, AWS Health visualizza gli eventi relativi allo stato di salute di tutti gli account dell'organizzazione.

Quando un account entra a far parte dell'organizzazione, AWS Health lo aggiunge automaticamente alla visualizzazione dell'organizzazione. 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 effettiva della chiusura dell'account amministratore. Alla fine del periodo di 90 giorni, elimina AWS definitivamente tutti i dati relativi alle politiche 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.
- Purché AWS conservi i dati della politica, quando riapri l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati dei criteri di servizio per l'account.
- Per ulteriori informazioni, consulta Chiusura di un account.

Important

Per i clienti nelle 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 presenti nella AWS Health Dashboard — Service Health negli ultimi 7 giorni. Questi eventi pubblici non sono specifici per gli account della tua organizzazione. Eventi dal AWS Health dashboard — Service health forniscono 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 modifiche Servizi AWS e risorse che influiscono sull'organizzazione.

Per visualizzare gli eventi di visualizzazione dell'organizzazione

1. Apri la tua AWS Health dashboard all'indirizzo https://health.aws.amazon.com/health/home.
2. Nel pannello di navigazione, in 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
   - Description

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 programmata 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 di 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 dell'evento , lo stato e l'ora di inizio.

Per visualizzare gli eventi di visualizzazione organizzativa nella scheda Registro eventi

1. Apri la tua AWS Health dashboard all'indirizzo https://health.aws.amazon.com/health/home.
2. Nel pannello di navigazione, in Lo stato della tua organizzazione, scegli Registro eventi.
3. In Registro eventi, scegli il nome dell'evento. Puoi rivedere le seguenti informazioni sull'evento:
   - Nome evento
   - Stato
   - Regione/Zona di disponibilità
   - Account interessati
   - Ora di inizio
   - Ora di fine
   - Categoria
   - Description

Viewing affected accounts and resources (Console)

In 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 istanze Amazon EC2 possono essere visualizzati 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 tua AWS Health dashboard all'indirizzo https://health.aws.amazon.com/health/home.
2. Nel riquadro di navigazione, in 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 dell'attivazione della 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 effettiva della chiusura dell'account amministratore. Alla fine del periodo di 90 giorni, elimina AWS definitivamente tutti i dati relativi alle politiche 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.
- Purché AWS conservi i dati della politica, quando riapri l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati dei criteri di servizio per l'account.

- Per ulteriori informazioni, consulta Chiusura di un account.

> **Important**
>
> Per i clienti nelle 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 gli eventi dal punto di vista organizzativo.

Example: descrivere gli eventi di visualizzazione organizzativa

Il AWS CLI comando seguente restituisce gli eventi di integrità 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 ai servizi nella Guida per l'utente 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, chiamate l'operazione RegisterDelegatedAdministratorAPI. Dopo aver registrato gli account dei membri, questi diventano un account amministratore delegato 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 storici 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 in AWS Health con Amazon EventBridge

Puoi usare Amazon EventBridge per rilevare e reagire agli AWS Health eventi. Quindi, in base alle regole che crei, EventBridge 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 hai AWS risorse a disposizione per Account AWS cui sono previsti aggiornamenti, come le istanze Amazon Elastic Compute Cloud (Amazon EC2).

> **Note**
>
> - AWS Health fornisce eventi su base duratura e tenta di distribuirli con successo EventBridge almeno una volta.
> - Tutte EventBridge le regole che crei possono ricevere notifiche solo per te Account AWS. Per ricevere eventi organizzativi per altri account all'interno del tuo AWS Organizations, vedi Aggregazione AWS Health degli eventi utilizzando la vista organizzativa e l'accesso amministratore delegato.
> - L'invio degli eventi sulla salute pubblica potrebbe richiedere fino a un'ora dopo la creazione di una EventBridge regola.

Puoi scegliere tra diversi 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)
- Built-in obiettivi (ad esempio azioni CloudWatch di allarme)
- Argomenti su Amazon Simple Notification Service (Amazon SNS)

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

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

Argomenti

- Creazione di EventBridge regole per Regione AWS copertura
- Monitoraggio di eventi pubblici e specifici per account per AWS Health
- Visualizzazione di elenchi suddivisi in pagine di AWS Health eventi in corso EventBridge
- Aggregazione AWS Health eventi che utilizzano la visualizzazione organizzativa e l'accesso amministratore delegato
- Integrazione AWS Health monitoraggio e notifiche degli eventi con JIRA e ServiceNow
- Configurazione di una EventBridge regola per inviare notifiche sugli eventi in AWS Health
- Configurazione di Amazon Q Developer in applicazioni di chat per inviare notifiche sugli eventi in AWS Health
- Esecuzione automatica delle operazioni sulle istanze EC2 in risposta agli eventi in AWS Health
- Riferimento: AWS Health eventi Amazon EventBridge schema

Creazione di EventBridge regole per Regione AWS copertura

Puoi creare una EventBridge regola per ogni regione per la quale desideri ricevere AWS Health eventi. Ad esempio, per ricevere eventi dalla regione Europa (Francoforte), puoi creare una regola per questa regione.

Per migliorare l'affidabilità delle AWS Health notifiche, puoi impostare regole nelle regioni di backup dedicate. Nella AWS partizione standard, la regione Stati Uniti occidentali (Oregon) funge da regione di backup per tutte le altre regioni, mentre la regione Stati Uniti orientali (Virginia settentrionale) funge da backup per la regione Stati Uniti occidentali (Oregon). Quando si verificano eventi sanitari, questi vengono inviati automaticamente sia alla regione principale che alla regione di backup designata. Ad esempio, se stai monitorando gli eventi nella regione Europa (Francoforte), tutti gli eventi relativi alla salute vengono inviati sia nella regione Europa (Francoforte) che nella regione Stati Uniti occidentali (Oregon). Questo sistema ti assicura di continuare a ricevere notifiche sullo stato di salute anche in caso di problemi nella tua regione principale. Per creare una regola di backup, segui la procedura perConfigurazione di una EventBridge regola per inviare notifiche sugli eventi in AWS Health.

Se preferisci non utilizzare la funzionalità di backup, devi aggiungere un filtro alla regola della regione di backup. Ad esempio, implementa un filtro per`detail.backupEvent = False`. Ciò impedisce di ricevere eventi di backup da altre regioni.

Configurazione ad alta disponibilità (opzionale)

Se desideri creare un' EventBridge integrazione con disponibilità elevata, assicurati di aver implementato le regole sia nella regione pertinente che in quella di backup, quindi implementa la deduplicazione utilizzando. `detail.communicationId` Questo ti assicura di ricevere tutti gli eventi evitando i duplicati. Per ulteriori informazioni, consulta Riferimento: AWS Health eventi Amazon EventBridge schema.

Integrazione semplificata

Se desideri acquisire eventi specifici dell'account da più account Regioni AWS, ma preferisci configurare solo una singola regola, l'integrazione semplificata è l'opzione appropriata. Per ricevere AWS Health eventi specifici dell'account da tutte le regioni della AWS partizione standard, puoi impostare una regola centrale nella regione Stati Uniti occidentali (Oregon). Questa singola regola aggrega automaticamente gli eventi specifici dell'account provenienti da tutte le regioni di partizione standard. Tuttavia, non avrai una configurazione ad alta disponibilità.

> **Note**
>
> L'integrazione semplificata non consente di ricevere eventi pubblici visualizzati nella AWS Health Dashboard. L'integrazione semplificata è consigliata solo per l'inserimento di eventi che richiedono un'azione. AWS Health Per ulteriori informazioni sugli eventi pubblici e specifici dell'account, consulta. Monitoraggio di eventi pubblici e specifici per account per AWS Health

Eventi globali

Alcuni AWS Health eventi non lo sono Region-specific. Gli eventi che non sono specifici di una regione sono denominati eventi globali. Questi includono gli eventi inviati per AWS Identity and Access Management (IAM). Per ricevere eventi globali, devi creare una regola per la regione Stati Uniti orientali (Virginia settentrionale).

Monitoraggio di eventi pubblici e specifici per account per AWS Health

Quando si crea una EventBridge regola da cui monitorare gli eventi AWS Health, la regola fornisce sia eventi specifici dell'account che eventi pubblici:

- Account-specificgli eventi influiscono sull'account e sulle risorse, ad esempio un evento che indica un aggiornamento richiesto a un'istanza Amazon EC2 o altri eventi di modifica pianificati.
- Gli eventi pubblici vengono visualizzati nel AWS Health Dashboard — Service health. 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.

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

Per visualizzare un esempio di evento pubblico per Amazon Elastic Compute Cloud, consultaEvento sulla salute pubblica - Problema operativo di Amazon EC2.

Regole di backup per AWS Health eventi

Se stai monitorando eventi pubblici da un Regione AWS, ti consigliamo di creare una regola di backup. Gli eventi pubblici per AWS Health vengono inviati simultaneamente sia alla regione interessata che alla regione di backup quando viene impostata una regola valida nella regione interessata.

> **Important**
>
> Se non hai una regola nella regione interessata, la regione di backup non invierà automaticamente l'evento pubblico come backup. È necessario disporre di una regola valida

nella regione interessata affinché gli eventi pubblici vengano distribuiti nella regione di backup.

AWS Health invia eventi specifici dell'account sia alla regione interessata che alla regione di backup, indipendentemente dalle regole configurate nella regione interessata.

Si consiglia di deduplicare AWS Health gli eventi utilizzando `eventARN` e `communicationId` poiché questi valori rimangono coerenti per i AWS Health messaggi inviati alla regione di backup.

Visualizzazione di elenchi suddivisi in pagine di AWS Health eventi in corso 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 EventBridge di 256 KB.

AWS Health include tutti i `detail.affectedEntities` campi `resources` e del messaggio. Se questo elenco di `detail.affectedEntities` valori `resources` e supera i 256 KB, AWS Health suddivide l'evento di integrità in più pagine e pubblica queste pagine come singoli messaggi in. EventBridge Ogni pagina mantiene gli stessi `eventARN` `communicationId` valori per aiutare a ricombinare l'elenco di `resources` o `detail.affectedEntities` dopo che tutte le pagine sono state ricevute.

Questi messaggi aggiuntivi potrebbero causare 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 possono aggiungere un filtro per consentire al `detail.page` campo di elaborare solo la prima pagina, eliminando così i messaggi non necessari creati dalle pagine successive.

Nello schema, ogni CommunicationID include il numero di pagina con trattino dopo il communicationID, anche quando è presente una sola pagina. I campi `detail.page` e `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 AWS Health eventi che utilizzano la visualizzazione organizzativa e l'accesso amministratore delegato

AWS Health supporta la visualizzazione organizzativa e l'accesso amministratore delegato per AWS Health gli eventi pubblicati su Amazon. EventBridge Quando la visualizzazione organizzativa è attiva AWS Health, l'account di gestione o un account amministratore delegato riceve un singolo feed di AWS Health eventi da tutti gli account all'interno della tua 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. L'impostazione 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 amministratore delegato AWS Health, consulta Aggregazione degli AWS Health eventi.

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

⚠ Avviso di fine del supporto

Il 31 marzo 2027, AWS terminerà il supporto per. AWS Service Management Connector Dopo il 31 marzo 2027, non sarà più possibile accedere alla console di Service Management Connector o alle risorse di Service Management Connector. Per ulteriori informazioni, vedi AWS Service Management Connector fine del supporto.

Puoi integrare AWS Health gli eventi con JIRA e ServiceNow ricevere informazioni operative e sull'account, prepararti per le modifiche programmate e gestire gli eventi sanitari utilizzando il Service Management Connector (SMC). L'integrazione con SMC AWS Health può utilizzare gli eventi sanitari inviati EventBridge per creare, mappare e aggiornare automaticamente i ticket e gli incidenti JIRA. ServiceNow

Puoi utilizzare la visualizzazione organizzativa e l'accesso amministratore delegato per gestire facilmente gli eventi sanitari 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, consulta Integrating in. AWS Health ServiceNow

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

Configurazione di una EventBridge regola per inviare notifiche sugli eventi in AWS Health

Puoi creare una EventBridge regola Amazon per integrare programmaticamente AWS Health gli eventi con altri servizi, applicazioni e carichi di lavoro. EventBridge fornisce un'interfaccia di console drag and drop e un'API per impostare regole che si attivano quando viene creato un AWS Health evento corrispondente per il tuo account o la tua organizzazione. Per informazioni su come impostare una regola per EventBridge acquisire AWS Health eventi, consulta Creating rules using the Enhanced Builder e Creating rules using the Advanced Builder nella Amazon EventBridge User Guide.

A seconda dell'integrazione, ti EventBridge consente di aggiungere parametri alla EventBridge regola per filtrare solo gli AWS Health eventi che desideri integrare nel tuo caso d'uso. Per i casi d'uso relativi alla risposta agli incidenti, potresti concentrarti sulla categoria `issue` degli eventi e su alcuni servizi critici. Per i casi d'uso della gestione delle modifiche, ad esempio gli eventi del ciclo di vita pianificati, potresti concentrarti sugli AWS Health eventi `ACTION_REQUIRED` nel campo Actionability. Per l'integrazione con i casi d'uso relativi alla sicurezza, potresti concentrarti su tutti gli eventi di AWS Health abuso e AWS Health sugli eventi con il campo persona. `SECURITY`

Puoi utilizzare esempi di casi d'uso per verificare che la tua regola raccolga gli eventi di cui hai bisogno. Esempi di casi d'uso sono disponibili inRiferimento: AWS Health eventi Amazon EventBridge schema. Puoi trovarli anche nella EventBridge console, sotto l'opzione Usa gli eventi di esempio forniti nel modello di eventi di test - pannello opzionale

Utilizzando l'API o AWS Command Line Interface

Per una regola nuova o esistente, usa l'operazione PutRule API o il `aws events put-rule` comando per aggiornare il pattern degli eventi. Per visualizzare un AWS CLI comando di esempio, vedi put-rule nel AWS CLI Command Reference.

Example Esempio: impostazione di regole per i problemi solo per il servizio Amazon EC2

Il seguente schema di eventi crea una regola per monitorare gli eventi di problema per il servizio Amazon EC2.

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

Example Esempio: impostazione delle regole per tutte le azioni richieste AWS Health eventi, inclusi gli eventi del ciclo di vita pianificati

Il seguente schema di eventi crea una regola per monitorare tutti AWS Health gli eventi che richiedono un'azione, inclusi gli eventi del ciclo di vita pianificati.

```
{
  "detail": {
    "eventTypeCategory": [
      "accountNotification",
      "scheduledChange"
    ],
    "actionability": [
      "ACTION_REQUIRED"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
```

```
  ]
}
```

Example Esempio: impostazione di regole per tutti AWS Health eventi per 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 i tipi di `scheduledChange` evento per tre AWS servizi: Amazon EC2 Auto Scaling, Amazon VPC e Amazon EC2. `accountNotification`

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

Configurazione di Amazon Q Developer in 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 i 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 disporre di 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 Getting started with Amazon Q Developer in chat applications nella Amazon Q Developer in chat applications Administrator Guide.
- 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 le istruzioni per impostare una regola in Amazon EventBridge per catturare AWS Health gli eventi descritti in Creating rules using the Enhanced Builder e Creating rules using the Advanced Builder nella Amazon EventBridge User Guide. Per ulteriori informazioni, consulta Configurazione di una EventBridge regola per inviare notifiche sugli eventi in AWS Health.

   a. Al termine della configurazione dello schema degli eventi, 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 . Consulta Visualizzazione di elenchi suddivisi in pagine di AWS Health eventi in corso EventBridge.

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

   b. Quando scegli il target, scegli un argomento SNS. Utilizzi lo stesso argomento SNS nella console delle applicazioni Amazon Q Developer in chat.

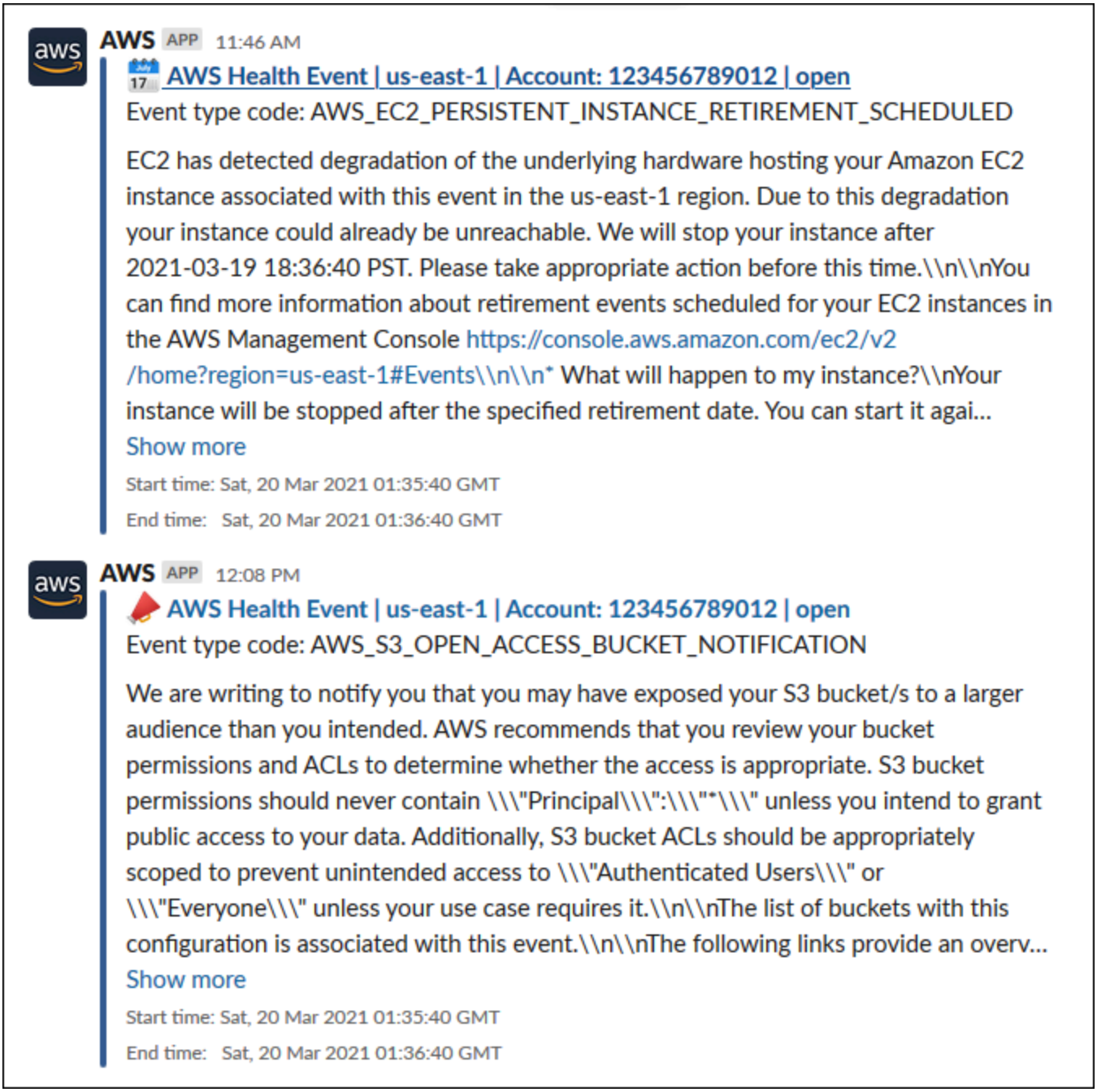
   c. Completa il resto della procedura per creare la regola.
2. Accedi alla console delle applicazioni Amazon Q Developer in chat.
3. Scegli il tuo client di chat, ad esempio il nome del tuo canale Slack, quindi scegli Modifica.
4. Nella sezione Notifiche - opzionale, per Argomenti, scegli lo stesso argomento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

   Quando AWS Health invia un evento a EventBridge cui corrisponde la 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 istanze EC2 in risposta agli eventi in AWS Health

Puoi automatizzare le azioni che rispondono agli eventi pianificati per le tue istanze Amazon EC2. Quando AWS Health invia un evento al tuo AWS account, la tua 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 dell'istanza Amazon EC2 per un'istanza EC2 supportata da Amazon Elastic Block Store (Amazon EBS), AWS Health invierà il tipo di evento alla tua dashboard. `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` 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 istanze Amazon EC2, 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 Console di gestione AWS 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 JSON e quindi sostituisci il JSON predefinito nell'editor.

   JSON

```
{
  "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 Revisione della politica, inserisci un Nome, ad esempio *`AutomationEVRolePolicy`* e una Descrizione opzionale.
10. Rivedi la pagina di riepilogo per visualizzare 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 service

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello 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 EC2 per il servizio a cui desideri consentire di assumere questo ruolo.
5. Scegli Successivo: autorizzazioni.
6. Inserisci il nome della policy che hai creato, ad esempio*`AutomationEVRolePolicy`*, quindi seleziona la casella di controllo accanto alla policy.

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 che appare nell'ARN della policy IAM che hai creato.
11. (Facoltativo) In Descrizione del ruolo, immetti una descrizione per il nuovo ruolo.
12. Rivedere il ruolo e scegliere Crea ruolo.

Per ulteriori informazioni, consulta Creazione di un ruolo per un AWS servizio 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 fiducia per il ruolo

1. Accedi Console di gestione AWS 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 JSON, rimuovi la policy predefinita e incolla il JSON copiato al suo posto.

   JSON

```
{
    "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 istanze EC2 pianificate per il ritiro.

Per creare una regola per le azioni automatiche di EventBridge 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 Definisci modello, scegli Schema evento, quindi scegli Pre-defined modello per servizio.
5. Per Service provider (Provider di servizi), selezionare AWS.
6. Per Nome del servizio, scegli Salute.
7. Per Tipo di evento, scegli Eventi sanitari specifici.
8. Scegli Servizi specifici, quindi scegli EC2.
9. Scegli Categorie di tipi di eventi specifici, quindi scegli ScheduledChange.
10. Scegli Codici per tipi di eventi specifici, quindi scegli il codice del tipo di evento.

    Ad esempio, per le EBS-backed istanze Amazon EC2, scegli. **AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED** Per le istanze supportate da un archivio di istanze Amazon EC2, scegli. **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**
11. Seleziona Qualsiasi risorsa.

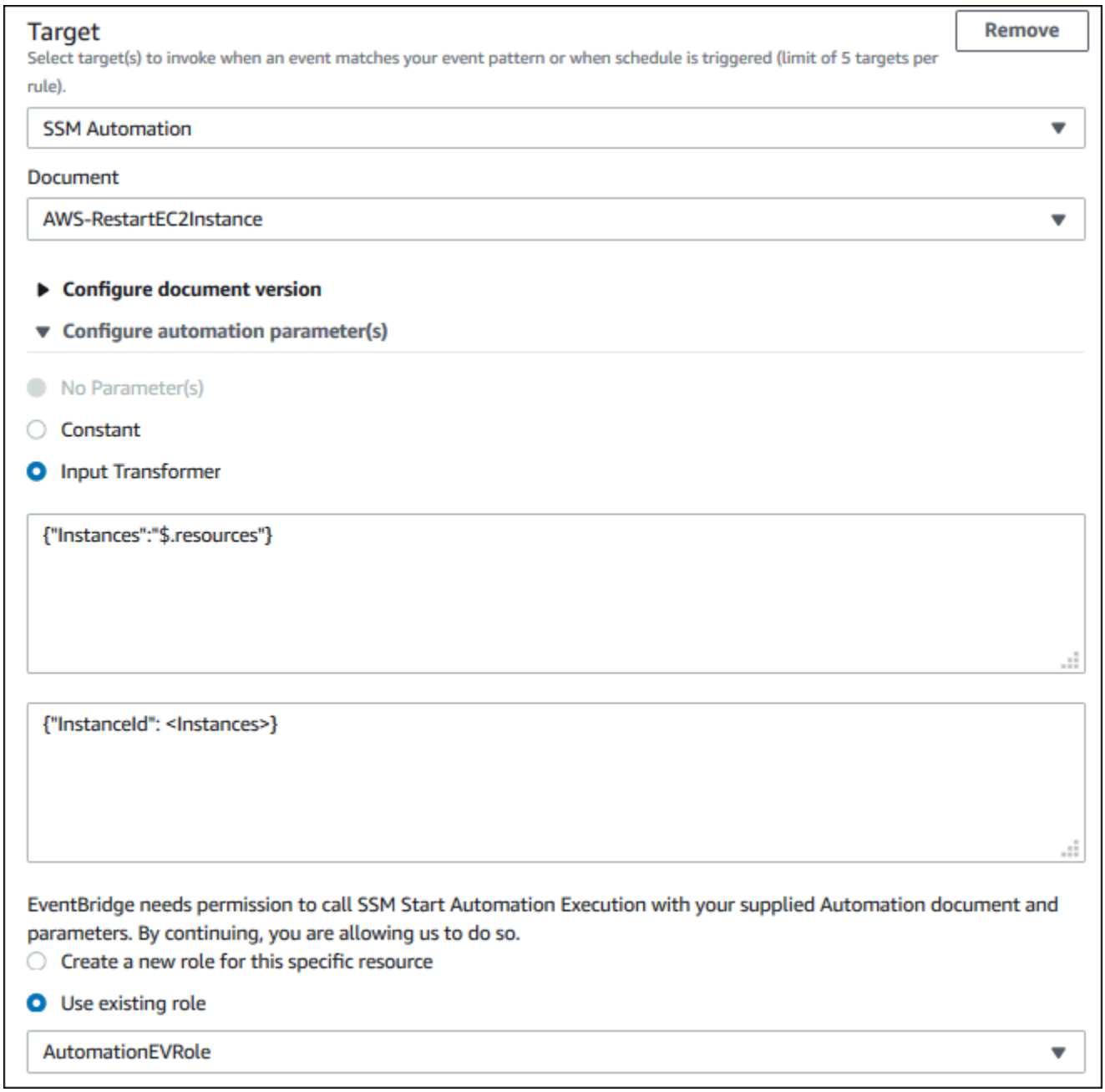
    Il tuo modello di evento sarà simile all'esempio seguente.

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 Percorso di input, inserisci**`{"Instances":"$.resources"}`**.
16. Per il secondo campo, inserisci**`{"InstanceId": <Instances>}`**.
17. Scegli Usa ruolo esistente, quindi scegli il ruolo IAM che hai creato, ad esempio*`AutomationEVRole`*.

    Il tuo obiettivo dovrebbe assomigliare al seguente esempio.



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

18. Scegli Crea.

Se nel tuo account si verifica un evento che corrisponde alla tua regola, EventBridge invierà l'evento al target specificato.

Riferimento: AWS Health eventi Amazon EventBridge schema

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

AWS Health schema evento

AWS Health schema evento

Parametro	Description	Richiesto
versione	EventBridge versione, attualmente «0".	Sì
id	L'identificatore univoco dell'evento. EventBridge	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	Description	Richiesto
source (origine)	La fonte del bus degli eventi. Per AWS Health gli eventi, il valore supportato è `aws.health`	Sì

Parametro	Description	Richiesto
account	L'ID dell'account a cui è stato inviato l'AWS Health evento. **Note** Dal punto di vista organizzativo, si tratta di un account diverso dall'account interessato se ricevuto nell'account di gestione o nell'account amministratore delegato.	Sì

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

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

Parametro	Description	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 degli eventi: contenuto del parametro di dettaglio

contenuto del parametro 'detail'	Description	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 univoco per una regione specifica Account AWS .	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
Evento .TypeCode	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 'detail'	Description	Richiesto
	due settimane prima dell'orario di inizio. **Note** Tutti i nuovi eventi del ciclo di vita pianificati hanno questo tipo di evento. `AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT`	
Evento .TypeCategory	Il codice della categoria dell'evento. I valori supportati includono`issue`, `accountNotification` `investigation` , e. `scheduledChange`	Sì
Evento .ScopeCode	Indica se l' AWS Health evento è specifico dell'account o pubblico. I valori supportati sono `ACCOUNT_SPECIFIC` o `PUBLIC`.	Sì

contenuto del parametro 'detail'	Description	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 facilitare la deduplicazione dei messaggi. Con il supporto per l'impaginazione 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 suddivisi in pagine di AWS Health eventi in corso EventBridge.	Sì

contenuto del parametro 'detail'	Description	Richiesto
startTime	L'ora di inizio dell'evento, nel formato. AWS Health `DoW, DD, MMM, YYYY, HH:MM:SS TZ` L'ora di inizio può essere futura per gli eventi programmati.	Sì
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 orario futuro.	No
ultimo UpdatedTime	L'ora dell'ultimo aggiornamento per l' 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
Regione dell'evento	La regione interessata descritta da questo AWS Health evento.	Sì

contenuto del parametro 'detail'	Description	Richiesto
Descrizione dell'evento	Una sezione che descrive l' AWS Health evento. Sono inclusi i campi relativi alla lingua e al 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 l'evento è pubblicato. Ad esempio, nella `us-east-1` Regione, questo è in genereen_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 'detail'	Description	Richiesto
Metadati dell'evento	Metadati aggiuntivi che possono essere forniti per l'evento. AWS Health • <metadata key 1>— Stringhe di coppia 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

contenuto del parametro 'detail'	Description	Richiesto
Entità interessate	Un array che descrive il valore e lo stato delle risorse interessate all'interno dell'even to. AWS Health • EntityValue: l'ID. resource/ entity • lastUpdatedTime: l'ora dell'ultimo aggiornamento di questo resource/entity stato, nel formato. `DoW, DD MMM YYYY HH:MM:SS TZ` • status: lo stato della persona interessata. resource/entity I valori supportati includono `IMPAIREDUNIMPAIRE D ,PENDING,RESOLVED`, e`UNKNOWN`. **Note** Per gli eventi del ciclo di vita pianificati, gli aggiornamenti dello stato delle risorse vengono eseguiti in modo asincrono e periodico e possono avere un ritardo fino a 72 ore in rare occasioni. Per ulteriori informazioni, consulta	No

contenuto del parametro 'detail'	Description	Richiesto
	Cosa devo aspettarmi quando ricevo una notifica relativa a un evento relativo al ciclo di vita pianificato?.	
pagina	La pagina rappresentata da questo messaggio. Per ulteriori informazioni, consulta Visualizzazione di elenchi suddivisi in pagine di AWS Health eventi in corso EventBridge. **Note** L'impaginazione avviene solo sulle risorse. Se il limite di dimensione di 256 KB viene superato per un altro motivo, la comunicazione non riesce.	Sì

contenuto del parametro 'detail'	Description	Richiesto
Pagine totali	Il numero totale di pagine per questo evento sulla salute. Per ulteriori informazioni, consulta Visualizzazione di elenchi suddivisi in pagine di AWS Health eventi in corso EventBridge. Puoi utilizzare questo valore per determinare se hai ricevuto tutte le pagine di una comunicazione multipagina relativa a un account.	Sì
BackupEvent	Questo flag filtra gli eventi di backup nella regione di backup designata all'interno di una partizione se i clienti non vogliono sfruttare la ridondanza. Questo valore può essere vero o falso.	Sì
Account interessato	L'ID dell'account interessato. Questo può essere diverso dal valore nel `account` campo se questo evento di integrità viene inviato a un account che fa parte di un account di gestione o di amministratore delegato AWS Organizations e viene ricevuto nell'account di gestione.	Sì

contenuto del parametro 'detail'	Description	Richiesto
praticabilità	Metadati per attivare la determinazione programmatica di quali eventi richiedono un'azione senza ispezione manuale. Il valore (singolo) possibile può essere`ACTION_REQUIRED` , `ACTION_MAY_BE_REQUIRED` o. `INFORMATIONAL`	No
persone	Questo elenco di metadati attiva la determinazione programmatica dello stakeholder a cui indirizzare l'evento. I valori possibili (multipli) sono, e. `OPERATIONAL` `SECURITY` `BILLING`	No

Evento sulla salute pubblica - Problema operativo di Amazon EC2

```
{
    "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",
        "backupEvent": "false",
        "affectedAccount": "123456789012",
        "personas": ["OPERATIONS"]
    }
}
```

Account-specific AWS Health Evento - Problema con l'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",
        "backupEvent": "false",
        "affectedAccount": "123456789012",
        "personas": ["OPERATIONS"]
    }
}
```

Account-specific AWS Health Evento: evento di backup per Amazon EC2 Instance Store Drive con prestazioni ridotte

```
{
    "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-east-1::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-east-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "affectedEntities": [{
            "entityValue": "i-abcd1111"
        }],
        "page": "1",
        "totalPages": "1",
        "backupEvent": "true",
        "affectedAccount": "123456789012",
        "personas": ["OPERATIONS"]
    }
}
```

Account-specific AWS Health Evento: ritiro dell'istanza Amazon EC2

```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2026-01-27T01:43:21Z",
    "region": "us-east-1",
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED_90353408594353983",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED",
        "eventTypeCategory": "scheduledChange",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "1234abc01232a4012345678-1",
        "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
        "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "eventMetadata": {
```

```
            "keystring1": "valuestring1",
            "keystring2": "valuestring2",
            "keystring3": "valuestring3",
            "keystring4": "valuestring4",
            "truncated": "true"
        },
        "affectedEntities": [{
            "entityValue": "arn:aws:ec2:us-east-1:123456789012:instance/
i-1234567890abcdef0",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
            "status": "PENDING"
        }],
        "affectedAccount": "123456789012",
        "page": "1",
        "totalPages": "1",
        "backupEvent": "false",
        "personas": ["OPERATIONS"],
        "actionability": "ACTION_REQUIRED"
    }
}
```

Account-specific AWS Health Evento - Evento sul ciclo di vita pianificato Lambda

```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T01:43:21Z",
    "region": "us-west-2",
    "resources": ["arn:lambda-1-101002929", "arn:lambda-1-101002930",
 "arn:lambda-1-101002931", "arn:lambda-1-101002932"],
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT_90353408594353980",
        "service": "LAMBDA",
        "eventTypeCode": "AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT",
        "eventTypeCategory": "scheduledChange",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "1234abc01232a4012345678-1",
```

```
        "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
        "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "eventMetadata": {
            "keystring1": "valuestring1",
            "keystring2": "valuestring2",
            "keystring3": "valuestring3",
            "keystring4": "valuestring4",
            "truncated": "true"
        },
        "affectedEntities": [{
            "entityValue": "arn:lambda-1-101002929",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
            "status": "PENDING"
        }, {
            "entityValue": "arn:lambda-1-101002930",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:05:12 GMT",
            "status": "PENDING"
        }, {
            "entityValue": "arn:lambda-1-101002931",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:07:13 GMT",
            "status": "PENDING"
        }, {
            "entityValue": "arn:lambda-1-101002932",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:10:59 GMT",
            "status": "RESOLVED"
        }],
        "affectedAccount": "123456789012",
        "page": "1",
        "totalPages": "10",
        "backupEvent": "false",
        "personas": ["OPERATIONS"],
        "actionability": "ACTION_REQUIRED"
    }
}
```

Monitoraggio AWS Health

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni di AWS Health e il tuo altro AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio da monitorare AWS Health, segnala quando qualcosa non va e intraprendi le azioni appropriate:

- Amazon CloudWatch monitora il tuo AWS le risorse e le applicazioni su cui esegui AWS in tempo reale. È possibile raccogliere e tenere traccia dei parametri, 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 Guida per l'utente.

  Puoi usare Amazon EventBridge in modo che tu riceva una notifica AWS Health eventi che potrebbero influire sui tuoi servizi e sulle tue risorse. Ad esempio, se AWS Health pubblica un evento sulle tue istanze Amazon EC2, puoi utilizzare queste notifiche per intervenire e aggiornare o sostituire le tue risorse, se necessario. Per ulteriori informazioni, consulta Monitoraggio degli eventi in 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 registro a un bucket Amazon S3 specificato. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e la data in cui sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente di AWS CloudTrail.

Argomenti

- Registrazione dei log AWS Health Chiamate API con AWS CloudTrail

Registrazione dei log AWS Health Chiamate 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 chiamate API per AWS Health come eventi. Le chiamate acquisite includono le chiamate provenienti da AWS Health chiamate da console e in codice verso AWS Health operazioni API. Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi eventi per AWS Health.

Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nel CloudTrail console in Cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata fatta a AWS Health, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per saperne di più su CloudTrail, incluso come configurarlo e abilitarlo, consulta AWS CloudTrail Guida per l'utente.

AWS Health informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account quando crei l'account. Quando l'attività dell'evento supportato si verifica in AWS Health, tale attività viene registrata in un CloudTrail evento insieme ad altri AWS eventi di servizio in cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, vedere Visualizzazione degli eventi con CloudTrail Cronologia degli eventi.

Per una registrazione continua degli eventi nel tuo AWS account, compresi gli eventi per AWS Health, crea un pista. Una pista consente CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, il percorso si applica a tutti 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 altre AWS servizi per analizzare ulteriormente e agire in base ai dati degli eventi raccolti in CloudTrail registri. 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 CloudTrail File di registro provenienti da più regioni e Ricezione CloudTrail File di registro da più account

Tutti AWS Health Le operazioni API vengono registrate da CloudTrail e sono documentate nel AWS Health Riferimento API. Ad esempio, le chiamate al `DescribeEvents`, `DescribeEventDetails`, e `DescribeAffectedEntities` le operazioni generano voci nel CloudTrail file di registro.

AWS Health supporta la registrazione delle seguenti azioni come eventi in CloudTrail file di 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 sulla consegna dei file di log, puoi configurare CloudTrail per pubblicare notifiche Amazon SNS quando vengono consegnati nuovi file di registro. Per ulteriori informazioni, consulta l'argomento relativo alla configurazione delle notifiche Amazon SNS per CloudTrail.

Puoi anche aggregare AWS Health file di registro da multiplo AWS regioni e multiplo 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 del file di log

Un trail è una configurazione che consente l'invio di eventi come file di registro a un bucket Amazon S3 specificato. CloudTrail i file di log contengono una o più voci di registro. Un evento rappresenta una singola richiesta 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 log non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra un CloudTrail voce di registro che dimostra il DescribeEntityAggregates operazione.

```
{
   "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"
   }
   ],
   ...
}
```

Domande frequenti sui protocolli supportati

Il AWS Il servizio sanitario sta aggiungendo il supporto SDK per Smithy RPC v2 CBOR protocollo in aggiunta a quello esistente AWS JSON protocollo. Il protocollo Smithy RPC v2 CBOR è più performante di AWS JSON per la maggior parte dei carichi di lavoro. AWS Gli SDK daranno la priorità al protocollo più performante per ogni lingua.

Quali sono i AWS Protocolli CBOR JSON e Smithy RPC v2, e in cosa differiscono?

Un protocollo cablato funge da mediatore tra un cliente e il servizio. Il AWS L'SDK gestisce la serializzazione (conversione di un oggetto in formato wire) e la deserializzazione (riconversione del formato wire in un oggetto) tra client e server in modo trasparente per entrambi i protocolli.

AWS JSON - JSON è uno dei formati di dati più utilizzati e accettati per la comunicazione tra sistemi. Questo servizio utilizza AWS JSON come mezzo per comunicare tra un AWS Client SDK e server. Una richiesta HTTP per un'operazione API di servizio accetta input sotto forma di JSON, l'operazione viene eseguita e la risposta viene restituita al client SDK sotto forma di JSON.

Smithy RPC v2 CBOR - Smithy RPC v2 CBOR (Concise Binary Object Representation) è un protocollo sviluppato da Amazon per una trasmissione dei dati più efficiente. È un formato di dati progettato per mantenere compatte le dimensioni dei messaggi e per consentire al formato di evolversi senza richiedere la negoziazione della versione tra i sistemi. La differenza fondamentale rispetto a AWS JSON è quello AWS JSON utilizza testo leggibile dall'uomo (come `{"name": "John"}`), mentre Smithy RPC v2 CBOR utilizza un formato binario (sequenze di 1 e 0). Questo approccio binario crea pacchetti di dati più piccoli che viaggiano più velocemente sulla rete e riduce i tempi di serializzazione poiché i computer elaborano direttamente i dati binari.

Come posso iniziare a usare il protocollo CBOR Smithy RPC v2?

Per iniziare, usa la versione più recente AWS SDK/CLI versione per utilizzare il protocollo CBOR Smithy RPC v2 per questo servizio. L'SDK utilizzerà automaticamente il protocollo Smithy RPC v2 CBOR quando disponibile. Aggiorna il tuo AWS SDK alla versione specificata o a qualsiasi versione successiva.

A partire dal 2026-10-06, quanto segue AWS Gli SDK utilizzeranno il protocollo Smithy RPC v2 CBOR, mentre gli altri SDK continueranno a utilizzare il AWS Protocollo JSON:

- AWS SDK per C++
- AWS SDK per Go V2
- AWS SDK per Java 2.x
- AWS SDK per .NET v4
- AWS Strumenti per PowerShell v5
- AWS SDK per Swift
- AWS SDK per Kotlin

Quali sono i rischi dell'abilitazione del protocollo Smithy RPC v2 CBOR?

Il supporto aggiuntivo di Smithy RPC v2 CBOR negli SDK dovrebbe essere completamente trasparente e semplice per i clienti. Tuttavia, se si utilizza un'implementazione personalizzata di AWS SDK, o una combinazione di client personalizzati e AWS SDK, che dipende da AWS JSON-specific comportamento di serializzazione, potrebbe essere incompatibile con il protocollo CBOR Smithy RPC v2.

Cosa succede se la mia soluzione non supporta Smithy RPC v2 CBOR?

Per utilizzare il AWS Protocollo JSON, esegui il downgrade del tuo SDK a una versione rilasciata prima del 2026-10-06.

What AWS Le regioni supportano il protocollo Smithy RPC v2 CBOR?

Il protocollo Smithy RPC v2 CBOR è supportato in tutti AWS Regioni dove questo servizio è disponibile.

Quali miglioramenti della latenza posso aspettarmi dall'aggiornamento alle versioni SDK che supportano Smithy RPC v2 CBOR?

Smithy RPC v2 CBOR offre una latenza inferiore fino al 13% e una riduzione fino al 15% delle dimensioni del payload rispetto a AWS JSON. La codifica binaria elimina il sovraccarico dell'analisi del testo JSON e dell'escape delle stringhe, riducendo sia i tempi di trasferimento in rete che i costi di serializzazione.

Sarà il AWS Il protocollo JSON sarà obsoleto?

AWS Il protocollo JSON continuerà a essere supportato nelle versioni precedenti degli SDK. Inoltre, alcuni SDK specifici per lingua continueranno a utilizzare AWS JSON in quanto è più performante di Smithy RPC v2 CBOR poiché l'implementazione JSON disponibile per il linguaggio è più veloce della sua implementazione CBOR.

Dove posso trovare ulteriori informazioni su Smithy RPC v2 CBOR?

Puoi trovare ulteriori informazioni su AWS Protocollo JSON all'indirizzo AWS Protocollo JSON 1.0 e AWS protocollo JSON 1.1 nella documentazione di Smithy e su Smithy RPC v2 CBOR all'indirizzo Protocollo Smithy RPC v2 CBOR nella documentazione di Smithy.

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 gli aggiornamenti importanti di AWS Health documentazione, a partire dal 28 agosto 2020. Puoi ora iscriverti a un feed RSS per ricevere notifiche sugli aggiornamenti.

Modifica	Descrizione	Data
È stato aggiunto il `AWSServiceRoleForTagsHealth` ruolo collegato al servizio e `TagsHealthServiceRolePolicy` politica gestita	È stato aggiunto il `AWSServiceRoleForTagsHealth` ruolo collegato al servizio e `TagsHealthServiceRolePolicy` AWS politica gestita. La politica concede AWS Health accesso in sola lettura ai tag sulle risorse del tuo account. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Health e AWS Health aggiornamenti a AWS politiche gestite.	30 ottobre 2026
È stata aggiunta la pagina delle domande frequenti per i protocolli supportati	È stata aggiunta una nuova pagina delle domande frequenti con le risposte alle domande più frequenti su AWS Protocolli cablati JSON e Smithy RPC v2 CBOR. Per ulteriori informazioni, vedere Domande frequenti sui protocolli supportati.	6 ottobre 2026

È stato aggiunto il catalogo delle versioni	È stata aggiunta una nuova pagina che descrive il catalogo delle versioni per AWS Health, che fornisce una panoramic a a livello di servizio delle versioni supportate e delle relative tempistiche. Per ulteriori informazioni, consulta Catalogo delle versioni per AWS Health.	2 ottobre 2026
Ha chiarito che gli eventi pubblici non sono disponibi li tramite Notifiche AWS agli utenti	Sono state aggiunte didascali e per chiarire che gli eventi pubblici non sono disponibili tramite AWS notifiche gestite in Notifiche AWS agli utenti. Per ricevere eventi pubblici, devi creare un Amazon EventBridge regola o a User-configured notifica (UCN). Per ulteriori informazioni, vedere Evento pubblico.	26 agosto 2026
È stata aggiunta una nota sui tempi di aggiornamento dello stato delle risorse per gli eventi del ciclo di vita pianifica ti	È stata aggiunta una nota per chiarire che gli aggiornam enti dello stato delle risorse per gli eventi del ciclo di vita pianificati vengono eseguiti in modo asincrono e possono avere un ritardo fino a 72 ore in rare occasioni. Per ulteriori informazioni, vedere Riferimen to: AWS Health eventi Amazon EventBridge schema.	26 agosto 2026

Copertura regionale chiarita per un'integrazione semplificata	È stata aggiornata la sezione sull'integrazione semplificata per chiarire che una regola per una singola regione aggrega solo gli eventi specifici dell'account, non gli eventi pubblici. Gli eventi pubblici vengono distribuiti solo alla Regione interessata e alla relativa Regione di backup. Per ulteriori informazioni, consulta Integrazione semplificata.	2 luglio 2026
È stato aggiunto l'avviso di fine del supporto per AWS Connettore di gestione dei servizi	È stato aggiunto un avviso di fine del supporto alla sezione sull'integrazione del Service Management Connector. AWS terminerà il supporto per AWS Service Management Connector il 31 marzo 2027. Per ulteriori informazioni, vedere AWS Fine del supporto di Service Management Connector.	28 aprile 2026

Configurazione aggiornata di un EventBridge regola per inviare notifiche sugli eventi in AWS Health	Semplificata la procedura di creazione EventBridge regola collegandosi ad Amazon EventBridge Guida per l'utente per le fasi generali di creazione delle regole. L'argomento ora si concentra su AWS Health-filtri e casi d'uso specifici. Per ulteriori informazioni, vedere Configurazione di un EventBridge regola per inviare notifiche sugli eventi in AWS Health.	13 marzo 2026
Aggiornato AWS Health eventi Amazon EventBridge esempi di schemi	Sono stati aggiornati gli esempi di schema per includere personaggi e campi di azionabilità. Gli esempi includono il problema operativo di Public Health Event for Amazon EC2, Account-specific eventi per Elastic Load Balancing API Issue e Amazon EC2 Instance Store Drive, evento di backup con riduzione delle prestazioni e Lambda Planned Lifecycle Event. Per ulteriori informazioni, consulta Riferimento: AWS Health eventi Amazon EventBridge schema.	13 marzo 2026

Gestione aggiornata AWS Health notifiche in Notifiche AWS agli utenti	Informazioni aggiornate in questa sezione per riflettere la migrazione di AWS Health eventi a Notifiche AWS agli utenti. Per ulteriori informazioni, vedere Gestisci AWS Health notifiche in Notifiche AWS agli utenti.	22 dicembre 2025
Eventi pubblici e specifici per account di monitoraggio aggiornati per AWS Health	Sono state aggiunte informazioni a questa sezione che descrivono in dettaglio il comportamento delle regole di backup per eventi pubblici ed eventi specifici dell'account. Per ulteriori informazioni, consulta Regole di backup per AWS Health eventi.	11 dicembre 2025
Sono state aggiunte informazioni sui campi Actionability e Personas per gli eventi sulla salute	Sono state aggiunte informazioni per i campi Actionability e Personas nei Concepts for AWS Health sezione e il contenuto dello schema del parametro 'details' nel Riferimento: AWS Health eventi Amazon EventBridge sezione schema. Per ulteriori informazioni, vedere Concetti per AWS Health e Riferimento: AWS Health eventi Amazon EventBridge schema.	20 novembre 2025

Sezione aggiornata: Creazione EventBridge regole per Regione AWS copertura	Informazioni aggiornate da creare EventBridge regole. Per ulteriori informazioni, vedere Creando EventBridge regole per Regione AWS copertura.	3 novembre 2025
Sezione aggiornata: Gestisci AWS Health notifiche in Notifiche AWS agli utenti	Informazioni aggiornate sui passaggi per configurare il tuo AWS abbonamento alle notifiche gestite per AWS Health eventi. Per ulteriori informazioni, vedere Gestisci AWS Health notifiche in Notifiche AWS agli utenti.	16 settembre 2025
Sezione aggiornata: Monitoraggio degli eventi in AWS Health con Amazon EventBridge	Informazioni aggiornate nella nota per AWS Health fornisce eventi a EventBridge. Per ulteriori informazioni, vedere Monitoraggio degli eventi in AWS Health con Amazon EventBridge.	15 settembre 2025
Sezione aggiornata: AWS Health Dashboard	Sono stati rimossi i passaggi opzionali per iscriversi al feed RSS per gli eventi sanitari. È stata aggiunta la nota che per ricevere notifiche relative agli eventi sanitari, i clienti possono utilizzare EventBridge. Per ulteriori informazioni, vedere AWS Health Dashboard .	15 agosto 2025

Sezione aggiornata: Monitoraggio degli eventi in AWS Health con Amazon EventBridge	È stato rimosso l'argomento Installazione di un ruolo collegato al servizio da utilizzare AWS Rilevamento e risposta agli incidenti in Monitoraggio degli eventi in AWS Health con Amazon EventBridge	8 agosto 2025
Sezione aggiornata: Monitoraggio degli eventi in AWS Health con Amazon EventBridge	Sono state aggiunte informazioni alla sezione Note che indicano che potrebbe trascorrere fino a un'ora prima di iniziare a ricevere notifiche relative a eventi di salute pubblica. Per ulteriori informazioni, consulta Monitoraggio degli eventi in AWS Health con Amazon EventBridge	22 luglio 2025
Sezione aggiornata: Abilitazione della visualizzazione organizzativa	Sono state aggiunte informazioni alla sezione Note che indicano che AWS Health aggrega automaticamente tutti gli eventi sanitari cronologici dell'organizzazione quando si abilita la visualizzazione organizzativa. La cronologia degli eventi potrebbe richiedere fino a 24 ore per essere visualizzati nella visualizzazione organizzativa. Per ulteriori informazioni, consulta Abilitazione della visualizzazione organizzativa	27 giugno 2025

Sezione aggiornata: Aggregazione AWS Health eventi tra gli account	Ho rimosso la nota che AWS Health non mostra gli eventi che si sono verificati prima dell'attivazione della visualizzazione organizzativa. Per ulteriori informazioni, consulta Aggregazione AWS Health eventi tra gli account	27 giugno 2025
WorkDocs obsoleta	Sono stati rimossi i riferimenti a quelli obsoleti WorkDocs nel Eventi del ciclo di vita pianificati per AWS Health.	19 giugno 2025
Nota aggiunta per AWS cronologia di migrazione delle notifiche gestite	È stata aggiunta una nota relativa alle date chiave per la migrazione delle email a AWS notifiche gestite in Notifiche AWS agli utenti. Per ulteriori informazioni, vedere Gestisci AWS Health notifiche in Notifiche AWS agli utenti.	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 irrisolte. Per ulteriori informazioni, consulta la Cosa devo aspettarmi quando ricevo una notifica di un evento del ciclo di vita pianificato? sezione in Eventi del ciclo di vita pianificati per AWS Health.	18 aprile 2025

È stata aggiornata la descrizione del Elenco delle risorse interessate per gli eventi del ciclo di vita pianificati	Il Elenco delle risorse interessate per gli eventi del ciclo di vita pianificati di solito si aggiorna una volta ogni 24 ore, ma potrebbe richiedere fino a 72 ore per riflettere lo stato corrente delle risorse. Per ulteriori informazioni, consulta Dettagli dell'evento sezione in Visualizzazione degli eventi del tuo account nella AWS Health Dashboard.	7 aprile 2025
È stata aggiunta una FAQ per la gestione AWS Health notifiche in Notifiche AWS agli utenti	Per ulteriori informazioni, vedere Gestisci le notifiche in Notifiche AWS agli utenti FAQ.	18 febbraio 2025
Sono state aggiunte informazioni riguardanti IPv6-only richieste agli endpoint.	Per ulteriori informazioni, vedere Scelta degli endpoint per AWS Health Richieste API.	28 gennaio 2025
Gestisci AWS Health notifiche in Notifiche AWS agli utenti	Per ulteriori informazioni, vedere Gestisci le notifiche in Notifiche AWS agli utenti.	16 gennaio 2025
JSON corretto in Monitoraggio AWS Health eventi con Amazon EventBridge	Per ulteriori informazioni, consulta Monitoraggio AWS Health eventi con Amazon EventBridge.	3 settembre 2024
Informazioni aggiornate sullo scaricamento delle risorse interessate	Per ulteriori informazioni, vedere Visualizzazione delle risorse interessate.	27 luglio 2024

È stata rimossa la privacy del traffico Internet dalla sezione Sicurezza AWS Health documentazione	Per ulteriori informazioni, vedere Sicurezza in AWS Health.	27 marzo 2024
Aggiornato il AWS Health Dashboard: integrità del servizio ed eventi del ciclo di vita pianificati per AWS Health documentazione.	Per ulteriori informazioni, vedere AWS Health Dashboard — Integrità del servizio e Eventi del ciclo di vita pianificati per AWS Health.	15 febbraio 2024
È stato rimosso un elenco duplicato in Creazione di un EventBridge regola per AWS Health	È stato rimosso un punto elenco duplicato in Creando un EventBridge regola per AWS Health.	04 dicembre 2023
È stata aggiunta la documentazione per gli eventi del ciclo di vita pianificati	Per ulteriori informazioni, vedere Eventi del ciclo di vita pianificati per AWS Health.	31 ottobre 2023
Documentazione per `AWSHealthFullAccess` aggiornata	Ora puoi usare `AWSHealthFullAccess` politica gestita in AWS GovCloud (US) Regions. Vedi AWS politiche gestite per AWS Health.	16 ottobre 2023
È stata aggiunta la documentazione per la configurazione AWS Notifiche utente in AWS Health.	Ora puoi configurare AWS Notifiche utente in AWS Health. Per ulteriori informazioni, vedere Configura AWS Notifiche utente per AWS Health.	30 agosto 2023
È stata aggiunta la documentazione per la funzionalità di amministratore delegato al Aggregazione AWS Health eventi sezione.	Per ulteriori informazioni, vedere Vista organizzativa degli amministratori delegati.	27 luglio 2023

Aggiornamento della politica SLR	Aggiornamento a AWS politica gestita: Health_OrganizationsServiceRolePolicy. 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 da AWS Health eventi. Per ulteriori informazioni, vedere Monitoraggio AWS Health eventi con Amazon EventBridge.	20 giugno 2023
Documentazione aggiornata per Amazon EventBridge	Ora puoi usare Amazon EventBridge regola per monitorare sia gli eventi specifici dell'account che quelli pubblici. Per ulteriori informazioni, consulta Monitoraggio AWS Health eventi con Amazon EventBridge.	2 maggio 2023
Documentazione aggiunta per AWS politiche gestite	È stata aggiunta la documentazione per AWS politiche gestite per AWS Health e Utilizzo di ruoli collegati ai servizi per AWS Health.	18 gennaio 2023

È stata aggiunta la documentazione sull'impostazione del fuso orario	Usa la nuova funzione di fuso orario per visualizzare AWS Health Dashboard nel tuo fuso orario locale o in UTC. Per ulteriori informazioni, consulta Guida introduttiva al tuo AWS Health Dashboard: stato del tuo account e il AWS Health Dashboard — Stato del servizio.	21 settembre 2022
Documentazione aggiornata	Documentazione aggiunta per AWS Health Consapevole. Per ulteriori informazioni, vedere AWS Health Consapevole.	25 maggio 2022
Documentazione aggiornata	Il Service Health Dashboard e il AWS Personal Health Dashboard sono stati rinominati in AWS Health Dashboard. Per ulteriori informazioni, consulta Guida introduttiva al tuo AWS Health Dashboard: stato del tuo account e il AWS Health Dashboard — Stato del servizio.	28 febbraio 2022
Documentazione aggiornata per Amazon EventBridge	Nuovo argomento per AWS Health per usare Amazon EventBridge per monitorare gli eventi sulla salute. Per ulteriori informazioni, vedere Monitoraggio AWS Health eventi con Amazon EventBridge.	3 febbraio 2022

Documentazione aggiornata	Se hai un Enterprise On-Ramp Piano di supporto, puoi usare il AWS Health API.	24 novembre 2021
Documentazione aggiunta	Nuovo argomento per AWS Health concetti. Per ulteriori informazioni, vedere Concetti per AWS Health.	29 luglio 2021
Documentazione aggiornata per CloudWatch Eventi	È stata aggiunta una sezione su come creare una regola per più servizi e categorie di tipi di eventi. Per ulteriori informazioni, consulta Creazione di una regola per più servizi e categorie.	7 maggio 2021
Documentazione aggiornata per CloudWatch Eventi	Aggiornata la sezione per automatizzare AWS Systems Manager azioni per Amazon CloudWatch Regole degli eventi. Per ulteriori informazioni, vedere Automazione delle azioni per le istanze Amazon EC2.	28 Aprile 2021
Documentazione aggiornata per CloudWatch Eventi	È stata aggiunta una sezione per ricevere AWS Health eventi nel tuo client di chat. Per ulteriori informazioni, consulta Ricezione AWS Health eventi con Amazon Q Developer nelle applicazioni di chat.	16 marzo 2021

Documentazione aggiornata	I seguenti argomenti sono stati aggiornati: • Aggiornato il Aggregazione AWS Health eventi argomento • Riorganizzato e aggiornato il Monitor per AWS Health eventi con Amazon CloudWatch Eventi argomento • Aggiornato il Condizioni basate su risorse e azioni sezione	29 gennaio 2021
Aggiunto il AWS Health Dashboard per la visualizzazione organizzativa in AWS Health plancia	Puoi usare AWS Health console per abilitare la funzionalità di visualizzazione organizzativa. Puoi quindi visualizzare gli eventi relativi allo stato di salute degli account dei membri nel tuo AWS organizzazione.	14 dicembre 2020
Demo sugli endpoint ad alta disponibilità	È possibile utilizzare il codice di esempio per determinare l'endpoint regionale attivo e la firma AWS Regione per AWS Health.	22 ottobre 2020
Aggiornamenti al AWS Health Guida per l'utente	Aggiornamenti dell'organizzazione e aggiunto un feed RSS in modo da poterti iscrivere agli ultimi aggiornamenti di AWS Health documentazione.	28 agosto 2020

Aggiornamenti precedenti

Modifica	Descrizione	Data
Aggiornato l'argomento della vista organizzativa per includere esempi.	Consulta Aggregazione AWS Health eventi tra gli account.	3 giugno 2020
Sicurezza e AWS Health	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di AWS Health. Consulta 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.	Consulta Aggregazione AWS Health eventi tra gli account.	18 dicembre 2019
Aggiunta nuova sezione «Resource- and Action-based Condizioni» per spiegare le restrizioni relative agli Eventi previste da AWS Health API.	Consulta Gestione delle identità e degli accessi per AWS Health.	2 agosto 2018
È stata aggiunta una nota sulla visibilità di AWS Health informazioni.	Consulta Gestione delle identità e degli accessi per 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.