



Guida per l'utente

# AWS Health



# AWS Health: Guida per l'utente

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

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

---

# Table of Contents

Cos'è AWS Health? .....	1
È il primo utilizzo di AWS Health? .....	2
Concetti per AWS Health .....	3
AWS Health evento .....	3
Evento specifico dell'account .....	4
Evento pubblico .....	4
AWS Health Dashboard .....	4
AWS Health Dashboard: stato del servizio .....	5
Codice del tipo di evento .....	5
Categorie di tipi di evento .....	5
Stato dell'evento .....	7
Entità interessate .....	7
AWS Health eventi su Amazon EventBridge .....	7
AWS Health API .....	8
Visualizzazione organizzativa .....	8
AWS Health Dashboard — Integrità del servizio .....	9
Eventi pianificati del ciclo di vita per AWS Health .....	12
Cosa sono gli eventi pianificati del ciclo di vita? .....	12
Cosa devo aspettarmi quando ricevo una notifica relativa a un evento relativo al ciclo di vita pianificato? .....	13
Modello di responsabilità condivisa per la resilienza .....	15
Accesso agli eventi pianificati del ciclo di vita .....	16
Inizia a usare la AWS Health dashboard: lo stato del tuo account .....	17
Visualizza gli eventi dell'account nella AWS Health Dashboard .....	18
Problemi aperti e recenti .....	18
Modifiche pianificate .....	20
Altre notifiche .....	21
Log degli eventi .....	21
Dettagli dell'evento .....	22
Tipi di eventi .....	24
Visualizzazione del calendario .....	24
Visualizzazione delle risorse interessate .....	25
Impostazioni del fuso orario .....	27
Lo stato di salute della tua organizzazione .....	27

Configura Amazon EventBridge .....	28
AWS Health Consapevole .....	28
Avvisi per eventi AWS Health .....	28
ConfiguraAWSNotifiche utente perAWS Health .....	30
Accesso all'API AWS Health .....	31
Endpoint .....	31
Utilizzo della demo degli endpoint ad alta disponibilità .....	33
Utilizzo della demo Java ava ava ava .....	33
Usare la demo di Python .....	36
Firma delle richieste API AWS Health .....	39
Operazioni supportate in AWS Health .....	40
Esempio di codice Java .....	41
Fase 1: Inizializzazione delle credenziali .....	42
Fase 2: Inizializzazione diAWS HealthClient API .....	42
Fase 3: UtilizzaAWS HealthOperazioni API per ottenere informazioni sugli eventi .....	42
Sicurezza .....	46
Protezione dei dati .....	47
Crittografia dei dati .....	47
Gestione dell'identità e degli accessi .....	48
Destinatari .....	49
Autenticazione con identità .....	49
Gestione dell'accesso con policy .....	52
Come AWS Health funziona con IAM .....	55
Esempi di policy basate su identità .....	61
Risoluzione dei problemi .....	74
Uso di ruoli collegati ai servizi .....	77
AWS politiche gestite per AWS Health .....	78
Registrazione e monitoraggio AWS Health .....	83
Convalida della conformità .....	84
Resilienza .....	86
Sicurezza dell'infrastruttura .....	86
Analisi della configurazione e delle vulnerabilità .....	86
Best practice di sicurezza .....	86
Concedi AWS Health agli utenti le autorizzazioni minime possibili .....	87
Visualizza il AWS Health Dashboard .....	87
Integrazione AWS Health con Amazon Chime o Slack .....	87

Monitora gli AWS Health eventi .....	87
Aggregazione degli eventi AWS Health .....	88
Prerequisiti .....	89
Visualizzazione organizzativa (console) .....	89
Attivazione della visualizzazione organizzativa (console) .....	90
Visualizzazione degli eventi di visualizzazione organizzativa (console) .....	91
Visualizzazione degli account e delle risorse interessati (console) .....	95
Disattivazione della visualizzazione organizzativa (console) .....	97
Vista organizzativa (CLI) .....	98
Attivazione della visualizzazione organizzativa (CLI) .....	98
Visualizzazione degli eventi di visualizzazione organizzativa (CLI) .....	101
Disattivazione della visualizzazione organizzativa (CLI) .....	102
Operazioni API di visualizzazione organizzativa AWS Health .....	103
Visualizzazione organizzativa dell'amministratore delegato .....	104
Registra un amministratore delegato per la tua visione organizzativa .....	105
Rimuovi un amministratore delegato dalla tua vista organizzativa .....	105
Monitoraggio degli eventi Health con EventBridge .....	107
Informazioni per Regioni AWSAWS Health .....	108
Informazioni sugli eventi pubblici per AWS Health .....	109
Processore di eventi per AWS Health .....	111
Informazioni correlate .....	111
Creazione di una EventBridge regola per AWS Health .....	111
Creazione di una regola per più servizi e categorie .....	115
AWS Health Schema degli eventi Amazon EventBridge .....	117
AWS Health Schema degli eventi .....	117
Public Health Event - Problema operativo di Amazon EC2 .....	144
AWS Health Evento specifico dell'account - Problema dell'API Elastic Load Balancing .....	145
AWS Health Evento specifico dell'account: riduzione delle prestazioni di Amazon EC2 Instance Store Drive .....	146
AWS Health Impaginazione degli eventi su EventBridge .....	147
Aggregazione degli AWS Health eventi utilizzando la visualizzazione organizzativa e l'accesso amministrativo delegato .....	147
Ricezione di eventi con AWS HealthAWS Chatbot .....	148
Prerequisiti .....	148
Automazione delle azioni per le istanze Amazon EC2 .....	150
Prerequisiti .....	151

---

Crea una regola per EventBridge .....	155
Configura i connettori SMC per AWS Health .....	158
Monitoraggio AWS Health .....	159
Registrazione delle AWS Health API chiamate con AWS CloudTrail .....	159
AWS Health informazioni in CloudTrail .....	160
Esempio: voci AWS Health dei file di registro .....	161
Cronologia dei documenti .....	163
Aggiornamenti precedenti .....	168
Glossario AWS .....	170
.....	clxxi

# Cos'è AWS Health?

AWS Health offre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità delle tue AWS servizi 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 notifiche e avvisi attivati da cambiamenti di stato delle risorse AWS per offrirti visibilità quasi istantanea e indicazioni al fine di 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.

Per comprendere le nozioni di base AWS Health e come utilizzare il servizio, consulta [È il primo utilizzo di AWS Health?](#)

Per un elenco dei termini che vedrai quando utilizzerai AWS Health, vedi [Concetti per AWS Health](#).

## Note

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

# È il primo utilizzo di AWS Health?

Se utilizzi AWS Health per la prima volta, ti consigliamo di iniziare leggendo le sezioni seguenti:

- [Cos'è AWS Health?](#)— Questa sezione descrive il modello di dati sottostante, le operazioni che supporta e gli AWS SDK che puoi utilizzare per interagire con il servizio.
- [Concetti per AWS Health](#)— Scopri le nozioni di base AWS Health e i termini che incontrerai durante l'utilizzo del servizio.
- [Guida introduttiva alla AWS Health dashboard: stato del tuo account](#)— Scopri come visualizzare gli eventi e le entità interessate ed eseguire filtri avanzati. Questa dashboard include eventi specifici del tuo account e della tua organizzazione.
- [AWS Health Dashboard — Integrità del servizio](#)— Se non ne possiedi uno Account AWS, puoi visualizzare le informazioni sullo stato di salute e sullo stato di ognuno AWS servizi Regione AWS di essi.
- [Monitoraggio AWS Health degli eventi con Amazon EventBridge](#)— Puoi utilizzare Amazon EventBridge per ricevere notifiche push da AWS Health.
- [Accesso all'API AWS Health](#)— La sezione AWS Health API descrive le operazioni che recuperano informazioni su eventi ed entità.

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.

Puoi impostare una EventBridge regola per ricevere AWS Health eventi su Amazon EventBridge. Ciò consente di utilizzare le notifiche push per automatizzare la gestione AWS Health degli eventi creando EventBridge regole Amazon per intraprendere azioni.

Se disponi di un piano Business, Enterprise On-Ramp o Enterprise Support, puoi accedere alle informazioni presentate nella dashboard in modo programmatico. Puoi utilizzare AWS Command Line Interface (AWS CLI) o scrivere codice per effettuare richieste, utilizzando direttamente l'API REST o gli SDK. AWS

Per ulteriori informazioni sull'utilizzo AWS Health degli eventi su Amazon EventBridge, consulta [Monitoraggio AWS Health degli eventi con Amazon EventBridge](#). Per ulteriori informazioni sull'utilizzo di AWS Health con l'AWS CLI, consulta la [documentazione di riferimento dell'AWS CLI per AWS Health](#). Per istruzioni su come installare AWS CLI, consulta [Installazione dell'AWS Command Line Interface](#).



# Concetti per AWS Health

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

## Argomenti

- [AWS Health evento](#)
- [AWS Health Dashboard](#)
- [Codice del tipo di evento](#)
- [Categorie di tipi di evento](#)
- [Stato dell'evento](#)
- [Entità interessate](#)
- [AWS Health eventi su Amazon EventBridge](#)
- [AWS Health API](#)
- [Visualizzazione organizzativa](#)

## AWS Health evento

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

Esistono due tipi di eventi Health:

### Indice

- [Evento specifico dell'account](#)
- [Evento pubblico](#)

## Evento specifico dell'account

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

Puoi trovare eventi specifici dell'account dalla [AWS Health dashboard](#), dall'[AWS Health API](#) o utilizzare [Amazon CloudWatch Events per ricevere notifiche](#).

## Evento pubblico

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

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

Se hai un account, consulta [Guida introduttiva alla AWS Health dashboard: stato del tuo account](#).

Se non disponi di un account, consulta [AWS Health Dashboard — Integrità del servizio](#).

## AWS Health Dashboard

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

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

[Puoi accedere alla Dashboard per visualizzare la tua AWS Health Dashboard AWS Management Console all'indirizzo https://health.aws.amazon.com/health/home.](https://health.aws.amazon.com/health/home)

Per ulteriori informazioni, consulta [Guida introduttiva alla AWS Health dashboard: stato del tuo account](#).

## AWS Health Dashboard: stato del servizio

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

Per ulteriori informazioni, consulta [AWS Health Dashboard — Integrità del servizio](#).

## Codice del tipo di evento

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

## Categorie di tipi di evento

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

Ti consigliamo di monitorare tutte le categorie di tipi di eventi. Tieni presente che ogni categoria viene visualizzata per diversi tipi di eventi. Puoi anche utilizzare l'operazione API [DescribeEventTypes](#) per trovare la categoria del tipo di evento.

### Notifica dell'account

Questi eventi forniscono informazioni sull'amministrazione o sulla sicurezza degli account e dei servizi. Questi eventi potrebbero essere informativi o richiedere un intervento urgente da parte tua. Ti consigliamo di prestare attenzione a questi tipi di eventi e di esaminare tutte le azioni consigliate.

Di seguito sono riportati alcuni esempi di codici di tipo di evento per le notifiche degli account:

- **AWS\_S3\_OPEN\_ACCESS\_BUCKET\_NOTIFICATION**— Hai un bucket Amazon S3 che potrebbe consentire l'accesso pubblico.
- **AWS\_BILLING\_SUSPENSION\_NOTICE**— Il tuo account presenta addebiti in sospeso ed è stato sospeso oppure lo hai disattivato.
- **AWS\_WORKSPACES\_OPERATIONAL\_NOTIFICATION**— C'è un problema di servizio per Amazon WorkSpaces.

## Problema

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

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

- **AWS\_EC2\_OPERATIONAL\_ISSUE**— Un problema operativo di un servizio, ad esempio ritardi nell'utilizzo di un servizio.
- **AWS\_EC2\_API\_ISSUE**— Un problema operativo per l'API di un servizio, ad esempio una maggiore latenza per un'operazione API.
- **AWS\_EBS\_VOLUME\_ATTACHMENT\_ISSUE**— Un problema localizzato a livello di risorsa che potrebbe influire sulle tue risorse Amazon Elastic Block Store (Amazon EBS).
- **AWS\_ABUSE\_PII\_CONTENT\_REMOVAL\_REPORT**— Questo evento significa che il tuo account potrebbe essere sospeso se non agisci.

## Modifica programmata

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

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

- **AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED**— Un'istanza Amazon EC2 richiede un riavvio.
- **AWS\_SAGEMAKER\_SCHEDULED\_MAINTENANCE**— SageMaker richiede un evento di manutenzione, ad esempio la risoluzione di un problema di servizio.

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

#### Tip

Se utilizzi l' AWS Health API o il AWS Command Line Interface (AWS CLI) per restituire i dettagli dell'evento, l'Eventoggetto contiene il eventScopeCode campo con il valore. ACCOUNT\_SPECIFIC Per ulteriori informazioni, consulta la [Documentazione di riferimento delle API di AWS Health](#).

## Stato dell'evento

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

## Entità interessate

Le entità interessate sono AWS risorse che potrebbero essere interessate dall'evento. Ad esempio, se ricevi un evento pianificato per la 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. Utilizza queste informazioni per risolvere qualsiasi potenziale problema di servizio, come la creazione o l'obsolescenza di risorse.

## AWS Health eventi su Amazon EventBridge

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

Per ulteriori informazioni, consulta [Monitoraggio AWS Health degli eventi con Amazon EventBridge](#).

# AWS Health API

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

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

Per ulteriori informazioni, consulta la [Documentazione di riferimento delle API di AWS Health](#).

## Note

È necessario disporre di un piano Business, Enterprise On-Ramp o Enterprise Support [AWS Support](#) per utilizzare l' AWS Health API. Se chiami l' AWS Health API da un account che non dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, ricevi un `SubscriptionRequiredException` errore.

## Visualizzazione organizzativa

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

# AWS Health Dashboard — Integrità del servizio

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

## Tip

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

Per visualizzare la AWS Health Dashboard — Stato del servizio

1. Vai 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 informativo o di degradazione
  - Una cronologia degli aggiornamenti recenti dell'evento
  - Un elenco di AWS servizi 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](#).

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

**Tip**

Puoi filtrare per servizio Regione AWSe data.

- Accanto a un evento di servizio in corso, scegli l'icona di stato



per visualizzare ulteriori informazioni sull'evento.

- (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.

**Service history**

List of services

List of events

The following table is a running log of AWS service interruptions for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in Pacific Standard Time (PST). To update your time zone, see [Time zone settings](#).

 Add filter

**Note**

Selezionando un evento pubblico dopo settembre 2023, nell'URL del browser verrà inserito un link a quell'evento pubblico. AWS Health Dopo aver selezionato questo link, accedi alla visualizzazione dell'elenco degli eventi con il pop-up dell'evento.



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

# 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 AWS servizi 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.](#)
  - [Amazon WorkDocs Companion sta raggiungendo la fine del ciclo di vita e non è più disponibile.](#)

### 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 SOSPEO». Se alle 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 SOSPEO» 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 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 ricevere più ARN se l'organizzazione dispone di un gran numero di risorse o risorse interessate. Account AWS

Visibilità tempestiva sugli eventi pianificati del ciclo di vita: gli eventi del ciclo di vita pianificato sono progettati per avere un lead time minimo di 180 giorni per le versioni/modifiche principali e di 90 giorni per le versioni/modifiche minori, ove possibile.

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 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 alle 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.

Open and recent issues
Scheduled changes
Other notifications
Event log

### Scheduled changes Table Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

< 1 >

Event	Status	Region / Zone <a href="#">Info</a>	Start time	End time	Affected resources
<a href="#">EKS planned lifecycle event</a>	Upcoming	us-west-2	January 30, 2024 at 6:00:00 PM UTC-8		<a href="#">9 pending</a>
<a href="#">DMS planned lifecycle event</a>	Upcoming	us-east-1	January 29, 2024 at 6:00:00 PM UTC-8		<a href="#">1 pending</a>
<a href="#">DMS planned lifecycle event</a>	Upcoming	eu-west-1	January 29, 2024 at 6:00:00 PM UTC-8		<a href="#">10 pending</a>
<a href="#">EKS planned lifecycle event</a>	Completed	eu-west-1	January 30, 2024 at 6:00:00 PM UTC-8		-

#### EKS planned lifecycle event ⚙️ ×

Resource data is typically refreshed every 24 hours. 0 Resolved 0%  
No actions required

#### Affected resources in account 745485236264 (5)

< 1 >

Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	⏸ Pending	15 days ago
arn:aws:eks:us-west-1:745485236264:cluster/prod-refactor	⏸ Pending	15 days ago

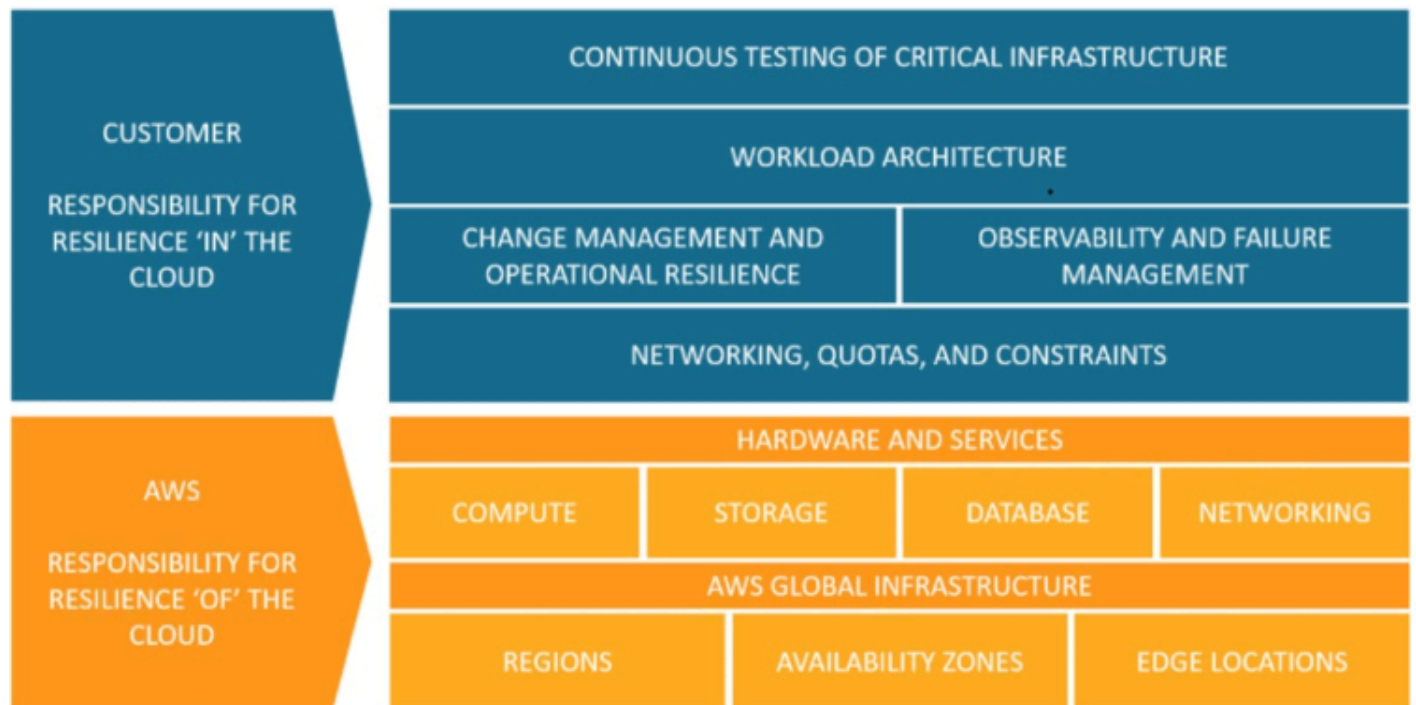
Una volta trascorsa la data prevista per l'evento:

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, l' AWS Health evento passerà allo stato «Chiuso».
3. Se hai risorse in sospeso dopo la data di inizio o di fine che non sono state risolte, l' AWS Health evento rimane aperto per 90 giorni dopo la data di inizio o di fine. Quindi l'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 AWS fornito. 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](#)

# Guida introduttiva alla AWS Health dashboard: stato del tuo account

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

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

## Note

Se non ne hai uno Account AWS, puoi utilizzarlo [AWS Health Dashboard — Integrità del servizio](#) per conoscere la disponibilità generale del servizio.

Se disponi di un account, ti consigliamo di accedere alla AWS Health dashboard per ottenere informazioni più approfondite sugli eventi e sulle modifiche imminenti che potrebbero influire sui tuoi servizi e risorse.

## Indice

- [Visualizzazione degli eventi del tuo account nella AWS Health Dashboard](#)
  - [Problemi aperti e recenti](#)
  - [Modifiche pianificate](#)
  - [Altre notifiche](#)
  - [Log degli eventi](#)
- [Dettagli dell'evento](#)
- [Tipi di eventi](#)
- [Visualizzazione del calendario](#)

- [Visualizzazione delle risorse interessate](#)
- [Impostazioni del fuso orario](#)
- [Lo stato di salute della tua organizzazione](#)
- [Configura Amazon EventBridge](#)
- [AWS Health Consapevole](#)
- [Avvisi per eventi AWS Health](#)

## Visualizzazione degli eventi del tuo account nella AWS Health Dashboard

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

Per visualizzare gli eventi dell'account nella AWS Health dashboard

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

### Problemi aperti e recenti


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

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

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



Per visualizzare tutti gli eventi, anziché quelli recenti visualizzati nella dashboard, scegli la [Log degli eventi](#) scheda.

 Note

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

Example : problema operativo per Amazon Elastic Compute Cloud (AmazonEC2)

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

# Your account health

Stay informed of important events affecting your AWS resources.

### Configure EventBridge

Get notifications for events that might affect your services and resources.

[Go to EventBridge](#)

**Open and recent issues (16)**
Scheduled changes (0)
Notifications (3)
Event log

### Open and recent issues (16)

View events that might affect your AWS infrastructure. **35 issues** were resolved in the past 24 hours.

Service: Elastic Compute Cloud ✕

Clear filter

< 1 >

#### Event summary

**Operational issue - EC2 (Ohio)**  
 Last update: February 20, 2022 at 11:16:34 PM UTC-8  
 us-east-2

**Operational issue - EC2 (Ohio)**  
 Last update: February 17, 2022 at 11:56:09 PM UTC-8  
 us-east-2

**Operational issue - EC2 (N. Virginia)**  
 Last update: February 16, 2022 at 1:36:29 AM UTC-8  
 us-east-1

### Operational issue - EC2 (Ohio) [Back to list view](#)

**Details**
Affected resources

#### Event data

<p>Service EC2</p> <p>Status Open</p> <p>Region / Availability Zone us-east-1</p> <p>Account specific No</p>	<p>Start time February 20, 2022 at 11:16:24 PM UTC-8</p> <p>End time -</p> <p>Category Issue</p> <p>Affected resources 1</p>
--	--

#### Description

[04:35 AM PST] We are investigating increased EC2 launch failures and networking connectivity issues for some instances in a single Availability Zone (USE1-AZ4) in the US-EAST-1 Region. Other Availability Zones within the US-EAST-1 Region are not affected by this issue.

## Modifiche pianificate

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

## Altre notifiche

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

## Log degli eventi

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

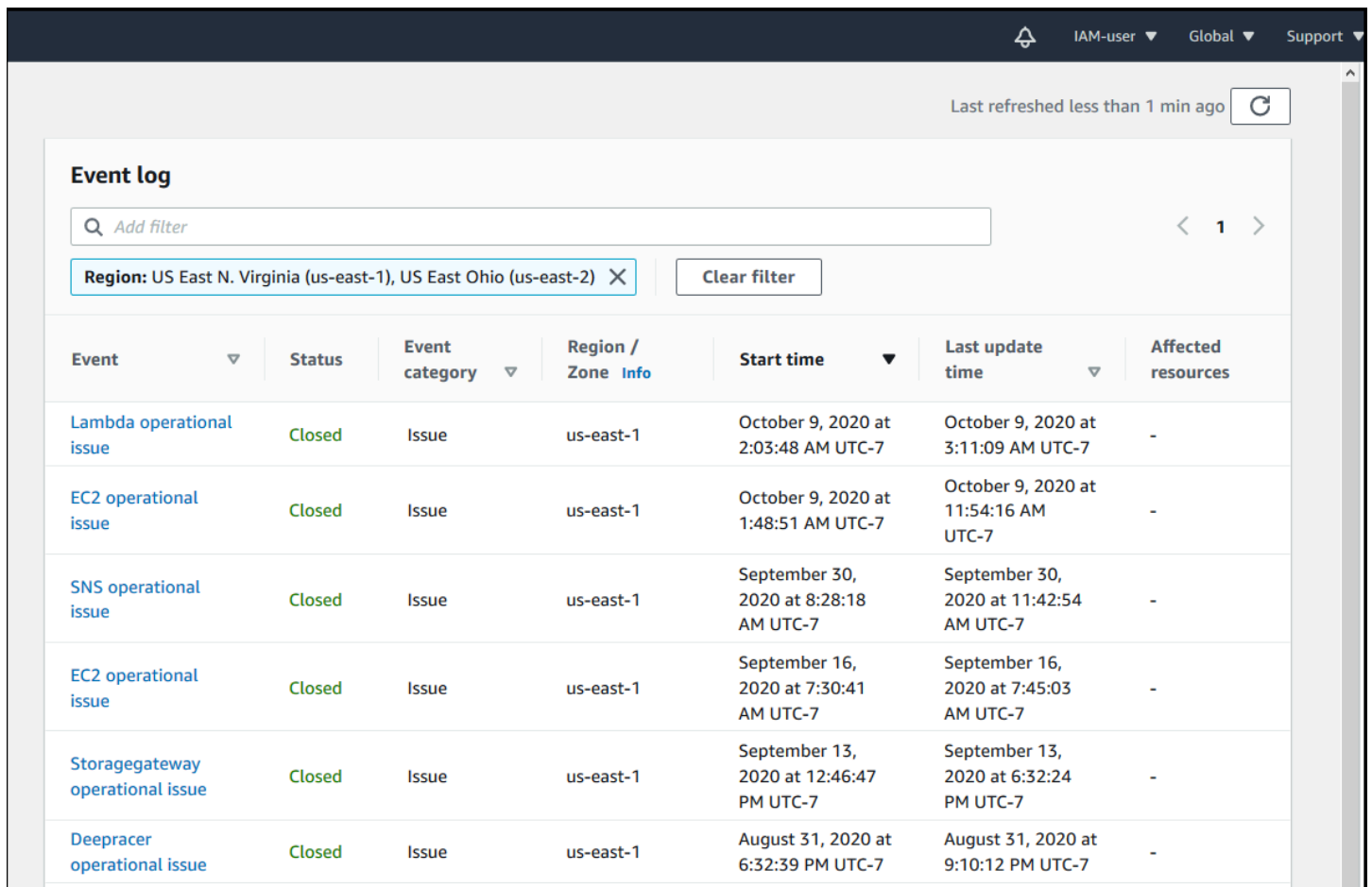
Quando si sceglie un evento nella tabella del registro eventi, viene visualizzato il riquadro Dettagli con informazioni sull'evento e l'elenco delle risorse interessate. Per ulteriori informazioni, consulta [Dettagli dell'evento](#).

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

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

Example : registro eventi

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



Event log

Q Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X Clear filter

Event	Status	Event category	Region / Zone	Start time	Last update time	Affected resources
Lambda operational issue	Closed	Issue	us-east-1	October 9, 2020 at 2:03:48 AM UTC-7	October 9, 2020 at 3:11:09 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	October 9, 2020 at 1:48:51 AM UTC-7	October 9, 2020 at 11:54:16 AM UTC-7	-
SNS operational issue	Closed	Issue	us-east-1	September 30, 2020 at 8:28:18 AM UTC-7	September 30, 2020 at 11:42:54 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	September 16, 2020 at 7:30:41 AM UTC-7	September 16, 2020 at 7:45:03 AM UTC-7	-
Storagegateway operational issue	Closed	Issue	us-east-1	September 13, 2020 at 12:46:47 PM UTC-7	September 13, 2020 at 6:32:24 PM UTC-7	-
Deepracer operational issue	Closed	Issue	us-east-1	August 31, 2020 at 6:32:39 PM UTC-7	August 31, 2020 at 9:10:12 PM UTC-7	-

## Dettagli dell'evento

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

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

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

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

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

Example : AWS Health evento per AWS Lambda

La schermata seguente mostra un evento di esempio per Lambda.

The screenshot displays the AWS Health console interface. On the left, the 'Event log' section shows a search bar with 'Add filter' and a filter for 'Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2)'. Below the filter is a 'Clear filter' button and a pagination indicator showing '1' of 1 items. The 'Event summary' section lists several operational issues, with the first one, 'Lambda operational issue', highlighted in blue. This issue has a last update of 'October 9, 2020 at 3:11:09 AM UTC-7 us-east-1'. On the right, the 'Lambda operational issue' details are shown. It includes a 'Back to list view' link, tabs for 'Details' and 'Affected resources', and a table of event data. The event data table shows the event name, status (Closed), start and end times, region/availability zone (us-east-1), and category (Issue). The description section contains a '[RESOLVED] Increased Invoke Error Rate' and two update messages: one at 02:03 AM PDT stating that an increase in invoke error rates was identified and resolution is being worked on, and another at 03:11 AM PDT stating that the issue has been resolved and the service is operating normally.

## Tipi di eventi

Esistono due tipi di AWS Health eventi:

- Gli eventi pubblici sono eventi di servizio che non sono specifici di un account. Ad esempio, se si verifica un problema con Amazon EC2 in un Regione AWS, AWS Health fornisce informazioni sull'evento, anche se non utilizzi servizi o risorse in quella regione.
- Gli eventi specifici dell'account sono specifici del tuo account o di un account della tua organizzazione. Ad esempio, se c'è un problema con un'EC2istanza Amazon in una regione che utilizzi, AWS Health fornisce informazioni sull'evento e l'elenco delle EC2 istanze Amazon interessate.

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

- Nella AWS Health Dashboard, scegli la scheda Risorse interessate per un evento. Gli eventi con risorse sono specifici per il tuo account. Gli eventi senza risorse sono pubblici e non sono specifici per il tuo account. Per ulteriori informazioni, consulta [Guida introduttiva alla AWS Health dashboard: stato del tuo account](#).
- Utilizzate il AWS Health API per restituire il eventScopeCode parametro. Gli eventi possono avere il valore PUBLIC, ACCOUNT\_SPECIFIC o NONE. Per ulteriori informazioni, vedete l'[DescribeEventDetails](#) operazione nella Guida AWS Health API di riferimento.

## Visualizzazione del calendario

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

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

### Scheduled changes

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Any event

< February 2024 >

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
28	29 2 Upcoming	30 2 Upcoming 1 Completed	31	1	2

30 January 2024

**Scheduled events starting on 30 January 2024** (Showing 3 of 3) [View all on the table view](#)

- [EKS planned lifecycle event \(us-west-2\)](#)  
Event status: **Upcoming**
- [EKS planned lifecycle event \(us-east-1\)](#)  
Event status: **Upcoming**
- [EKS planned lifecycle event \(eu-west-1\)](#)  
Event status: **Completed**

## Visualizzazione delle risorse interessate

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

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

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

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

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

The screenshot displays the AWS Health console interface for 'Scheduled changes (1)'. It features a navigation bar with tabs for 'Open and recent issues (0)', 'Scheduled changes (1)', 'Other notifications (0)', and 'Event log'. The main content area is titled 'Scheduled changes (1)' and includes a search filter, a table view selector, and a table of affected resources. The table has columns for 'Resource ID / ARN', 'Resource status', and 'Last update time'. Two resources are listed, both in a 'Pending' status, with their ARNs and last update times (3 months ago).

Resource ID / ARN	Resource status	Last update time
<a href="#">arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUU6P</a>	Pending	3 months ago
<a href="#">arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy</a>	Pending	3 months ago



# Impostazioni del fuso orario

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

Per aggiornare le impostazioni del fuso orario

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




# Lo stato di salute della tua organizzazione

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


Per ulteriori informazioni, consulta [Aggregazione di eventi AWS Health tra account con vista organizzativa](#).

### Enable organizational view

**Key benefits**

 <b>Organization-wide visibility</b> Aggregate your Health events from all member AWS accounts in your AWS organization. This provides a centralized view for all events, such as operational issues, scheduled maintenance, and account notifications.	 <b>API access</b> If you have a Business or Enterprise Support plan, you can integrate with the AWS Health API to programmatically use organizational view and look up details for events that occur in your organization. <a href="#">Learn more</a>	 <b>Chat integration</b> Using the AWS Health API, you can ingest events into your Amazon Chime or Slack channel to get notified when an event occurs. Filter events to get the ones that matter most to your organization. <a href="#">Learn more</a>
--	---	---

**Get started**

<b>1. Set up AWS Organizations</b> You must have an AWS organization with all features enabled. <span>✔ Success</span> <a href="#">Manage AWS Organizations</a>  <a href="#">View documentation</a>	<b>2. Enable organizational view for AWS Health</b> After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard. <a href="#">Enable organizational view</a> <a href="#">View documentation</a>
---	--

# Configura Amazon EventBridge

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

Da utilizzare EventBridge con AWS Health

1. Apri la AWS Health dashboard a <https://health.aws.amazon.com/health/casa>.
2. Per accedere alla EventBridge console e creare una regola, esegui una delle seguenti operazioni:
  - Dal pannello di navigazione, in Health Integrations, scegli Amazon EventBridge.
  - In Configura EventBridge, scegli Vai a. EventBridge
3. Segui questa procedura per creare regole e monitorare gli eventi. Per informazioni, consulta [Monitoraggio AWS Health degli eventi con Amazon EventBridge](#).

## AWS Health Consapevole

Puoi iniziare AWS Health API utilizzando [AWS Health Aware](#), un'applicazione a basso costo che puoi utilizzare per inviare eventi sanitari a Slack ServiceNow e altro JIRA ancora.

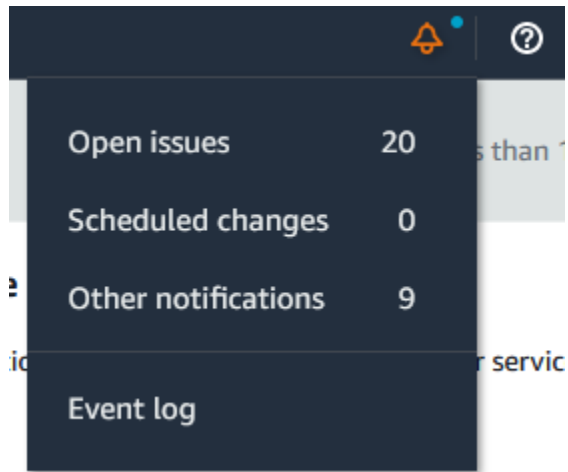
## Avvisi per eventi AWS Health

La AWS Health dashboard presenta un'icona a forma di campana nella barra di navigazione della console con un menu di avviso. Questa funzione mostra il numero di AWS Health eventi recenti che appaiono sulla dashboard in ogni categoria. Questa icona a forma di campana appare su diverse AWS console, come quelle per AmazonEC2, Amazon Relational Database Service (RDSAmazon) AWS Identity and Access Management , IAM () e. AWS Trusted Advisor

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

Example : Eventi aperti

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



A dark-themed dropdown menu is shown, likely from the AWS Health console. At the top of the menu, there is a notification bell icon with a blue dot and a help icon (a question mark in a circle). Below these icons, the menu lists four categories with their respective counts:

Category	Count
Open issues	20
Scheduled changes	0
Other notifications	9
Event log	

The menu is partially overlapping a light-colored background. Some text from the background is visible, including "s than" and "r servic".

## Configura AWS Notifiche utente per AWS Health

AWS Health fornisce informazioni sulle operazioni di assistenza, ad esempio problemi operativi, manutenzione pianificata ed eventi pianificati del ciclo di vita del software. Per una visibilità completa su AWS Health i dettagli degli eventi, come gli ID delle risorse interessate, lo stato attuale (aperto o chiuso) e lo stato delle risorse, sono una buona pratica da utilizzare AWS Health endpoint, come AWS Health API, la fonte `aws.health` in Amazon EventBridge, e il AWS Health Cruscotto. Questi endpoint forniscono le informazioni più dettagliate e in tempo reale sugli eventi e le modifiche in corso che potrebbero influire sui carichi di lavoro.

[AWS Notifiche per gli utenti](#) ti avvisa tramite canali UX aggiuntivi (e-mail, chat o notifiche push al AWS Console (applicazione mobile)). AWS Health le notifiche di eventi non contengono tutti i dati dettagliati degli endpoint sopra elencati; tuttavia, forniscono un modo semplice ed efficace per notificare agli stakeholder problemi e modifiche. In base alle regole create dall'utente, User Notifications crea e invia una notifica quando un evento corrisponde ai valori specificati in una regola. Puoi selezionare i canali di distribuzione UX a cui inviare una notifica e configurare l'aggregazione per ridurre il numero di notifiche generate per eventi specifici. Le notifiche sono visibili anche nel Centro notifiche della console. Ad esempio, puoi ricevere notifiche via chat se disponi di risorse AWS account per i quali sono previsti aggiornamenti, come le istanze di Amazon Elastic Compute Cloud (Amazon EC2).

Per saperne di più sulla configurazione AWS Notifiche utente, vedi [Guida introduttiva con AWS Notifiche per gli utenti](#).

# Accesso all'API AWS Health

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 richieste per firmare e autenticare le richieste. Per ulteriori informazioni sulle AWS Health operazioni e i parametri, consulta la Documentazione di riferimento delle [AWS Health API di riferimento](#) per ulteriori informazioni sulle operazioni e i parametri

## Note

È necessario disporre di un piano di Support Business, Enterprise On-Ramp o Enterprise [AWS Support](#) per utilizzare l'AWS Health API. Se si richiama l'AWS Health API da un AWS account che non dispone di un piano di Support Business, Enterprise On-Ramp o Enterprise, viene visualizzato un `SubscriptionRequiredException` errore di errore.

Puoi utilizzare gli AWS SDK per completare le chiamate API AWS Health REST, il che può semplificare lo sviluppo delle tue applicazioni. Tu specifichi AWS le tue credenziali e queste librerie si occupano dell'autenticazione e richiedono la firma per te.

AWS Health fornisce anche un AWS Health pannello di controllo AWS Management Console che puoi utilizzare per visualizzare e cercare gli eventi e le entità interessate. Consultare [Guida introduttiva alla AWS Health dashboard: stato del tuo account](#).


## Endpoint

L'AWS Health API segue un'architettura applicativa [multiregionale L'architettura](#) e dispone di due endpoint regionali in una configurazione attiva-passiva. Per supportare il failover DNS attivo-passivo, AWS Health fornisce un unico endpoint globale. È possibile eseguire una ricerca DNS sull'endpoint globale per determinare l'endpoint attivo e la AWS regione di firma corrispondente. Questo ti aiuta a sapere quale endpoint utilizzare nel tuo codice, in modo da poter ottenere le informazioni più recenti AWS Health.

Quando si effettua una richiesta all'endpoint globale, è necessario specificare le credenziali di AWS accesso all'endpoint regionale scelto come destinazione e configurare la firma per la propria regione. In caso contrario, l'autenticazione potrebbe fallire. Per ulteriori informazioni, consulta [Firma delle richieste API AWS Health](#).

La seguente tabella rappresenta la configurazione di default per Java è stata configurata di default

Descrizione	Regione di firma	Endpoint	Protocollo
Attivo	us-east-1	health.us-east-1.amazonaws.com	HTTPS
Passivo	us-east-2	health.us-east-2.amazonaws.com	HTTPS
Globale	us-east-1	global.health.amazonaws.com	HTTPS

 **Note**

Questa è la regione di firma dell'endpoint attivo corrente.

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

Example : ricerca DNS sull'endpoint globale

Il comando seguente completa una ricerca DNS sull'endpoint global.health.amazonaws.com . Il comando restituisce quindi l'endpoint della regione us-east-1 . Questo output indica per quale endpoint utilizzareAWS Health.

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

 **Tip**

Entrambi gli endpoint attivi e passivi restituisconoAWS Health dati. Tuttavia, iAWS Health dati più recenti sono disponibili solo dall'endpoint attivo. I dati dell'endpoint passivo saranno infine

coerenti con l'endpoint attivo. Ti consigliamo di riavviare qualsiasi flusso di lavoro quando l'endpoint attivo cambia.

## Utilizzo della demo degli endpoint ad alta disponibilità

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. Quindi, il codice riavvia il flusso di lavoro se l'endpoint attivo cambia.

### Argomenti

- [Utilizzo della demo Java ava ava ava](#)
- [Usare la demo di Python](#)

## Utilizzo della demo Java ava ava ava

### Prerequisito

È necessario installare [Gradle](#).

Per usare l'esempio di Java

1. Scarica la [demo degli endpoint AWS Health ad alta disponibilità](#) da GitHub.
2. Accedere alla `high-availability-endpoint/java` directory del progetto demo.
3. In una finestra della riga di comando, immetti il seguente comando per fare richieste ad, immetti il seguente comando

```
gradle build
```

4. Inserisci i seguenti comandi per specificare le credenziali di accesso per specificare le AWS credenziali di accesso alle credenziali

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

5. Per eseguire la demo, immettere il seguente comando per eseguire la demo demo.

**gradle run**

Example : outputAWS Health dell'evento

L'esempio di codice restituisce l'AWS Health evento recente degli ultimi sette giorni nel tuoAWS account. Nell'esempio seguente, l'output include unAWS Health evento per ilAWS 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 AWS Support [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 ava ava

- Per ulteriori informazioni, consulta l'[interfaccia HealthClient](#) nel riferimento AWS SDK for Java API e il [codice sorgente](#).
- Per ulteriori informazioni sulla libreria utilizzata in questa demo per le ricerche DNS, consulta [dnsjava](#) in GitHub.

## Usare la demo di Python

### Prerequisito

È necessario installare [Python 3](#).

Per usare l'esempio di Python

1. Scarica la [demo degli endpoint AWS Health ad alta disponibilità](#) da GitHub.
2. Accedere all'`high-availability-endpoint/python` directory del progetto demo.
3. In una finestra della riga di comando, immetti i seguenti comandi per fare richieste ad:

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

**Note**

Per Python 3.3 e versioni successive, puoi utilizzare il `venv` modulo integrato per creare l'ambiente virtuale, anziché installare `virtualenv`. Per ulteriori informazioni, vedere [venv - Creazione di ambienti virtuali](#) sul sito Web di Python.

```
python3 -m venv v-aws-health-env
```

- Per attivare l'ambiente virtuale, immettere il seguente comando per attivare l'ambiente virtuale.

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

- Inserisci il seguente comando per installare le dipendenze, immettere il seguente comando per installare le dipendenze.

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

- Inserisci i seguenti comandi per specificare le credenziali di accesso per specificare leAWS credenziali di accesso alle credenziali

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

- Per eseguire la demo, immettere il seguente comando per eseguire la demo demo.

```
python3 main.py
```

Example : outputAWS Health dell'evento

L'esempio di codice restituisce l'AWS Health evento recente degli ultimi sette giorni nel tuoAWS account. L'output seguente restituisce unAWS Health evento per una notificaAWS 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 AWS Support [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] Usare la demo di Python
```

```
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. Al termine, immetti il seguente comando per disattivare la macchina virtuale.

```
deactivate
```

## Risorse Python thon thon thon thon

- Per ulteriori informazioni su `HealthClient`, consulta la Documentazione di riferimento delle API [AWSSDK for Python \(Boto3\) per Python \(Boto3\) API Reference](#) 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.

## Firma delle richieste API AWS Health

Quando utilizzi gli AWS SDK per effettuare le richieste ad AWS, questi strumenti firmano automaticamente le richieste per te con la chiave di accesso specificata al momento della configurazione. AWS Command Line Interface AWS CLI Ad esempio, se si utilizza AWS SDK for Java per la precedente demo di endpoint ad alta disponibilità, non è necessario firmare le richieste personalmente per fare richieste ad, non è necessario firmare le richieste personalmente per fare richieste ad, per fare richieste ad, non è necessario

### Esempi di codice Java

Per altri esempi su come utilizzare l'AWS Health API con AWS SDK for Java, consulta questo [codice di esempio](#).

Quando effettui richieste ad, ti consigliamo di non utilizzare le credenziali dell'account AWS root per l'accesso regolare ad AWS Health. Puoi utilizzare le credenziali di un utente IAM. Per ulteriori informazioni, consulta [Lock Away Your AWS Account Root User Access Keys](#) nella Guida per l'utente IAM.

Se non utilizzi gli AWS SDK per fare richieste ad AWS CLI, devi firmare le richieste personalmente per firmare le richieste. Ti consigliamo di utilizzare AWS la versione Signature 4. Per ulteriori informazioni, [consulta la sezione relativa alla AWS firma delle richieste API](#) nella Riferimenti generali di AWS.

# Operazioni supportate in AWS Health

AWS Health supporta le seguenti operazioni volte a ottenere informazioni sugli eventi che interessano un account AWS:

- Tipi di evento supportati da AWS Health.
- Informazioni su uno o più eventi che soddisfano i criteri di filtro specificati.
- Informazioni sulle entità interessate da uno o più eventi.
- Conteggio suddiviso per categoria di eventi o entità che soddisfano i criteri di filtro specificati.

Tutte le operazioni sono non mutanti, ovvero recuperano i dati ma senza modificarli. Le seguenti sezioni descrivono le operazioni di AWS Health:

## Event types (Tipi di evento)

Il [DescribeEventTypes](#) operazione recupera i tipi di eventi che corrispondono al filtro opzionale specificato. Un tipo di evento è un modello di definizione di un evento AWS servizio, codice del tipo di evento e categoria. Tipo di evento ed evento sono simili a classe e oggetto nella programmazione orientata agli oggetti. Il numero di tipi di eventi supportati da AWS Health è in costante aumento.

## Eventi

Il [DescribeEvents](#) operazione recupera informazioni di riepilogo sugli eventi correlati a un AWS account. Gli eventi possono essere correlati a problemi operativi di AWS, a modifiche programmate all'infrastruttura di AWS o a notifiche di sicurezza e fatturazione. Il [DescribeEventDetails](#) operazione recupera informazioni dettagliate su uno o più eventi, come AWS servizio, regione, zona di disponibilità, orari di inizio e fine dell'evento e una descrizione testuale.

## Entità interessate

Il [DescribeAffectedEntities](#) operazione recupera informazioni sulle entità interessate da uno o più eventi. I risultati possono essere filtrati in base a criteri aggiuntivi, ad esempio lo stato, che è possibile assegnare alle risorse AWS.

## Aggregazione

Il [DescribeEventAggregates](#) operation recupera un conteggio degli eventi in ogni categoria di tipo di evento, filtrati opzionalmente in base ad altri criteri. Il [DescribeEntityAggregates](#) operazione recupera un conteggio delle entità (risorse) interessate da uno o più eventi specificati.

## AWS Organizations e visualizzazione organizzazione

### DescribeEventsForOrganization

[DescribeEventsForOrganization](#) restituisce informazioni riassuntive sugli eventi in tutto ilAWS Organizations, che soddisfa i criteri di filtro specificati.

### DescribeAffectedAccountsForOrganization

[DescribeAffectedAccountsForOrganization](#) restituisce un elenco diAWS conti nelAWS Organizationsche sono interessati dall'evento fornito.

### DescribeEventDetailsForOrganization

[DescribeEventDetailsForOrganization](#) restituisce informazioni dettagliate su uno o più eventi specificati per uno o più account inAWS Organizations.

### DescribeAffectedEntitiesForOrganization

[DescribeAffectedEntitiesForOrganization](#) restituisce un elenco di entità che sono state interessate da uno o più eventi per uno o più account dell'organizzazione, in base ai criteri di filtro.

### EnableHealthServiceAccessForOrganization

[EnableHealthServiceAccessForOrganization](#) l'operazione concede ilAWS Healthautorizzazione al servizio per interagire conAWS Organizationsper conto del cliente e applica un ruolo collegato al servizio all'account di gestione dell'organizzazione.

### DisableHealthServiceAccessForOrganization

[DisableHealthServiceAccessForOrganization](#) l'operazione revoca l'autorizzazione per ilAWS Healthservizio con cui interagireAWS Organizationsper conto del cliente.

### DescribeHealthServiceStatusForOrganization

[DescribeHealthServiceStatusForOrganization](#) l'operazione fornisce informazioni sullo stato dell'attivazione o della disabilitazioneAWS Healthlavorare con la tua organizzazione

Per ulteriori informazioni su queste operazioni, consultare[AWS HealthRiferimento alle API](#).

## Esempio di codice Java per l'API AWS Health

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

## Fase 1: Inizializzazione delle credenziali

Per comunicare con l'API AWS Health sono necessarie credenziali valide. Puoi utilizzare la key pair di qualsiasi utente IAM associato alAWSconto.

Crea e inicializza 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: Inizializzazione diAWS HealthClient API

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

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

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

## Fase 3: UtilizzaAWS HealthOperazioni 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(singletonList("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.amazonaws.services.health.model.DescribeAffectedEntitiesResult;

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

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

```
DescribeAffectedEntitiesResult response =
    awsHealthClient.describeAffectedEntities(request);

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

## DescribeEntityAggregates

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

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

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

DescribeEntityAggregatesResult response =
    awsHealthClient.describeEntityAggregates(request);

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

# Sicurezza in AWS Health

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS Health, consulta [AWS Servizi nell'ambito del programma di conformitàAWS](#) .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

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

## Argomenti

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

# Protezione dei dati in AWS Health

Il modello di [responsabilità AWS condivisa modello](#) di di si applica alla protezione dei dati in AWS Health. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione [Privacy dei dati FAQ](#). Per informazioni sulla protezione dei dati in Europa, consulta il [Modello di responsabilitàAWS condivisa e GDPR](#) il post sul blog sulla AWS sicurezza.

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere [Federal Information Processing Standard \(\) 140-3. FIPS](#)

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori AWS Health o AWS servizi utilizzi in altro modo la console, API AWS CLI, o. AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

## Crittografia dei dati

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

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

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

## Crittografia a riposo

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

## Crittografia in transito

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

## Gestione delle chiavi

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

# Gestione delle identità e degli accessi per l' AWS Health

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

## Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come AWS Health funziona con IAM](#)
- [AWS Health esempi di politiche basate sull'identità](#)
- [Risoluzione dei problemi relativi AWS Health all'identità e all'accesso](#)
- [Utilizzo di ruoli collegati ai servizi per AWS Health](#)

- [AWS politiche gestite per AWS Health](#)

## Destinatari

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

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

**Amministratore del servizio:** se sei responsabile delle AWS Health risorse della tua azienda, probabilmente hai pieno accesso a AWS Health. È tuo compito determinare a quali AWS Health funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS Health, consulta [Come AWS Health funziona con IAM](#).

**IAM amministratore:** se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche a cui gestire l'accesso AWS Health. Per visualizzare esempi di policy AWS Health basate sull'identità che puoi utilizzare in IAM, consulta [AWS Health esempi di politiche basate sull'identità](#)

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Firmare AWS API le richieste nella Guida per l'IAMutente](#).

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

## AWS account (utente root)

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

## IAM users and groups

Un [IAMutente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

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



potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

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

## IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console [cambiando ruolo](#). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Utilizzo IAM dei ruoli](#) nella Guida per l'IAMutente.

IAMI ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere [Creazione di un ruolo per un provider di identità di terze parti](#) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni IAM utente temporanee:** un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso su più account:** puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente](#). IAM
- **Accesso tra servizi:** alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni

in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- **Sessioni di accesso diretto (FAS):** quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [IAM ruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAM utente](#).
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un AWS servizio. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2 istanza e che effettuano AWS CLI o effettuano AWS API richieste. È preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2 istanza. Per assegnare un AWS ruolo a un'EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAM utente](#).

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta [Quando creare un IAM ruolo \(anziché un utente\)](#) nella Guida per l'IAM utente.

## Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni.

AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAMutente.

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

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

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

## Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

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

## Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o AWS servizi

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

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

Per ulteriori informazioni, consulta [Risorse](#).

## Liste di controllo accessi

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

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

AWS Health non supporta ACLs.

## Altri tipi di policy

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

- **Limiti delle autorizzazioni:** un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM](#)

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

## Più tipi di policy

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

## Come AWS Health funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Health, è necessario comprendere con quali IAM funzionalità è disponibile l'uso AWS Health. Per una panoramica generale del funzionamento AWS Health degli altri AWS servizi IAM, consulta [AWS Services That Work with IAM](#) nella Guida per l'IAM utente.

### Argomenti

- [Policy AWS Health basate su identità](#)
- [Policy di AWS Health basate sulle risorse](#)
- [Autorizzazione basata su tag AWS Health](#)
- [AWS Health IAM ruoli](#)

## Policy AWS Health basate su identità

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. AWS Health supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una JSON policy, consulta [IAMJSONPolicy Elements Reference](#) nella Guida per l'IAMutente.

### Azioni

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

L'Actionelemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

Le azioni politiche AWS Health utilizzano il seguente prefisso prima dell'azione: `health:`. Ad esempio, per concedere a qualcuno il permesso di visualizzare informazioni dettagliate su eventi specifici relativi all'[DescribeEventDetails](#)APIoperazione, è necessario includere l'`health:DescribeEventDetails`azione nella politica.

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

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

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

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

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

Per visualizzare un elenco di AWS Health azioni, vedere [Azioni definite da AWS Health](#) nella Guida per l'IAMutente.

## Risorse

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

L'elemento Resource JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento Resourceo un elemento NotResource. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

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

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

Ad esempio, per specificare l'EC2\_INSTANCE\_RETIREMENT\_SCHEDULED\_ABC123-DEF456evento nella tua dichiarazione, usa quanto segueARN.

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

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

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

Per ulteriori informazioni sul formato diARNs, consulta [Amazon Resource Names \(ARNs\) e AWS Service Namespaces](#).

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

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

AWS Health API le operazioni possono coinvolgere più risorse. Ad esempio, l'[DescribeEvents](#) operazione restituisce informazioni sugli eventi che soddisfano i criteri di filtro specificati. Ciò significa che un IAM utente deve disporre delle autorizzazioni per visualizzare questo evento.

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

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

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

Per visualizzare un elenco dei tipi di AWS Health risorse e relativi ARNs, consulta la sezione [Risorse definite da AWS Health](#) nella Guida per l'utente. IAM Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, consulta [Azioni definite da AWS Health](#).

## Chiavi di condizione

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

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

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



Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta [gli elementi IAM della politica: variabili e tag](#) nella Guida IAM per l'utente.

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

AWS Health definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta [AWS Global Condition Context Keys](#) nella Guida IAM per l'utente.

Le [DescribeEventDetails](#) API operazioni [DescribeAffectedEntities](#) and supportano i tasti `health:eventTypeCode` and `health:service condition`.

Per visualizzare un elenco di chiavi di AWS Health condizione, consulta [Condition Keys AWS Health nella Guida per](#) l'IAMutente. 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 politiche AWS Health basate sull'identità, vedere. [AWS Health esempi di politiche basate sull'identità](#)

## Policy di AWS Health basate sulle risorse

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

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come [principale in](#) una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il

principale e la risorsa si trovano in AWS account diversi, è inoltre necessario concedere all'entità principale l'autorizzazione ad accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [In che modo IAM i ruoli differiscono dalle politiche basate sulle risorse](#) nella Guida per l'IAMutente.

AWS Health supporta solo politiche basate sulle risorse per le operazioni e.

[DescribeAffectedEntitiesDescribeEventDetails](#)API È possibile specificare queste azioni in una politica per definire quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire azioni sull'evento. AWS Health

## Esempi

Per visualizzare esempi di politiche AWS Health basate sulle risorse, vedere. [Condizioni basate su risorse e operazioni](#)

## Autorizzazione basata su tag AWS Health

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

## AWS Health IAMruoli

Un [IAMruolo](#) è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

## Utilizzo di credenziali temporanee con AWS Health

Puoi utilizzare credenziali temporanee per accedere con la federazione, assumere un IAM ruolo o assumere un ruolo tra account. È possibile ottenere credenziali di sicurezza temporanee chiamando AWS STS API operazioni come o. [AssumeRoleGetFederationToken](#)

AWS Health supporta l'utilizzo di credenziali temporanee.

## Ruoli collegati ai servizi

[I ruoli collegati ai](#) AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nell'IAMaccount e sono di proprietà del servizio. Un IAM amministratore può visualizzare ma non modificare le autorizzazioni per i ruoli collegati al servizio.

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

È possibile utilizzare l'[EnableHealthServiceAccessForOrganization](#) operazione per creare il ruolo collegato al servizio nell'account. Tuttavia, se si desidera disabilitare questa funzionalità, è necessario prima richiamare l'[DisableHealthServiceAccessForOrganization](#) operazione. È quindi possibile eliminare il ruolo tramite la IAM console IAMAPI, o AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, vedere [Utilizzo dei ruoli collegati ai servizi nella Guida](#) per l'IAMutente.

Per ulteriori informazioni, consulta [Aggregazione di eventi AWS Health tra account con vista organizzativa](#).

## Ruoli dei servizi

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

AWS Health non supporta i ruoli di servizio.

## AWS Health esempi di politiche basate sull'identità

Per impostazione predefinita, IAM gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse. AWS Health Inoltre, non possono eseguire attività utilizzando AWS Management Console AWS CLI, o AWS API. Un IAM amministratore deve creare IAM politiche che concedano a utenti e ruoli l'autorizzazione a eseguire API operazioni specifiche sulle risorse specifiche di cui ha bisogno. L'amministratore deve quindi allegare tali politiche agli IAM utenti o ai gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta [Creazione di politiche nella JSON scheda nella Guida per l'utente](#). IAM

### Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console di AWS Health](#)

- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Accedere a e a AWS Health DashboardAWS Health API](#)
- [Condizioni basate su risorse e operazioni](#)

## Best practice per le policy

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

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere [Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM](#)
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per

richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere [Configurazione dell'API accesso MFA protetto nella Guida](#) per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate in IAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM nella Guida](#) per l'IAMutente.

## Utilizzo della console di AWS Health

Per accedere alla AWS Health console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Health risorse del tuo AWS account. Se crei una politica basata sull'identità più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per le entità (IAMutenti o ruoli) che applicano tale politica.

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

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

- Abilita o disabilita la funzionalità di visualizzazione AWS Health organizzativa per tutti gli account di un' AWS organizzazione
- AWS Health Dashboard Nella AWS Health console
- AWS Health API operazioni e notifiche
- Visualizza le informazioni sugli account che fanno parte della tua AWS organizzazione
- Visualizza le unità organizzative (OU) dell'account di gestione

Example : `AWSHealthFullAccess`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ]
    }
  ],
}
```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": "health.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "health:*",
      "organizations:DescribeAccount",
      "organizations:ListAccounts",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListParents"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "health.amazonaws.com"
      }
    }
  }
]
}

```

### Note

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

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il AWS API. Consenti invece l'accesso solo alle azioni che corrispondono all'API/operazione che stai cercando di eseguire.

Per ulteriori informazioni, consulta [Aggiungere autorizzazioni a un utente](#) nella Guida per l'IAM utente.

## Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI  
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 a e a AWS Health Dashboard AWS Health API

AWS Health Dashboard È disponibile per tutti gli AWS account. AWS Health API È disponibile solo per gli account con un piano Business, Enterprise On-Ramp o Enterprise Support. Per ulteriori informazioni, consulta [AWS Support](#).

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

Per impostazione predefinita, IAM gli utenti non hanno accesso a AWS Health Dashboard o al AWS Health API. Consenti agli utenti di accedere alle AWS Health informazioni del tuo account associando IAM politiche a un singolo utente, a un gruppo di utenti o a un ruolo. Per ulteriori informazioni, consulta [Identità \(utenti, gruppi e ruoli\)](#) e [Panoramica delle IAM politiche](#).

Dopo aver creato IAM gli utenti, puoi assegnare a tali utenti password individuali. Possono quindi accedere al tuo account e visualizzare le AWS Health informazioni utilizzando una pagina di accesso specifica per l'account. Per ulteriori informazioni, consulta [Modalità di accesso degli utenti al tuo account](#).

### Note

Un IAM utente con autorizzazioni di visualizzazione AWS Health Dashboard ha accesso in sola lettura alle informazioni sanitarie su tutti i AWS servizi dell'account, che possono includere, a titolo esemplificativo, AWS risorse IDs come EC2 istanze Amazon, indirizzi IP delle IDs EC2 istanze e notifiche di sicurezza generali.

Ad esempio, se una IAM policy concede l'accesso solo a AWS Health Dashboard e il AWS Health API, allora l'utente o il ruolo a cui si applica la policy può accedere a tutte le informazioni pubblicate sui AWS servizi e sulle risorse correlate, anche se altre IAM politiche non consentono tale accesso.

È possibile utilizzare due gruppi di APIs per AWS Health.

- Account individuali: puoi utilizzare operazioni come [DescribeEventse](#) [DescribeEventDetails](#) per ottenere informazioni sugli AWS Health eventi relativi al tuo account.
- Account organizzativo: puoi utilizzare operazioni come [DescribeEventsForOrganization](#) [DescribeEventDetailsForOrganization](#) ottenere informazioni sugli AWS Health eventi per gli account che fanno parte della tua organizzazione.



Per ulteriori informazioni sulle API operazioni disponibili, consulta la Guida [AWS Health API di riferimento](#).

## Singole operazioni

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

## Descrivere l'accesso

Questa dichiarazione politica garantisce l'accesso a tutte AWS Health Dashboard le operazioni. `Describe*` AWS Health API Ad esempio, un IAM utente con questo criterio può accedere AWS Health Dashboard a AWS Management Console e richiamare l' AWS Health `DescribeEventsAPI` operazione.

### Example : Descrivere l'accesso

```
{
  "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 al AWS Health API. Un IAM utente con questo criterio non può visualizzare AWS Management Console e non può richiamare nessuna delle AWS Health API operazioni. AWS Health Dashboard

### Example : Negare l'accesso

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

```
{
  "Effect": "Deny",
  "Action": [
    "health:*"
  ],
  "Resource": "*"
}]
}
```

## Visualizzazione organizzativa

Se si desidera abilitare la visualizzazione organizzativa per AWS Health, è necessario consentire l'accesso alle AWS Organizations azioni AWS Health e.

L'Actionelemento di una IAM policy deve includere le seguenti autorizzazioni:

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

Per comprendere esattamente le autorizzazioni necessarie per ciascuna di esseAPIs, consulta [Azioni definite da AWS Health APIs e Notifiche nella Guida](#) per l'IAMutente.

### Note

È necessario utilizzare le credenziali dell'account di gestione di un'organizzazione per accedere al AWS Health APIs modulo. AWS Organizations Per ulteriori informazioni, consulta [Aggregazione di eventi AWS Health tra account con vista organizzativa](#).

## Consenti l'accesso alla visualizzazione AWS Health organizzativa

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

## Example : Consenti l'accesso alla visualizzazione AWS Health organizzativa

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

## Negare l'accesso alla visualizzazione AWS Health organizzativa

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

## Example : nega l'accesso alla visualizzazione AWS Health organizzativa

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

**Note**

Se l'utente o il gruppo a cui desideri concedere le autorizzazioni dispone già di una IAM politica, puoi aggiungere la dichiarazione politica AWS Health specifica a quella politica.

## Condizioni basate su risorse e operazioni

AWS Health supporta [IAM le condizioni per le](#) operazioni [DescribeAffectedEntities](#) e [DescribeEventDetails](#) API. È possibile utilizzare condizioni basate su risorse e azioni per limitare gli eventi che AWS Health API invia a un utente, gruppo o ruolo.

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

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

- `eventTypeCode`
- `service`

**Note**

- Le [DescribeEventDetails](#) API operazioni [DescribeAffectedEntities](#) supportano le autorizzazioni a livello di risorsa. Ad esempio, è possibile creare una politica per consentire o negare eventi specifici. AWS Health
- Le [DescribeEventDetailsForOrganization](#) API operazioni [DescribeAffectedEntitiesForOrganization](#) and non supportano le autorizzazioni a livello di risorsa.
- Per ulteriori informazioni, consulta [Azioni, risorse e chiavi di condizione per AWS Health APIs e notifiche](#) nel Service Authorization Reference.

### Example : Condizione basata su operazioni

La presente informativa garantisce l'accesso AWS Health Dashboard e le AWS Health `Describe*` API operazioni, ma nega l'accesso a qualsiasi AWS Health evento relativo ad Amazon. EC2

```
{
```

```

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

```

Example : Condizione basata su risorse

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

```

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

```

```

  ]]
}

```

Example : condizione eventTypeCode

Questa dichiarazione politica concede l'accesso AWS Health Dashboard e le AWS Health Describe\* API operazioni, ma nega l'accesso a qualsiasi AWS Health evento eventTypeCode che corrisponda. AWS\_EC2\_\*

```

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

```

### Important

Se chiami le [DescribeEventDetails](#) operazioni [DescribeAffectedEntities](#) and e non disponi dell'autorizzazione per accedere all' AWS Health evento, viene AccessDeniedException visualizzato l'errore. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi AWS Health all'identità e all'accesso](#).

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

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

### Argomenti

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

### Non sono autorizzato a eseguire un'azione in AWS Health

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

L'`AccessDeniedException` viene visualizzato quando un utente non dispone dell'autorizzazione per l'uso AWS Health Dashboard o le AWS Health API operazioni.

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

AWS Health API richiede un piano Business, Enterprise On-Ramp o Enterprise Support di. [AWS Support](#) Se lo chiami AWS Health API da un account che non dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, viene restituito il seguente codice di errore: `SubscriptionRequiredException`

### Non sono autorizzato a eseguire iam: PassRole

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

Alcuni AWS servizi 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 IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AWS Health. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

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

Se hai bisogno di assistenza, contatta AWS l'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 IAM utente, è possibile visualizzare l'ID della 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 perdi la chiave di accesso segreta, devi aggiungere nuove chiavi di accesso all'IAM utente. 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 IAM per l'utente.

## Sono un amministratore e desidero consentire ad altri di accedere AWS Health

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

Se non si utilizza IAM Identity Center, è necessario creare IAM entità (utenti o ruoli) per le persone o le applicazioni che necessitano di accesso. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in AWS Health. Dopo aver concesso le autorizzazioni, fornisci le credenziali all'utente o allo sviluppatore dell'applicazione. Utilizzeranno tali credenziali per accedere. AWS Per ulteriori informazioni sulla creazione di IAM utenti, gruppi, politiche e autorizzazioni, consulta [IAM identità](#) e [politiche e autorizzazioni IAM nella](#) Guida per l'utente. IAM

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

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Health supporta queste funzionalità, consulta. [Come AWS Health funziona con IAM](#)
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà](#) nella Guida per l'IAM utente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAM utente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAM utente.

- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM IAM

## Utilizzo di ruoli collegati ai servizi per AWS Health

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

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

## Autorizzazioni del ruolo collegato ai servizi per AWS Health

AWS Health ha due ruoli collegati ai servizi:

- [AWSServiceRoleForHealth\\_Organizations](#)— Questo ruolo si fida che AWS Health (health.amazonaws.com) assuma il ruolo a cui accedere AWS servizi al posto tuo. A questo ruolo è associata la politica Health\_OrganizationsServiceRolePolicy AWS gestita.
- [AWSServiceRoleForHealth\\_EventProcessor](#)— Questo ruolo prevede che il AWS Health service principal (event-processor.health.amazonaws.com) assuma il ruolo al posto tuo. A questo ruolo è associata la politica AWSHealth\_EventProcessorServiceRolePolicy AWS gestita. Il responsabile del servizio utilizza il ruolo per creare una regola EventBridge gestita da Amazon per il rilevamento e la risposta agli AWS incidenti. Questa regola è l'infrastruttura necessaria Account AWS per fornire informazioni sulla modifica dello stato di allarme dal tuo account a AWS Health.

Per ulteriori informazioni sulle politiche AWS gestite, vedere [AWS politiche gestite per AWS Health](#).

## Creazione di un ruolo collegato ai servizi per AWS Health

Non è necessario creare il ruolo AWSServiceRoleForHealth\_Organizations collegato al servizio. Quando richiami l'[EnableHealthServiceAccessForOrganization](#) operazione, AWS Health crea questo ruolo collegato al servizio nell'account per te.

È necessario creare manualmente il ruolo `AWSServiceRoleForHealth_EventProcessor` collegato al servizio nel proprio account. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato al servizio](#) nella Guida per l'utente. IAM

## 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 puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Tuttavia, puoi modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio nella Guida](#) per l'IAMutente.

## Eliminazione di un ruolo collegato ai servizi per AWS Health

Per eliminare il `AWSServiceRoleForHealth_Organizations` ruolo, è necessario innanzitutto richiamare l'[DisableHealthServiceAccessForOrganization](#) operazione. È quindi possibile eliminare il ruolo tramite la IAM console IAMAPI, o AWS Command Line Interface (AWS CLI).

Per eliminare il `AWSServiceRoleForHealth_EventProcessor` ruolo, contatta AWS Support e chiedi che eliminino i tuoi carichi di lavoro da AWS Incident Detection and Response. Al termine di questo processo, puoi quindi eliminare uno dei ruoli tramite la IAM console oppure. IAM API AWS CLI

### Informazioni correlate

Per ulteriori informazioni, vedere [Utilizzo dei ruoli collegati ai servizi](#) nella Guida per l'IAMutente.

## AWS politiche gestite per AWS Health

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

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

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità

principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne AWS servizio viene lanciata una nuova o quando diventano disponibili nuove API operazioni per i servizi esistenti.

Per ulteriori informazioni, consulta [le politiche AWS gestite](#) nella Guida IAM per l'utente.

AWS Health dispone delle seguenti politiche gestite.

#### Indice

- [AWS Policy gestita: AWSHealth\\_EventProcessorServiceRolePolicy](#)
- [AWS Policy gestita: Health\\_OrganizationsServiceRolePolicy](#)
- [AWS Policy gestita: AWSHealthFullAccess](#)
- [AWS Health aggiornamenti alle politiche AWS gestite](#)

### AWS Policy gestita: AWSHealth\_EventProcessorServiceRolePolicy

AWS Health utilizza la politica [AWSHealth\\_EventProcessorServiceRolePolicy](#) AWS gestita. Questa policy gestita è attribuita al ruolo collegato ai servizi `AWSServiceRoleForHealth_EventProcessor`. La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo. Non puoi allegare questa politica alle tue IAM entità. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per AWS Health](#).

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

#### Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

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

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

```

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

```

Per un elenco delle modifiche alla politica, vedere [AWS Health aggiornamenti alle politiche AWS gestite](#).

## AWS Policy gestita: Health\_OrganizationsServiceRolePolicy

AWS Health utilizza la politica [Health\\_OrganizationsServiceRolePolicy](#) AWS gestita. Questa policy gestita è attribuita al ruolo collegato ai servizi AWSServiceRoleForHealth\_Organizations. La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo. Non puoi allegare questa politica alle tue IAM entità. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per AWS Health](#).

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

### Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

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

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

Per un elenco delle modifiche alla politica, vedere [AWS Health aggiornamenti alle politiche AWS gestite](#).

## AWS Policy gestita: AWSHealthFullAccess

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

### Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

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

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



Per un elenco delle modifiche alla politica, vedere [AWS Health aggiornamenti alle politiche AWS gestite](#).

## AWS Health aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Health da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al RSS feed sulla [Cronologia dei documenti per AWS Health](#) pagina.

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

### AWS Health

Modifica	Descrizione	Data
<a href="#">AWS Policy gestita: AWSHealthFullAccess</a> - Aggiornamento a una policy esistente	AWS Health ha esteso la AWSHealthFullAccess politica AWS GovCloud (US) Regions alle regioni cinesi.	16 ottobre 2023
<a href="#">AWS Policy gestita: Health_OrganizationsServiceRolePolicy</a> - Aggiornamento a una policy esistente	AWS Health ha aggiunto nuove AWS Organizations azioni per consentire al ruolo collegato al servizio di descrivere gli account e i AWS servizi con cui è possibile utilizzare. AWS Organizations	19 luglio 2023
Log delle modifiche pubblicato	Registro delle modifiche per le politiche AWS Health gestite.	13 gennaio 2023

## Registrazione e monitoraggio AWS Health

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Health altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per

osservare AWS Health, segnalare quando qualcosa non va e intraprendere azioni laddove opportuno:

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

Per ulteriori informazioni, consulta [Monitoraggio AWS Health](#).


## Convalida della conformità per AWS Health

Per sapere se un AWS servizio programma rientra nell'ambito di specifici programmi di conformità, consulta AWS servizi la sezione [Scope by Compliance Program AWS servizi](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- [Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

 Note

Non tutte sono idonee. AWS servizi HIPAA Per ulteriori informazioni, consulta la [Guida ai servizi HIPAA idonei](#).

- [AWS Risorse per AWS](#) per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione AWS servizi e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- [Evaluating Resources with Rules](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub](#)— Ciò AWS servizio fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): AWS servizio rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò AWS servizio consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

## Resilienza in AWS Health

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

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

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta [AWS Global Infrastructure](#).

## Sicurezza dell'infrastruttura nell' AWS Health

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

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

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

## Analisi della configurazione e della vulnerabilità in AWS Health

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

## Best practice relative alla sicurezza di AWS Health

Consulta le seguenti best practice per lavorare con AWS Health.

## Concedi AWS Health agli utenti le autorizzazioni minime possibili

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

Per ulteriori informazioni, consulta [AWS Health esempi di politiche basate sull'identità](#).

## Visualizza il AWS Health Dashboard

Controlla AWS Health Dashboard spesso per identificare gli eventi che potrebbero influire sul tuo account o sulle tue applicazioni. Ad esempio, potresti ricevere una notifica di evento sulle tue risorse, come un'istanza Amazon Elastic Compute Cloud (AmazonEC2) che deve essere aggiornata.

Per ulteriori informazioni, consulta [Guida introduttiva alla AWS Health dashboard: stato del tuo account](#).

## Integrazione AWS Health con Amazon Chime o Slack

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

## Monitora gli AWS Health eventi

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

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

Per ulteriori informazioni, consulta [Monitoraggio AWS Health degli eventi con Amazon EventBridge](#).

# Aggregazione di eventi AWS Health tra account con vista organizzativa

Per impostazione predefinita, puoi usare AWS Health per visualizzare ilAWS Health eventi di un singoloAWS conto. Se si utilizza AWS Organizations, è anche possibile visualizzare gli eventi AWS Health a livello centrale nell'organizzazione. Questa funzione consente di accedere alle stesse informazioni delle operazioni con account singolo. Puoi utilizzare i filtri per visualizzare gli eventi in account, servizi e regioni AWS specifici.

Puoi aggregare gli eventi per identificare gli account della tua organizzazione interessati da un evento operativo o ricevere notifiche per le 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. Utilizzare questa funzionalità per rimanere informati sulle prossime modifiche ai servizi AWS che potrebbero richiedere aggiornamenti o modifiche al codice.

È una buona pratica utilizzare [Amministratore delegato](#) funzionalità per delegare l'accesso alAWS Health Visualizzazione organizzativa dell'account di un membro. Ciò semplifica l'accesso dei team operativi aAWS Health eventi nella tua organizzazione. La funzionalità Delegated Administrator ti consente di mantenere limitato il tuo account di gestione, fornendo al contempo ai team la visibilità di cui hanno bisogno per agireAWS Health eventi.

## Important

- AWS Health non registra gli eventi che si sono verificati nell'organizzazione prima che sia stata abilitata la visualizzazione organizzativa. Ad esempio, se un account membro (111122223333) della tua organizzazione ha ricevuto un evento per Amazon Elastic Compute Cloud (Amazon EC2) prima che tu abiliti questa funzione, questo evento non verrà visualizzato nella tua vista organizzativa.
- AWS Health gli eventi inviati per gli account dell'organizzazione verranno visualizzati nella visualizzazione organizzativa finché l'evento è disponibile, fino a 90 giorni, anche se uno o più di 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, è necessario:

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

Puoi anche accedere come utente root (opzione non consigliata) nell'account di gestione della tua organizzazione. Per ulteriori informazioni, vedere [Blocca il tuo AWS chiavi di accesso utente root dell'account](#) nel Guida per l'utente IAM.

- Se accedi come utente IAM, utilizza una policy IAM che concede l'accesso a AWS Health azioni delle organizzazioni, come [AWSHealthFullAccess](#) politica. Per ulteriori informazioni, consulta [AWS Health esempi di politiche basate sull'identità](#).

### Argomenti

- [Visualizzazione organizzativa \(console\)](#)
- [Vista organizzativa \(CLI\)](#)
- [Visualizzazione organizzativa dell'amministratore delegato](#)

## Visualizzazione organizzativa (console)

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

La visualizzazione organizzativa è disponibile nella AWS Health console per tutti i AWS Support 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](#) politica. Per ulteriori informazioni, consulta [AWS Health esempi di politiche basate sull'identità](#).

### Indice

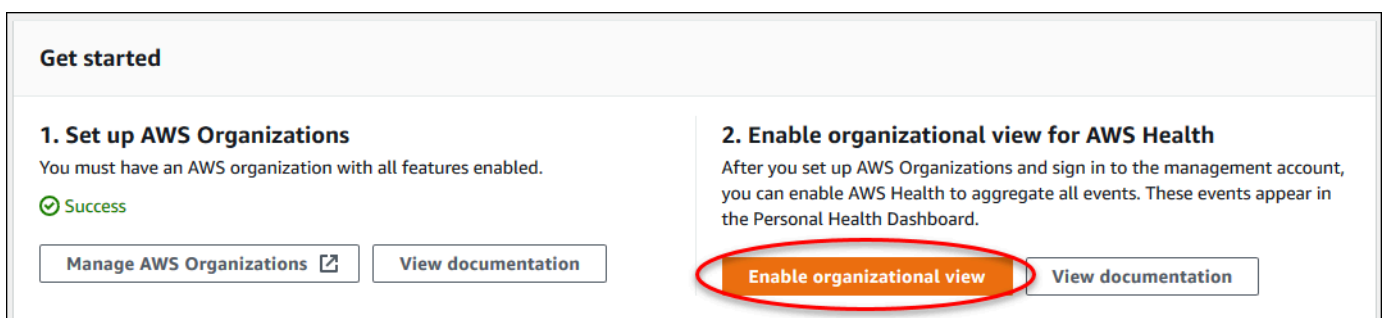
- [Attivazione della visualizzazione organizzativa \(console\)](#)
- [Visualizzazione degli eventi di visualizzazione organizzativa \(console\)](#)
  - [Questioni aperte e recenti](#)
  - [Modifiche pianificate](#)
  - [Altre notifiche](#)
  - [Log degli eventi](#)
- [Visualizzazione degli account e delle risorse interessati \(console\)](#)
- [Disattivazione della visualizzazione organizzativa \(console\)](#)

## Attivazione della visualizzazione organizzativa (console)

È possibile abilitare la visualizzazione organizzativa dallaAWS Health console. È necessario accedere all'account di gestione dell'AWSorganizzazione.

Per visualizzare ilAWS Health Dashboard dell'organizzazione

1. Apri la tuaAWS Health dashboard all'[indirizzo https://health.aws.amazon.com/health/home](https://health.aws.amazon.com/health/home).
2. Nel riquadro di navigazione, in Lo stato dell'organizzazione, in Lo stato di salute dell'organizzazione, in Lo stato di salute dell'organizzazione, in
3. Nella pagina Abilita visualizzazione organizzativa, scegli Abilita visualizzazione organizzativa.



4. (Facoltativo) Se desideri apportare modifiche alle tueAWS organizzazioni, ad esempio creare unità organizzative (OU), scegli GestisciAWS Organizations.

Per ulteriori informazioni, consulta [Nozioni di base su AWS Organizations](#) nella Guida per l'utente di AWS Organizations.



### Note

- L'attivazione di questa funzionalità è un processo asincrono e richiederà tempo per essere completata. A seconda del numero di account nell'organizzazione, il caricamento degli account può richiedere alcuni minuti. Puoi uscire e controllare laAWS Health console in un secondo momento.
- In presenza di un piano di Support Business, Enterprise On-Ramp o Enterprise, è possibile chiamare l'operazione [DescribeHealthServiceStatusForOrganization](#)API per verificare lo stato del processo.
- Quando si abilita questa funzionalità, il ruoloAWSServiceRoleForHealth\_Organizations collegato al servizio con la policyHealth\_OrganizationsServiceRolePolicyAWS gestita viene applicato all'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per AWS Health](#).

## Visualizzazione degli eventi di visualizzazione organizzativa (console)

Dopo avere abilitato la visualizzazione organizzativa,AWS Health visualizza gli eventi di salute per tutti gli account dell'organizzazione.

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

AWS manterrà i dati della policy dell'account per 90 giorni a partire dalla data di validità della chiusura dell'account amministratore. Al termine del periodo di 90 giorni, AWS elimina definitivamente tutti i dati delle policy per l'account.

- Per conservare i risultati per più di 90 giorni, puoi archiviare le policy. È inoltre possibile utilizzare un'operazione personalizzata con una EventBridge regola per memorizzare i risultati in un bucket S3.
- Finché AWS conserva i dati delle policy, quando si riapre l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati delle policy 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, laAWS Health console può visualizzare gli eventi pubblici dalla [AWS HealthDashboard — Stato del servizio](#) negli ultimi 7 giorni. Questi eventi pubblici non sono specifici degli account dell'organizzazione. Gli eventi delAWS Health Dashboard — Service Health forniscono informazioni pubbliche sulla disponibilità regionale deiAWS servizi.

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

#### Argomenti

- [Problemi aperti e recenti](#)
- [Modifiche pianificate](#)
- [Altre notifiche](#)
- [Log degli eventi](#)

#### Questioni aperte e recenti

È possibile utilizzare la scheda Problemi aperti e recenti per visualizzare gli eventi che potrebbero influire sull'AWSinfrastruttura, ad esempio modificheAWS servizi e risorse che influiscono sull'organizzazione.

#### Per visualizzare eventi organizzativi

1. Apri la tuaAWS Health dashboard all'[indirizzo https://health.aws.amazon.com/health/home](https://health.aws.amazon.com/health/home).
2. Nel riquadro di navigazione, sotto Salute della tua organizzazione, scegli Problemi aperti e recenti per visualizzare gli eventi segnalati di recente.
3. Scegliere un evento. Nella scheda Dettagli, è possibile esaminare le seguenti informazioni sull'evento:

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

Example : Questioni aperte per visualizzazione organizzativa

Il seguente evento Amazon Relational Database Service (Amazon RDS) viene visualizzato nella scheda Problemi aperti e recenti per la visualizzazione organizzativa e riguarda un account dell'organizzazione.

**Open issues** View event log

View events that might affect your AWS infrastructure, such as changes to AWS services and resources.

< 1 >

**Event summary**

- [EC2 operational issue](#)  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1
- [S3 operational issue](#)  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1
- [RDS storage issue](#)**  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1
- [RDS storage issue](#)  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1
- [EC2 operational issue](#)  
Last update: November 18, 2020 at 1:51:23 AM UTC-8 us-east-1
- [CloudFront operational issue](#)  
Last update: November 18, 2020 at 2:10:46 AM UTC-8 us-east-1
- [EC2 scheduled maintenance issue](#)  
Last update: November 18, 2020 at 7:50:26 AM UTC-8 us-east-1

**RDS storage issue** Back to list view

**Details** | Affected accounts

**Event data**

Event	RDS storage issue	Start time	November 18, 2020 at 7:50:10 AM UTC-8
Status	Open	End time	-
Region / Availability Zone	us-east-1a	Category	Issue
Affected accounts	1		

**Description**

Unfortunately, there was an unrecoverable storage failure on your Amazon RDS instance associated with this event. As a result, your instance has been put in a storage failed state.

You can recover your database instance at your earliest convenience by using one of the following methods:

- 1) Using your latest snapshot - you can view the available backups on the AWS Management Console under the "Snapshots" tab. More information on restoring from a DB snapshot can be found here: [http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ShareSnapshot.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapshot.html)

## 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 dei certificati, notifiche di fatturazione e vulnerabilità di sicurezza.

## Log degli eventi

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

Per visualizzare eventi organizzativi nella scheda Registro eventi

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

Example : scheda del registro degli eventi per la visualizzazione organizzativa

Il seguente esempio di evento Amazon DynamoDB (DynamoDB) viene visualizzato nella scheda Registro eventi e riguarda due account dell'organizzazione.

The screenshot displays the AWS Health console interface. On the left, an 'Event log' section contains a search bar and a list of events. The event 'EC2 instance network maintenance scheduled' is highlighted. The main area shows the 'Event data' for this event, including start and end times, status, region, and affected accounts. A detailed description explains the maintenance impact and provides links for more information.

**Event log**

Q Add filter

< 1 ... >

**Event summary**

- VPN emergency maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- VPN emergency maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- ElastiCache redis maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- ElastiCache redis maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- EC2 instance network maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- EC2 instance network maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- Direct Connect maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- Direct Connect maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- Lambda operational issue**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- API Gateway maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- RDS storage failure MAZ**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- RDS storage maintenance scheduled**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1
- CloudFront operational issue**  
Last update: November 27, 2020 at 8:38:41 AM UTC-8 us-east-1

**EC2 instance network maintenance scheduled** Back to list view

**Details** | Affected accounts

**Event data**

Event	Start time
EC2 instance network maintenance scheduled	November 28, 2020 at 8:38:20 AM UTC-8
Status	End time
Upcoming	November 29, 2020 at 8:38:20 AM UTC-8
Region / Availability Zone	Category
us-east-1a	Scheduled change
Affected accounts	
2	

**Description**

One or more of your Amazon EC2 instances is scheduled for maintenance on for hours starting at UTC. During this time, the instances associated with this event in the us-east-1 region will continue to run but will experience a loss of network connectivity.

Normal network connectivity to your instances will be restored after the maintenance is complete. You can maintain normal network connectivity during this time by migrating the instances listed above to replacement instances. Replacement instances will not be affected by this scheduled maintenance. Otherwise, no action is required on your part.

You can see more information on this maintenance in the AWS Management Console at </ec2/home?region=us-east-1#s=Events>

Additional information about maintenance events, including how to migrate to replacement instances, can be found at [http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/monitoring-instances-status-check\\_sched.html](http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/monitoring-instances-status-check_sched.html)

We perform maintenance regularly to ensure that the EC2 service continues uninterrupted for our customers. In most cases, maintenance can be performed without service interruption. When maintenance cannot be performed without service interruption, we work hard to keep any impact as brief as possible.

If you have any questions or concerns, you can contact the AWS Support Team on the community forums and via AWS Premium Support at: <http://aws.amazon.com/support>

## Visualizzazione degli account e delle risorse interessati (console)

Nella sezione Stato della tua organizzazione, puoi visualizzare gli account dell'organizzazione interessati dall'evento e tutte le risorse correlate. Ad esempio, in presenza di un evento imminente per la manutenzione delle istanze Amazon Elastic Compute Cloud (Amazon EC2), gli account dell'organizzazione con 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](https://health.aws.amazon.com/health/home).
2. Nel riquadro di navigazione, in Lo stato di salute dell'organizzazione, in Lo stato di salute dell'organizzazione, in La salute dell'organizzazione, in La salute dell'organizzazione, in
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 sugli account:
  - ID account
  - Account name (Nome account)
  - Email primaria
  - Unità organizzativa (UO)

**EC2 instance network maintenance scheduled** Back to list view

Details | **Affected accounts**

**Affected accounts (1)** Show account details

Q Add filter < 1 >

Account ID	Account name	Primary email	Organizational unit
▼ 123456789012	Jane Doe AWS account	janedoe@example.com	r-abcd

6. Espandi l'account per visualizzare le risorse interessate.

**EC2 instance network maintenance scheduled** Back to list view

Details | **Affected accounts**

**Affected accounts (1)** Show account details

Q Add filter < 1 >

Account ID	Account name	Primary email	Organizational unit
▼ 123456789012	Jane Doe AWS account	janedoe@example.com	r-abcd
arn:aws:ec2:us-east-1:123456789012:instance/i-01cdfc3fc1example			
arn:aws:ec2:us-east-1:123456789012:instance/example-entity-name-2			

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 e quindi inserisci l'ID dell'account. Puoi inserire un solo ID account alla volta.
- b. Seleziona Apply (Applica). L'account che hai inserito viene visualizzato nell'elenco.

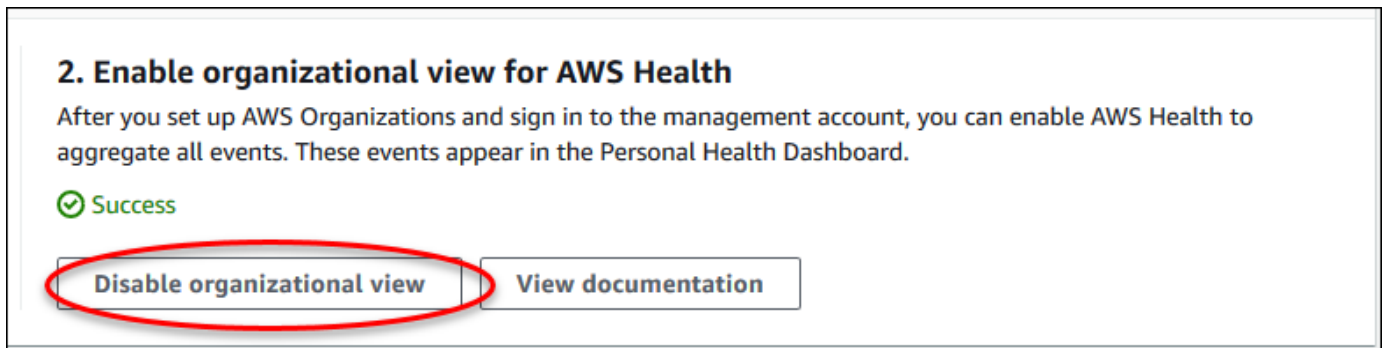
## Disattivazione della visualizzazione organizzativa (console)

Se non desideri aggregare eventi per la tua organizzazione, puoi disattivare questa funzionalità dall'account di gestione.

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

Per disattivare la visualizzazione organizzativa

1. Apri la tua AWS Health dashboard all'[indirizzo https://health.aws.amazon.com/health/home](https://health.aws.amazon.com/health/home).
2. Nel riquadro di navigazione, in Lo stato dell'organizzazione, in Lo stato di salute dell'organizzazione, in Lo stato di salute dell'organizzazione, in
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 viene eliminato tramite la console AWS Identity and Access Management (IAM), l'API IAM o la AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consultare [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Vista organizzativa (CLI)

È inoltre possibile abilitare la funzionalità di visualizzazione organizzativa dall'AWS Command Line Interface (AWS CLI) invece di AWS Health console. Per utilizzare la console, consulta [Attivazione della visualizzazione organizzativa \(console\)](#).

### Note

Se si desidera consentire agli utenti di accedere all'account di gestione per la funzionalità di visualizzazione organizzativa, devono disporre di autorizzazioni come [AWSHealthFullAccess](#) politica. Per ulteriori informazioni, consulta [AWS Health esempi di politiche basate sull'identità](#).

### Indice

- [Attivazione della visualizzazione organizzativa \(CLI\)](#)
- [Visualizzazione degli eventi di visualizzazione organizzativa \(CLI\)](#)
- [Disattivazione della visualizzazione organizzativa \(CLI\)](#)
- [Operazioni API di visualizzazione organizzativa AWS Health](#)

## Attivazione della visualizzazione organizzativa (CLI)

È possibile abilitare la visualizzazione organizzativa utilizzando [EnableHealthServiceAccessForOrganization](#) Funzionamento dell'API.

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

### Note

- Devi avere un [Affari](#), [Enterprise On-Ramp](#), oppure [Impresa](#) Piano di supporto per chiamare il AWS Health API.
- È necessario utilizzare l'endpoint della regione Stati Uniti orientali (Virginia settentrionale).



## Example

Il comando AWS CLI seguente abilita questa funzione dal tuo account AWS. 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 [EnableHealthServiceAccessForOrganization](#) Funzionamento dell'API.

### Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

### Java

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

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

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
    software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRequest;
import
    software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse;
import
    software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
import
    software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

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, `AWSServiceRoleForHealth_Organizations` [ruolo collegato ai servizi](#) `Health_OrganizationsServiceRolePolicy` AWS. La politica gestita viene applicata all'account di gestione dell'organizzazione.

#### Note

L'attivazione di questa funzionalità è un processo asincrono e richiederà tempo per essere completata. Puoi chiamare il [DescribeHealthServiceStatusForOrganization](#) operazione per verificare lo stato del processo.

## Visualizzazione degli eventi di visualizzazione organizzativa (CLI)

Dopo aver attivato questa funzionalità, AWS Health inizia a registrare eventi che interessano gli account nell'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 che sia stata abilitata la visualizzazione organizzativa.

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

AWS manterrà i dati della policy dell'account per 90 giorni a partire dalla data di validità della chiusura dell'account amministratore. Al termine del periodo di 90 giorni, AWS elimina definitivamente tutti i dati delle policy per l'account.

- Per conservare i risultati per più di 90 giorni, puoi archiviare le policy. Puoi anche usare un'azione personalizzata con `EventBridge` regola per archiviare i risultati in un bucket S3.
- Finché AWS conserva i dati delle policy, quando si riapre l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati delle policy di servizio per l'account.
- Per ulteriori informazioni, vedere [Chiusura di un account](#).

**⚠ Important**

Per i clienti nelle regioni AWS GovCloud (US):

- Prima di chiudere l'account, esegui il backup e quindi elimina le risorse dell'account. Dopo aver chiuso l'account, non avrai più accesso ad essi.

È possibile utilizzare le operazioni API AWS Health per restituire gli eventi dalla vista organizzativa.

Example : descrivere gli eventi di visualizzazione organizzativa

Il comando AWS CLI seguente restituisce eventi di integrità dello stato per gli account AWS dell'organizzazione.

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

Consulta la sezione seguente per altre operazioni API AWS Health.

## Disattivazione della visualizzazione organizzativa (CLI)

È possibile disattivare la visualizzazione organizzativa utilizzando [DisableHealthServiceAccessForOrganization](#) Funzionamento dell'API.

Example

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

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

**📘 Note**

È inoltre possibile disattivare la funzionalità organizzativa utilizzando le Organizzazioni [DisabilitaAWSServiceAccess](#) Funzionamento dell'API. Dopo aver chiamato questa operazione, AWS Health interrompe l'aggregazione degli eventi per tutti gli altri account dell'organizzazione. Se si chiamano le operazioni API AWS Health per la visualizzazione organizzativa, AWS Health restituisce un errore. AWS Health continua ad aggregare gli eventi sanitari per il tuo account AWS.

Dopo aver disattivato questa funzionalità, AWS Health non aggrega più gli eventi dell'organizzazione. Tuttavia, il ruolo collegato al servizio rimane nell'account di gestione fino a quando non lo si elimina tramite AWS Identity and Access Management console (IAM), API IAM o AWS CLI. Per ulteriori informazioni, vedere [Eliminazione di un ruolo collegato al servizio](#) nella Guida per l'utente IAM.

## Operazioni API di visualizzazione organizzativa AWS Health

È possibile utilizzare le seguenti operazioni API AWS Health per la visualizzazione organizzativa:

- [DescribeEventsForOrganization](#)— Restituisce informazioni di riepilogo sugli eventi in tutta l'organizzazione.
- [DescribeAffectedAccountsForOrganization](#)— Restituisce un elenco di AWS account dell'organizzazione interessati dall'evento specificato.
- [DescribeEventDetailsForOrganization](#)— Restituisce informazioni dettagliate sugli eventi specificati per uno o più account dell'organizzazione.
- [DescribeAffectedEntitiesForOrganization](#)— Restituisce un elenco di entità che sono state interessate da uno o più eventi per uno o più account di un'organizzazione.

È possibile utilizzare le seguenti operazioni per abilitare o disabilitare AWS Health dalla collaborazione con le organizzazioni:

- [EnableHealthServiceAccessForOrganization](#)— Sovvenziona l'autorizzazione a interagire con le organizzazioni e applica la reflex all'account di gestione dell'organizzazione.
- [DisableHealthServiceAccessForOrganization](#)— Revoca l'autorizzazione per interagire con le organizzazioni.
- [DescribeHealthServiceStatusForOrganization](#)— Restituisce informazioni sullo stato se AWS Health è abilitato per la tua organizzazione.

È necessario disporre di un piano Business, Enterprise On-Ramp o Enterprise Support per chiamare queste operazioni API. Se si chiamano le operazioni `DescribeEventForOrganization` e `DescribeAffectedAccountsForOrganization` da un account con almeno un piano di supporto Business, è possibile restituire informazioni su qualsiasi account dell'organizzazione, indipendentemente dal livello di supporto dei singoli account. Fare riferimento agli esempi riportati di seguito.

Example Esempio: un'organizzazione con account con piani di supporto Business e Developer

- Nella tua organizzazione sono presenti tre account. L'account di gestione dispone di un piano di supporto aziendale e gli altri due account hanno un piano di supporto per sviluppatori.
- Tu chiami il `DescribeEventForOrganization` Funzionamento dell'API dall'account di gestione o da un account che può assumere il ruolo con le autorizzazioni richieste.
- AWS Health restituisce informazioni per tutti e tre gli account.

Se chiami

il `DescribeEventDetailsForOrganizationDescribeAffectedEntitiesForOrganizationOper` API da un account che dispone almeno di un piano di supporto aziendale, puoi restituire solo informazioni sugli account dell'organizzazione che dispongono di un piano di supporto Business, Enterprise On-Ramp o Enterprise.

Example Esempio: un'organizzazione con account che dispone di piani di supporto aziendale, aziendale e per gli sviluppatori

- Hai cinque account nella tua organizzazione. L'account di gestione dispone di un piano di supporto Enterprise, due account hanno un piano di supporto aziendale e due account hanno un piano di supporto per sviluppatori.
- Tu chiami il `DescribeEventDetailsForOrganization` Funzionamento dell'API dall'account di gestione.
- AWS Health restituisce informazioni solo per gli account che dispongono di un piano di supporto Enterprise o Business. Gli account con un piano di supporto Developer vengono visualizzati nel `failedSet` della risposta.

## Visualizzazione organizzativa dell'amministratore delegato

Con AWS Health, puoi sfruttare la funzionalità di amministratore delegato da AWS Organizations che consente la visualizzazione aggregata di un account diverso dall'account di gestione AWS Health eventi sul [AWS Health Pannello di controllo](#) o programmaticamente tramite il [AWS Health API](#). La funzionalità di amministratore delegato offre la flessibilità ai diversi team di visualizzare e gestire gli eventi sanitari in tutta l'organizzazione. È un AWS best practice di sicurezza per delegare responsabilità al di fuori dell'account di gestione, ove possibile.

Indice

- [Registra un amministratore delegato per la tua visione organizzativa](#)
- [Rimuovi un amministratore delegato dalla tua vista organizzativa](#)

## Registra un amministratore delegato per la tua visione organizzativa

Dopo aver abilitato la visualizzazione organizzativa per la tua organizzazione, puoi registrare fino a cinque account membri nell'organizzazione come amministratore delegato. Per fare ciò, chiama il [RegisterDelegatedAdministrator](#) Funzionamento dell'API. Dopo aver registrato gli account dei membri, questi diventano amministratori delegati e possono accedere aiAWS Healthvista organizzativa dalAWS HealthPannello di controllo. Se l'account ha un [Affari](#), [Enterprise On-Ramp](#), oppure [Impresa](#) Piano di supporto, quindi gli amministratori delegati possono utilizzare ilAWS HealthAPI per accedere aAWS Healthvista organizzativa.

Per stabilire un amministratore delegato, dall'account di gestione della tua organizzazione, chiama quanto segueAWS Command Line Interface(AWS CLIcomando). È possibile utilizzare questo comando dall'account di gestione o da un account che può assumere il ruolo richiestoAWS Identity and Access Managementautorizzazioni. Nel seguente comando di esempio, sostituisciACCOUNT\_IDcon l'ID dell'account membro che desideri registrare insieme alAWS Healthresponsabile del 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, hai visibilità su tuttoAWS Healtheventi che riguardano gli account di tutta l'organizzazione. Puoi visualizzare gli eventi storici degli ultimi 90 giorni o da quando la funzionalità di visualizzazione organizzativa è stata attivata per la prima volta, 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 richiede fino a un minuto per essere completata.

## Rimuovi un amministratore delegato dalla tua vista organizzativa

Per rimuovere l'accesso a un amministratore delegato, chiama il [DeregisterDelegatedAdministrator](#) Funzionamento dell'API.

Dall'account di gestione della tua organizzazione, chiama quanto segueAWS CLIcomando per rimuovere un account membro come amministratore delegato. Nel seguente comando di esempio, sostituisciACCOUNT\_IDcon l'ID dell'account membro che desideri rimuovere.

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



# Monitoraggio AWS Health degli eventi con Amazon EventBridge

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

## Note

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

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

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

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

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

## Argomenti

- [Informazioni per Regioni AWSAWS Health](#)
- [Informazioni sugli eventi pubblici per AWS Health](#)
- [Processore di eventi per AWS Health](#)
- [Creazione di una EventBridge regola per AWS Health](#)
- [AWS Health Schema degli eventi Amazon EventBridge](#)
- [AWS Health Impaginazione degli eventi su EventBridge](#)
- [Aggregazione degli AWS Health eventi utilizzando la visualizzazione organizzativa e l'accesso amministrativo delegato](#)
- [Ricezione di eventi con AWS HealthAWS Chatbot](#)
- [Automazione delle azioni per le istanze Amazon EC2](#)
- [Configura i connettori SMC per AWS Health](#)

## Informazioni per Regioni AWSAWS Health

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

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

Ad esempio, se stai monitorando eventi nella regione Europa (Francoforte) e tale regione è temporaneamente non disponibile, AWS Health invieremo l'evento anche nella regione Stati Uniti occidentali (Oregon). Successivamente, la tua EventBridge regola di backup invia l'evento ai target

che hai specificato. Per creare una regola di backup, segui la procedura seguente [Creazione di una EventBridge regola per AWS Health](#) e utilizza la regione Stati Uniti occidentali (Oregon).

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

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

## Informazioni sugli eventi pubblici per AWS Health

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

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

### Important

Per ricevere entrambi i tipi di eventi, la regola deve utilizzare il "source":

[ "aws.health" ] valore. I caratteri jolly, ad esempio "source": [ "aws.health\*" ] non corrispondono allo schema da monitorare per eventuali eventi.

Se stai monitorando eventi pubblici da un Regione AWS, ti consigliamo di creare una regola di backup. Gli eventi pubblici di AWS Health vengono inviati contemporaneamente sia alla regione interessata che a una regione di backup. Si consiglia di deduplicare AWS Health gli eventi utilizzando eventARN e CommunicationID perché questi rimangono coerenti per AWS Health i messaggi inviati alla regione di backup.

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

Esempio: eventi pubblici per Amazon Elastic Compute Cloud

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

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

## Processore di eventi per AWS Health

Se utilizzi AWS Incident Detection and Response per il tuo account, devi [installare il ruolo `AWSServiceRoleForHealth\_EventProcessor` collegato al servizio](#) nel tuo account.

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

Questo ruolo crea quindi una regola EventBridge gestita da Amazon nel tuo account. La regola è denominata `AWSHealthEventProcessor-D0-NOT-DELETE`. Questa regola è l'infrastruttura necessaria per il tuo account in modo che EventBridge possa fornire informazioni sulla modifica dello stato di allarme dal tuo account a AWS Health.

### Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Utilizzo di ruoli collegati ai servizi per AWS Health](#)
- [AWS Policy gestita: `AWSHealth\_EventProcessorServiceRolePolicy`](#)

## Creazione di una EventBridge regola per AWS Health

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

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

Per creare una EventBridge regola per AWS Health

1. Apri la EventBridge console Amazon all'[indirizzo https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina. Scegli la regione in cui desideri tenere traccia degli eventi. AWS Health

3. Nel pannello di navigazione, scegli Regole.
4. Scegli Crea regola.
5. Nella pagina Definisci dettagli della regola, inserisci un nome e una descrizione per la regola.
6. Mantieni i valori predefiniti di per Bus di eventi e Tipo di regola, quindi scegli Avanti.
7. Nella pagina Crea modello di evento, per Origine evento, scegli AWS eventi ed eventi EventBridge partner.
8. In Event pattern, per Event source, scegli AWS servizi.
9. In Schema di eventi, per AWS servizio, scegli Health.
10. Per Tipo di evento, scegli una delle seguenti opzioni.
  - Specific Health Abuse Events: crea una regola per AWS Health gli eventi che hanno la parola Abuse nel nome del tipo di evento.
  - Eventi Health specifici: crea una regola per gli eventi per uno specifico AWS servizio, come Amazon EC2.
11. Puoi scegliere Qualsiasi servizio o Servizi specifici. Se hai scelto un servizio specifico, scegli una delle seguenti opzioni:
  - Scegliete Qualsiasi categoria di tipo di evento per creare una regola che si applica a tutte le categorie di tipi di evento.
  - Scegli le categorie di tipi di eventi specifici, quindi scegli un valore dall'elenco, ad esempio issue, AccountNotification o ScheduledChange.

#### Tip

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

12. Se hai scelto una categoria specifica di servizi e tipi di eventi, scegli una delle seguenti opzioni per i codici dei tipi di evento.

- Scegliete Qualsiasi codice del tipo di evento per creare una regola che si applica a tutti i codici dei tipi di evento.
  - Scegli uno o più codici di tipo di evento specifici, quindi scegli uno o più valori dall'elenco. Questo crea una regola che si applica solo a codici di tipi di eventi specifici. Ad esempio, se scegli **AWS\_EC2\_INSTANCE\_STOP\_SCHEDULED** e **AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED**, la regola si applica solo a questi eventi quando si verificano nel tuo account.
13. Scegli una delle seguenti opzioni per le risorse interessate.
    - Scegli Qualsiasi risorsa per creare una regola valida per tutte le risorse.
    - Scegli Risorse specifiche e inserisci gli ID di una o più risorse. Ad esempio, puoi specificare un ID di istanza Amazon EC2, come *I-ExampleA1B2C3DE4*, per monitorare gli eventi che riguardano solo questa risorsa.
  14. Rivedi la configurazione delle regole in modo che soddisfi i requisiti di monitoraggio degli eventi.
  15. Seleziona Successivo.
  16. Nella pagina Seleziona obiettivi, scegli il tipo di oggetto che hai creato per questa regola, quindi configura le opzioni aggiuntive necessarie per quel tipo. Ad esempio, potresti inviare l'evento a una coda Amazon SQS o a un argomento Amazon SNS.
  17. Seleziona Successivo.
  18. (Facoltativo) Nella pagina Aggiungi tag, aggiungi tag alla chiave, quindi scegli Avanti.
    - Nota: attualmente i tag non vengono inviati dalla fonte aws.health in. EventBridge
  19. Nella pagina Rivedi e crea, rivedi la configurazione della regola e fai in modo che soddisfi i requisiti di monitoraggio degli eventi.
  20. Scegli Crea regola.

Example : regola per tutti gli eventi Amazon EC2

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

**Event pattern** [Info](#)

Event pattern form

Custom patterns (JSON editor)

**AWS service**  
The name of the AWS service as the event source

Health ▼

**Event type**  
The type of events as the source of the matching pattern

Specific Health events ▼

**i** This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

Any service

Specific service(s)

EC2 ▼

Any event type category

Specific event type category(s)

▼

Any resource

Specific resource(s)

**Event pattern**  
Event pattern, or filter to match the events

```

1 {
2   "source": ["aws.health"],
3   "detail-type": ["AWS Health Event"],
4   "detail": {
5     "service": ["EC2"]
6   }
7 }
```

Copy

Test pattern

Edit pattern

Example : regola per eventi Amazon EC2 specifici

L'esempio seguente crea una regola in modo da EventBridge monitorare quanto segue:

- Il servizio Amazon EC2
- La categoria del tipo di evento ScheduledChange
- I codici dei tipi di evento per e AWS\_EC2\_INSTANCE\_TERMINATION\_SCHEDULED  
AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED
- L'istanza con l'ID i-EXAMPLEa1b2c3de4




**AWS service**  
The name of the AWS service as the event source

Health ▼

**Event type**  
The type of events as the source of the matching pattern

Specific Health events ▼

 This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

Any service

Specific service(s)

EC2 ▼

Any event type category

Specific event type category(s)

scheduledChange ▼

Any event type code

Specific event type code(s)

▼

AWS\_EC2\_INSTANCE\_TERMINATION\_SCHEDULED ✕

AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED ✕

Any resource

Specific resource(s)

i-EXAMPLEa1b2c3de4

## Creazione di una regola per più servizi e categorie

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

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

Puoi utilizzare una delle seguenti opzioni.

Per aggiungere servizi e categorie a una regola esistente

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

Per aggiungere servizi e categorie per una nuova regola

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

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

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

Example Esempio: più servizi e categorie di tipi di eventi

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

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

## AWS Health Schema degli eventi Amazon EventBridge


Di seguito è riportato lo schema degli AWS Health eventi. Le modifiche o le aggiunte alla versione precedente dello schema sono evidenziate come «Nuovo». Dopo lo schema viene fornito un payload di esempio.

### AWS Health Schema degli eventi


#### AWS Health Schema degli eventi


Parametro	Descrizione	Richiesto
versione	EventBridge Versione, attualmente «0»	Si
id	L'uniqueEventBridge	Si

Parametro	Descrizione	Richiesto
	identificatore dell'evento	
tipo di dettaglio	Descrive il tipo di dettaglio. Per AWS Health gli eventi questo sarà &AWS Health Event o AWS Health Abuse Event	Sì
source (origine)	La fonte del bus degli eventi. Per AWS Health gli eventi questo sarà aws.health	Sì

Parametro	Descrizione	Richiesto
account	<p>L'Account ID a cui è stato inviato l'AWS Health evento.</p> <div data-bbox="1068 495 1273 1619"><p> <b>Note</b> Dal punto di vista organizzativo, questo sarà diverso dall'AffectedAccount se viene ricevuto nell'account di gestione o amministratore delegato.</p></div>	Si


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

Parametro	Descrizione	Richiesto
Regione	<p>Identifica il destinatario a Regione AWS cui è stata recapitata la notifica.</p> <div data-bbox="1068 590 1273 1619"><p> <b>Note</b> Questo campo non indica la regione interessata da questo AWS Health evento. Questo è fornito da «detail.eventRegion».</p></div>	Sì

Parametro	Descrizione	Richiesto
resources	<p>Descrive l'elenco delle risorse interessate all'interno di un account, se esistono risorse interessate.</p> <div data-bbox="1068 684 1269 1430"><p> <b>Note</b></p><p>Questo campo può essere vuoto se non ci sono risorse a cui si fa riferimento.</p></div>	No
dettaglio	<p>Questa sezione contiene tutti i dettagli dell'AWS Health evento, come elencati di seguito.</p>	Sì




Parametro	Descrizione	Richiesto	
	<p data-bbox="354 226 505 258">EventARN</p>	<p data-bbox="1068 226 1256 642">Identificatore univoco dell' AWS Health evento per la regione specifica, include la regione e l'ID dell'evento.</p>	<p data-bbox="1308 226 1341 258">Sì</p>

 **Note**


Un eventARN non è unico per un account cliente specifico o per una regione.

Parametro	Descrizione	Richiesto
	service	Le AWS servizio persone colpite dall'evento. AWS Health Ad esempio, Amazon EC2, Amazon Simple Storage Service, Amazon Redshift o Amazon Relational Database Service.


Parametro		Descrizione	Richiesto
	evento TypeCode	<p>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 due settimane prima dello StartTime.</p> <div data-bbox="1068 1646 1269 1873" style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Tutti i nuovi eventi</p> </div>	Sì

Parametro	Descrizione	Richiesto	
		<p>del ciclo di vita pianificati hanno lo stesso tipo di evento. AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT</p>	
	<p>evento TypeCategory</p>	<p>Il codice della categoria dell'evento. I valori possibili sono issue, accountNotification, investigation e scheduledChange.</p>	<p>Sì</p>


Parametro	Descrizione	Richiesto
	evento ScopeCode	Sì

Parametro	Descrizione	Richiesto
	<p data-bbox="354 226 727 260">CommunicationID (nuovo)</p> <p data-bbox="1068 226 1263 546">Un identificatore univoco per questa comunicazione relativa all'evento. AWS Health</p> <p data-bbox="1068 592 1263 1486">I messaggi con lo stesso CommunicationID sono possibili messaggi o pagine di backup di un singolo evento. AWS Health Questo identificatore può essere utilizzato con AccountID per aiutare a deduplicare i messaggi.</p> <div data-bbox="1068 1528 1269 1852"><p data-bbox="1101 1570 1221 1604"> Note</p><p data-bbox="1149 1625 1269 1843">Con la versione della funzional</p></div>	Sì

Parametro	Descrizione	Richiesto
	<p>ità di impaginazione, CommunicationID include il numero di pagina per mantenere il CommunicationID univoco tra le pagine, ad esempio 12345678-10-1. Per ulteriori informazioni, consulta <a href="#">AWS Health Impaginazione degli eventi su</a></p>	

Parametro	Descrizione	Richiesto
	<a href="#">EventBridge</a> .	
startTime	<p>L'ora di inizio dell'evento nel formato: AWS Health DoW, DD, MMM, YYYY, HH:MM:SS TZ</p> <p> <b>Note</b> L'orario di inizio può essere futuro per gli eventi programmati.</p>	Sì




Parametro	Descrizione	Richiesto
endTime	L'ora di fine dell'AWS Health evento nel formato:DoW, DD MMM YYYY HH:MM:SS TZ. <div data-bbox="1068 684 1273 1289" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>L'EndTime potrebbe non essere fornito per eventi impostati nel futuro.</p> </div>	No
ultimo UpdatedTime	L'ora dell'ultimo aggiornamento dell'AWS Health evento nel formato:DoW, DD MMM YYYY HH:MM:SS TZ.	Sì

Parametro	Descrizione	Richiesto
	<p data-bbox="354 226 516 258">statusCode</p> <p data-bbox="1068 226 1247 499">Stato dell' AWS Health evento. Le categorie di tipi hanno stati diversi.</p> <p data-bbox="1068 548 1247 919">I valori possibili per le categorie di Issue eventi sono open, closed o upcoming.</p> <p data-bbox="1068 961 1295 1283">scheduled Changes le categorie di eventi hanno stati diversi: Upcoming, Ongoing o Completed.</p> <p data-bbox="1068 1377 1263 1787">Account Notifications le categorie di eventi non hanno uno stato e sono impostate su "_".</p>	<p data-bbox="1308 226 1341 258">Sì</p>


Parametro		Descrizione	Richiesto
	Regione dell'evento	La regione interessata descritta da questo AWS Health evento.	Sì
	Descrizione dell'evento	Una sezione che descrive l' AWS Health evento. Ciò include campi per la lingua e il testo per descrivere l'evento.	Sì
	linguaggio	Lingua utilizzata nell' AWS Health evento. Questo è in genere determinato dalla regione in cui viene pubblicato l'evento. Per la regione us-east-1, questo valore è in genere «en_US».	Sì

Parametro	Descrizione	Richiesto
	<p data-bbox="591 226 927 260">Descrizione più recente</p>	<p data-bbox="1305 226 1341 260">Sì</p>

 Note

Per gli eventi pubblici, contiene solo l'ultimo aggiornamento e non l'intera cronologia dell'evento.


Parametro	Descrizione	Richiesto
	Metadati dell'evento	No

Parametro	Descrizione	Richiesto
	<p data-bbox="591 226 847 260">&lt;metadata key 1&gt;</p>	<p data-bbox="1308 226 1351 260">No</p> <div data-bbox="1068 541 1269 1570"><p data-bbox="1101 583 1221 617"> Note</p><p data-bbox="1149 638 1295 1528">Le coppie chiave-valore per i metadati degli eventi sono determinate dal servizio che ha inviato l'evento. AWS Health</p></div>

Parametro		Descrizione	Richiesto
	Entità interessate	Un array che descrive il valore delle risorse e lo stato delle risorse interessate all'interno di questo evento. AWS Health	No
	EntityValue	L'ID della risorsa/entità	No
	Ora dell'ultimo aggiornamento (nuova)	L'ora in cui lo stato di questa risorsa/entità è stato aggiornato l'ultima volta nel formato: DoW, DD MMM YYYY HH:MM:SS TZ	No


Parametro	Descrizione	Richiesto	
	status (nuovo)	Lo stato della risorsa/entità interessata. I valori possibili includono IMPAIRED,,,UN D . PENDING RESOLVED UNKNOWN	No



Parametro	Descrizione	Richiesto	
	<p data-bbox="350 226 574 264">pagina (Nuova)</p>	<p data-bbox="1068 226 1269 789">La pagina rappresentata da questo messaggio. Per ulteriori informazioni, consulta <a href="#">AWS Health Impaginazione degli eventi su EventBridge</a>.</p> <div data-bbox="1068 827 1269 1866" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px;"> <p data-bbox="1101 865 1221 903"> Note</p> <p data-bbox="1149 924 1286 1866">L'impaginazione avviene solo sulle risorse. Altre cause della violazione e del limite di 256 KB causeranno l'interruzione della</p> </div>	<p data-bbox="1305 226 1334 264">Sì</p>

Parametro	Descrizione	Richiesto
	comunica: ione.	


Parametro	Descrizione	Richiesto
	<p>TotalPages (nuovo)</p>	<p>Si</p>

 **Note**

Puoi usarlo per determinare se hai ricevuto tutte le pagine di una comunicazione multipagina per

Parametro	Descrizione	Richiesto
	un account.	

Parametro	Descrizione	Richiesto	
	<p>Account interessato (nuovo)</p>	<p>Questo è l'AccountID dell'account interessato.</p>	<p>Si</p>

 **Note**

Questo campo può essere diverso dal campo «account» se questo evento sanitario viene inviato a un account che fa parte di un account AWS Organizations e viene ricevuto nell'account di

Parametro	Descrizione	Richiesto
	gestione o amministratore delegato.	

## Public Health Event - 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",
    "affectedAccount": "123456789012",
  }
}

```

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

```

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

```

```

    "affectedAccount": "123456789012",
  }
}

```

## AWS Health Evento specifico dell'account: riduzione delle prestazioni di Amazon EC2 Instance Store Drive

```

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

```



```
}  
}
```

## AWS Health Impaginazione degli eventi su EventBridge

AWS Health supporta l'impaginazione degli AWS Health eventi quando l'elenco di «risorse» o «AffectedEntities» fa sì che la dimensione del messaggio superi il limite di 256 KB di dimensione dei messaggi. In precedenza, AWS Health non comunicava l'elenco completo delle risorse con gli eventi quando superava questo limite.

AWS Health ora include tutte le «risorse» e «detail.affectedEntities» nel messaggio. Se questo elenco di «risorse» e «detail.affectedEntities» supera i 256 KB, AWS Health divide l'evento sanitario in più pagine e pubblica queste pagine come singoli messaggi in EventBridge. Ogni pagina conserva gli stessi eventARN e communicationID per aiutare a ricombinare l'elenco di «resources» o «detail.affectedEntities» dopo che tutte le pagine sono state ricevute.

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

Sono incluse diverse modifiche allo schema per supportare il lancio della paginazione. Ogni CommunicationID ora include il numero di pagina sillabato dopo il CommunicationID, anche quando è presente solo 1 pagina. Sono inoltre disponibili due nuovi campi, detail.page e detail.totalPages, che descrivono il numero di pagina corrente e il numero totale di pagine dell'evento. AWS Health Le informazioni contenute in ogni messaggio impaginato sono le stesse ad eccezione dell'elenco di «detail.affectedEntities» o «resources». Questi elenchi possono essere ricostruiti dopo aver ricevuto tutte le pagine. Le pagine delle risorse e delle entità interessate sono indipendenti dall'ordine.

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

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

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

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

## Ricezione di eventi con AWS HealthAWS Chatbot

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

### Prerequisiti

Prima di iniziare, devi avere quanto segue:

- Un client di chat configurato con AWS Chatbot. Puoi configurare Amazon Chime e Slack. Per ulteriori informazioni, consulta [Guida introduttiva AWS Chatbot](#) nella Guida per l'AWS Chatbot amministratore.
- 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 AWS Chatbot

1. Segui la procedura descritta [Creazione di una EventBridge regola per AWS Health](#) al punto 13.
  - a. Al termine della configurazione dello schema di eventi nel passaggio 13, aggiungi una virgola all'ultima riga dello schema e aggiungi la riga seguente per rimuovere i messaggi di chat non necessari dagli eventi impaginati AWS Health . Per informazioni, consulta [AWS Health Impaginazione degli eventi su EventBridge](#).

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



- b. Quando scegli l'obiettivo nel [passaggio 14](#), scegli un argomento SNS. Utilizzerai lo stesso argomento SNS nella AWS Chatbot console.
  - c. Completa il resto della procedura per creare la regola.
2. Passare alla [console AWS Chatbot](#).
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 EventBridge che corrisponde alla tua regola, l' AWS Health evento verrà visualizzato nel tuo client di chat.

6. Scegli il nome dell'evento per visualizzare ulteriori informazioni nella tua AWS Health dashboard.

Example : AWS Health eventi inviati a Slack

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

**AWS** APP 11:46 AM  
 [AWS Health Event | us-east-1 | Account: 123456789012 | open](#)  
Event type code: AWS\_EC2\_PERSISTENT\_INSTANCE\_RETIREMENT\_SCHEDULED  
EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance associated with this event in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2021-03-19 18:36:40 PST. Please take appropriate action before this time.\\n\\nYou can find more information about retirement events scheduled for your EC2 instances in the AWS Management Console <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Events>\\n\\n\* What will happen to my instance?\\nYour instance will be stopped after the specified retirement date. You can start it agai...  
[Show more](#)  
Start time: Sat, 20 Mar 2021 01:35:40 GMT  
End time: Sat, 20 Mar 2021 01:36:40 GMT

**AWS** APP 12:08 PM  
 [AWS Health Event | us-east-1 | Account: 123456789012 | open](#)  
Event type code: AWS\_S3\_OPEN\_ACCESS\_BUCKET\_NOTIFICATION  
We are writing to notify you that you may have exposed your S3 bucket/s to a larger audience than you intended. AWS recommends that you review your bucket permissions and ACLs to determine whether the access is appropriate. S3 bucket permissions should never contain \\\"Principal\\\": \\\"\*\\\" unless you intend to grant public access to your data. Additionally, S3 bucket ACLs should be appropriately scoped to prevent unintended access to \\\"Authenticated Users\\\" or \\\"Everyone\\\" unless your use case requires it.\\n\\nThe list of buckets with this configuration is associated with this event.\\n\\nThe following links provide an overv...  
[Show more](#)  
Start time: Sat, 20 Mar 2021 01:35:40 GMT  
End time: Sat, 20 Mar 2021 01:36:40 GMT

## Automazione delle azioni per le istanze Amazon EC2

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 EventBridge regola può quindi richiamare obiettivi, come i documenti di AWS Systems Manager automazione, per automatizzare le azioni per tuo conto.

Ad esempio, quando viene pianificato un evento di ritiro di un'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 istanze Amazon EC2, le istanze devono essere gestite da Systems Manager.

Per ulteriori informazioni, consulta [Automating Amazon EC2 EventBridge with nella Amazon EC2 User Guide](#).

## Prerequisiti

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

### Creazione di una policy IAM

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

### Per creare una policy IAM

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

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

```

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

```

- a. Nel Resource parametro, per Amazon Resource Name (ARN), inserisci l'ID del tuo AWS account.
- b. Puoi anche sostituire il nome del ruolo o utilizzare quello predefinito. Questo esempio utilizza *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 di revisione della politica, inserisci un nome, ad esempio **AutomationEV, e una descrizione facoltativa RolePolicy**.
10. Consulta la pagina di riepilogo per vedere le autorizzazioni consentite dalla politica. Se sei soddisfatto della tua politica, scegli Crea politica.

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

### Creazione di un ruolo IAM

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

Per creare un ruolo per un AWS servizio

1. Accedi AWS Management Console e apri la console IAM all'[indirizzo https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio).
4. Scegli EC2 per il servizio a cui desideri consentire l'assunzione di questo ruolo.
5. Scegli Successivo: autorizzazioni.
6. Inserisci il nome della politica che hai creato, ad esempio **AutomationEV RolePolicy**, quindi seleziona la casella di controllo accanto alla politica.
7. Scegli Successivo: Tag.
8. (Facoltativo) Puoi aggiungere metadati al ruolo collegando i tag come coppie chiave-valore.
9. Scegli Prossimo: Rivedi.
10. **Per Nome ruolo, inserisci AutomationEvRole**. Questo nome deve essere lo stesso nome che appare nell'ARN della policy IAM che hai creato.
11. (Facoltativo) In Role description (Descrizione ruolo), immettere una descrizione per il nuovo ruolo.
12. Rivedere il ruolo e scegliere Crea ruolo.

Per ulteriori informazioni, consulta [Creating a role for an AWS service](#) nella IAM User Guide.

## Aggiorna la politica di fiducia

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

Per aggiornare la politica di fiducia per il ruolo

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

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

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

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



## Crea una regola per EventBridge

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

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

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

Ad esempio, per le istanze supportate da Amazon EC2 EBS, scegli.

**AWS\_EC2\_PERSISTENT\_INSTANCE\_RETIREMENT\_SCHEDULED** Per le istanze archiviate su istanze Amazon EC2, scegli. **AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED**

11. Seleziona Qualsiasi risorsa.

Il modello del tuo evento sarà simile al seguente esempio.

### Example

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

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

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

Il tuo obiettivo dovrebbe essere simile all'esempio seguente.

### Target Remove

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

SSM Automation

Document

AWS-RestartEC2Instance

► **Configure document version**

▼ **Configure automation parameter(s)**

No Parameter(s)

Constant

**Input Transformer**

```
["Instances": "$resources"]
```

```
["InstanceId": <Instances>]
```

EventBridge needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

Create a new role for this specific resource

**Use existing role**

AutomationEVRole

#### 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 Create (Crea) .

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

## Configura i connettori SMC per AWS Health

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

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

[Per ulteriori informazioni sull' ServiceNow integrazione tramite SMC, vedere Integrazione in. AWS Health ServiceNow](#)

[Per ulteriori informazioni sull'integrazione di JIRA Management Cloud tramite SMC, vedere in JIRA.AWS Health](#)

# Monitoraggio AWS Health

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

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

Puoi utilizzare Amazon EventBridge per ricevere notifiche sugli AWS Health eventi che potrebbero influire sui tuoi servizi e risorse. Ad esempio, se AWS Health pubblica un evento sulle tue EC2 istanze Amazon, puoi utilizzare queste notifiche per intervenire e aggiornare o sostituire le tue risorse secondo necessità. Per ulteriori informazioni, consulta [Monitoraggio AWS Health degli eventi con Amazon EventBridge](#).

- AWS CloudTrail acquisisce le API chiamate e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di registro a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la [Guida per l'utente AWS CloudTrail](#).

## Argomenti

- [Registrazione delle AWS Health API chiamate con AWS CloudTrail](#)

## Registrazione delle AWS Health API chiamate con AWS CloudTrail

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

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

Per ulteriori informazioni CloudTrail, incluso come configurarlo e abilitarlo, consulta la [Guida per l'AWS CloudTrail utente](#).

## AWS Health informazioni in CloudTrail

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

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

- [Panoramica della creazione di un trail](#)
- [CloudTrail Servizi e integrazioni supportati](#)
- [Configurazione di Amazon SNS Notifications per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

[Tutte AWS Health API le operazioni vengono registrate CloudTrail e documentate nel Reference.AWS Health API](#) Ad esempio, le chiamate alle `DescribeAffectedEntities` operazioni `DescribeEvents` `DescribeEventDetails`, e generano voci nei file di CloudTrail registro.

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

- Se la richiesta è stata effettuata con root o credenziali 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 l'[CloudTrail userIdentityelemento](#).

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 registro sono crittografati con la crittografia lato server di Amazon S3 (). SSE

Per ricevere una notifica al momento della consegna dei file di registro, puoi CloudTrail configurare la pubblicazione di SNS notifiche Amazon quando vengono consegnati nuovi file di registro. Per ulteriori informazioni, consulta [Configurazione di Amazon SNS Notifications per CloudTrail](#).

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

Per ulteriori informazioni, consulta [Ricezione di file di CloudTrail registro da più regioni](#) e [Ricezione di file di CloudTrail registro da più account](#).

## Esempio: voci AWS Health dei file di registro

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

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'[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"
}
],
...
}
```



# Cronologia dei documenti per AWS Health

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

- APIversione: 2016-08-04

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

Modifica	Descrizione	Data
<a href="#">Informazioni aggiornate sul download delle risorse interessate</a>	Per ulteriori informazioni, consulta <a href="#">Visualizzazione delle risorse interessate</a> .	27 luglio 2024
<a href="#">È stata rimossa la privacy del traffico Internet dalla documentazione della sezione Sicurezza AWS Health</a>	Per ulteriori informazioni, consulta <a href="#">Sicurezza in AWS Health</a> .	27 marzo 2024
<a href="#">Aggiornamento della AWS Health dashboard: stato del servizio ed eventi del ciclo di vita pianificato per la documentazione. AWS Health</a>	Per ulteriori informazioni, consulta <a href="#">AWS Health Dashboard: stato del servizio ed eventi pianificati del ciclo di vita per. AWS Health</a>	15 febbraio 2024
<a href="#">È stato rimosso un bullet point duplicato in Creazione di EventBridge di una regola per AWS Health</a>	È stato rimosso un bullet point duplicato <a href="#">in Creazione di EventBridge una regola per. AWS Health</a>	4 dicembre 2023
<a href="#">È stata aggiunta documentazione per gli eventi del ciclo di vita pianificato</a>	Per ulteriori informazioni, vedere <a href="#">Planned Lifecycle Events</a> for. AWS Health	31 ottobre 2023
<a href="#">Documentazione per AWSHealthFullAccess aggiornata</a>	È ora possibile utilizzare e la politica AWSHealthFullAccess gestita in	16 ottobre 2023

---

	<p>AWS GovCloud (US) Regions. Vedi <a href="#">le politiche AWS gestite per AWS Health</a>.</p>	
<p><a href="#">È stata aggiunta la documentazione per la configurazione delle notifiche AWS utente in AWS Health.</a></p>	<p>Ora puoi configurare le notifiche AWS utente in AWS Health. Per ulteriori informazioni, consulta <a href="#">Configurare le notifiche AWS utente per AWS Health</a>.</p>	<p>30 agosto 2023</p>
<p><a href="#">È stata aggiunta la documentazione per la funzionalità di amministratore delegato alla sezione Aggregazione AWS Health degli eventi.</a></p>	<p>Per ulteriori informazioni, consulta <a href="#">Visualizzazione organizzativa dell'amministratore delegato</a>.</p>	<p>27 luglio 2023</p>
<p><a href="#">SLRaggiornamento della politica</a></p>	<p>Aggiornamento della politica AWS gestita: Health_OrganizationsServiceRolePolicy. Per ulteriori informazioni, consulta <a href="#">Policy gestite da AWS per AWS Health</a>.</p>	<p>19 luglio 2023</p>
<p><a href="#">AWS Health lo schema ora supporta i metadati degli eventi</a></p>	<p>Ora puoi ricevere i metadati degli eventi dagli AWS Health eventi. Per ulteriori informazioni, consulta <a href="#">Monitoraggio AWS Health degli eventi con Amazon EventBridge</a>.</p>	<p>20 giugno 2023</p>

---

<a href="#">Documentazione aggiornata per Amazon EventBridge</a>	Ora puoi utilizzare una EventBridge regola Amazon per monitorare sia gli eventi specifici dell'account che quelli pubblici. Per ulteriori informazioni, consulta <a href="#">Monitoraggio AWS Health degli eventi con Amazon EventBridge</a> .	2 maggio 2023
<a href="#">È stata aggiunta documentazione per le politiche AWS gestite</a>	È stata aggiunta documentazione per le <a href="#">politiche AWS gestite per AWS Health e l'utilizzo dei ruoli collegati ai servizi</a> per. AWS Health	18 gennaio 2023
<a href="#">Aggiunta documentazione sull'impostazione del fuso orario</a>	Utilizza la nuova funzionalità del fuso orario per visualizzare la AWS Health Dashboard nel tuo fuso orario locale o inUTC. Per ulteriori informazioni, vedi <a href="#">Guida introduttiva alla AWS Health dashboard — Stato dell'account e AWS Health Dashboard — Stato del servizio</a> .	21 settembre 2022
<a href="#">Documentazione aggiornata</a>	È stata aggiunta documentazione per AWS Health Aware. Per ulteriori informazioni, vedere <a href="#">AWS Health Aware</a> .	25 maggio 2022

---

<a href="#">Documentazione aggiornata</a>	<p>The Service Health Dashboard and the AWS Personal Health Dashboard sono stati rinominati Dashboard. AWS Health</p> <p>Per ulteriori informazioni, vedi <a href="#">Guida introduttiva alla AWS Health dashboard - Stato dell'account</a> e <a href="#">AWS Health Dashboard - Stato del servizio</a>.</p>	28 febbraio 2022
<a href="#">Documentazione aggiornata per Amazon EventBridge</a>	<p>Nuovo argomento per AWS Health utilizzare Amazon per EventBridge monitorar e gli eventi Health. Per ulteriori informazioni, consulta <a href="#">Monitoraggio AWS Health degli eventi con Amazon EventBridge</a>.</p>	3 febbraio 2022
<a href="#">Documentazione aggiornata</a>	<p>Se disponi di un piano <a href="#">Enterprise On-Ramp Support</a>, puoi utilizzare il. AWS Health API</p>	24 novembre 2021
<a href="#">Documentazione aggiunta</a>	<p>Nuovo argomento per AWS Health i concetti. Per ulteriori informazioni, vedere <a href="#">Concetti per AWS Health</a>.</p>	29 luglio 2021

<a href="#">Documentazione aggiornata per CloudWatch gli eventi</a>	È stata aggiunta una sezione su come creare una regola per più servizi e categorie di tipi di eventi. Per ulteriori informazioni, vedere <a href="#">Creazione di una regola per più servizi e categorie</a> .	7 maggio 2021
<a href="#">Documentazione aggiornata per CloudWatch gli eventi</a>	È stata aggiornata la sezione per automatizzare AWS Systems Manager le azioni per le regole di Amazon CloudWatch Events. Per ulteriori informazioni, consulta <a href="#">Automazione delle azioni per le EC2 istanze Amazon</a> .	28 Aprile 2021
<a href="#">Documentazione aggiornata per gli eventi CloudWatch</a>	È stata aggiunta una sezione per ricevere AWS Health eventi nel client di chat. Per ulteriori informazioni, consulta <a href="#">Ricezione di AWS Health eventi con AWS Chatbot</a> .	16 marzo 2021
<a href="#">Documentazione aggiornata</a>	<p>I seguenti argomenti sono stati aggiornati:</p> <ul style="list-style-type: none"><li>• È stato aggiornato l'argomento <a href="#">Aggregazione AWS Health degli eventi</a></li><li>• Riorganizzato e aggiornato l'argomento <a href="#">Monitor for AWS Health events with Amazon CloudWatch Events</a></li><li>• È stata aggiornata la <a href="#">sezione Condizioni basate su risorse e azioni</a></li></ul>	29 gennaio 2021

[È stata aggiunta la AWS Health dashboard per la visualizzazione organizzativa nella console AWS Health](#)

È possibile utilizzare la AWS Health console per abilitare la funzionalità di visualizzazione organizzativa. È quindi possibile visualizzare gli eventi sanitari relativi agli account dei membri AWS della propria organizzazione.

14 dicembre 2020

[Demo degli endpoint ad alta disponibilità](#)

È possibile utilizzare il codice di esempio per determinare l'endpoint regionale attivo e la AWS regione di firma per AWS Health

22 ottobre 2020

[Aggiornamenti alla Guida per l'AWS Health utente](#)

L'organizzazione si aggiorna e ha aggiunto un RSS feed per consentirti di abbonarti agli ultimi aggiornamenti della AWS Health documentazione.

28 agosto 2020

## Aggiornamenti precedenti

Modifica	Descrizione	Data
Aggiornato l'argomento della vista organizzativa per includere esempi.	Per informazioni, consulta <a href="#">Aggregazione di eventi AWS Health tra account con vista organizzativa</a> .	3 giugno 2020
Sicurezza e AWS Health	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di AWS Health. Per informazioni, consulta <a href="#">Sicurezza in AWS Health</a> .	5 maggio 2020

Modifica	Descrizione	Data
Aggiunta una nuova sezione per spiegare come utilizzare la visualizzazione organizzativa per gli eventi aggregati tra tutti gli account in AWS Organizations.	Per informazioni, consulta <a href="#">Aggregazione di eventi AWS Health tra account con vista organizzativa</a> .	18 dicembre 2019
È stata aggiunta una nuova sezione «Condizioni basate su risorse e azioni» per spiegare le restrizioni relative agli Eventi imposte dal. AWS Health API	Per informazioni, consulta <a href="#">Gestione delle identità e degli accessi per l' AWS Health</a> .	2 agosto 2018
È stata aggiunta una nota sulla visibilità delle informazioni. AWS Health	Per informazioni, consulta <a href="#">Gestione delle identità e degli accessi per l' AWS Health</a> .	16 agosto 2017
Release del servizio.	AWS Health rilasciato.	1° dicembre 2016

# Glossario AWS

Per la terminologia AWS più recente, consultare il [glossario AWS](#) nella documentazione di riferimento per Glossario AWS.



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