Guida per l'utente

AWS Support

Versione API 2013-04-15

AWS Support: Guida per l'utente

Table of Contents

Iniziare con AWS Support

AWS Support offre una gamma di piani che forniscono l'accesso a strumenti e competenze che supportano il successo e lo stato operativo AWS delle soluzioni. Tutti i piani di assistenza forniscono l'accesso 24 ore su 24, 7 giorni su 7 al servizio clienti, alla AWS documentazione, ai documenti tecnici e ai forum di supporto. Per il supporto tecnico e ulteriori risorse per pianificare, implementare e migliorare AWS l'ambiente, puoi scegliere un piano di supporto adatto al tuo caso d' AWS uso.

> **Note**
>
> - Per creare un caso di supporto in AWS Management Console, consultaCreazione di un caso di supporto.
> - Per ulteriori informazioni sui diversi AWS Support piani, consulta Confrontare AWS Support piani eModifica AWS Support dei piani.
> - I piani di supporto offrono tempi di risposta diversi per i tuoi casi di assistenza. Consulta Scelta del livello di gravità e Tempi di risposta.

Argomenti

Creazione di casi di supporto e gestione dei casi

In AWS Management Console, puoi creare tre tipi di casi relativi ai clienti in AWS Support:

- I casi di Supporto account e fatturazione sono disponibili per tutti i clienti AWS . Puoi ottenere assistenza su domande di fatturazione e account.
- Le richieste di aumento dei limiti di servizio sono disponibili per tutti i clienti AWS . Per ulteriori informazioni sulle Service Quotas predefinite, precedentemente chiamate limiti, consulta la sezione Service Quotas AWS nella Riferimenti generali di AWS.

- I casi di Technical support (Supporto tecnico) ti mettono in contatto con il supporto tecnico per ricevere assistenza relativa a problemi tecnici e, in alcuni casi, alle applicazioni di terze parti. Se hai sottoscritto un piano di supporto Basic, non puoi creare un caso di supporto tecnico.

> **Note**
>
> - Per modificare il piano di supporto, consulta la sezione Modifica AWS Support dei piani.
> - Per chiudere l'account, consulta la sezione Chiudere un Account nella Guida per l'utente AWS Billing .
> - Per trovare gli argomenti di risoluzione dei problemi più comuni per Servizi AWS, consultaRisorse per la risoluzione dei problemi.
> - Se sei un cliente di una società AWS Partner che fa parte di Resold Support e utilizzi Resold Support, contatta AWS Partner direttamente il tuo per qualsiasi problema relativo alla fatturazione. AWS Partner Network AWS Support non può fornire assistenza per problemi non tecnici per Resold Support, come la fatturazione e la gestione dell'account. Per ulteriori informazioni, consulta i seguenti argomenti:
>   - In che modo AWS i partner possono stabilire i AWS Support piani all'interno di un'organizzazione
>   - Supporto offerto da AWS Partner

Creazione di un caso di supporto

È possibile creare una caso di supporto nel Centro assistenza della AWS Management Console.

> **Note**
>
> - Puoi accedere a Support Center come utente root del tuo AWS account o come utente AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Gestisci l'accesso al AWS Support Centro.
> - Se non riesci ad accedere al Centro assistenza e creare una caso di supporto, in alternativa puoi usare la pagina Contattaci. Puoi utilizzare questa pagina per ottenere assistenza per problemi di fatturazione e account.

Per creare un caso di supporto

1. Accedi alla AWS Support Center Console.

   > **Tip**
   >
   > In AWS Management Console, puoi anche scegliere l'icona del punto interrogativo () e quindi scegliere Support Center.

2. Scegli Crea caso.
3. Selezionare una delle seguenti opzioni:

   - Account e fatturazione
   - Tecnico
   - Per aumenti delle quote di servizio, scegli Looking for service limit increases? (Stai cercando un aumento dei limiti di servizio?) e quindi seguire le istruzioni per Creazione di un aumento delle quote di servizio.

4. Scegli Service (Servizio), Category (Categoria), e Severity (Gravità).

   > **Tip**
   >
   > È possibile utilizzare le soluzioni consigliate che appaiono per le domande più frequenti.

5. Scegli Next step: Additional information (Fase successiva: ulteriori informazioni)
6. Nella pagina Informazioni aggiuntive, per Oggetto, inserisci un titolo relativo al problema.
7. Per Descrizione, segui le istruzioni per descrivere il caso, ad esempio:

   - Ricezione di messaggi di errore
   - Procedure di risoluzione dei problemi seguite
   - Come accedere al servizio:
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)
     - Operazioni API

8. (Facoltativo) Scegli Attach files (Allega file) per aggiungere qualsiasi file pertinente al tuo caso, come registri di errori o screenshot. Puoi allegare fino a tre file. Ogni file può essere fino a 5 MB.

9. Scegli Passaggio successivo: risolvi ora o contattaci.
10. Nella pagina Contattaci, scegli la lingua preferita.
11. Scegli il tuo metodo di contatto preferito. Puoi scegliere una delle seguenti opzioni:

    a. Web: ricevi una risposta nel Centro di Support.

    b. Chat: avvia una live chat con un agente dell'assistenza. In caso di mancata connessione a una chat, consulta Risoluzione dei problemi.

    c. Telefono – Ricevi una telefonata da un operatore di supporto. Se si sceglie questa opzione, immetti le informazioni riportate di seguito:

    - Paese o regione
    - Numero di telefono
    - (Facoltativo) Estensione

    > **Note**
    >
    > - Le opzioni di contatto che appaiono dipendono dal tipo di caso e dal piano di supporto.
    > - È possibile scegliere Discard draft (Eliminare una bozza) per cancellare la bozza del caso di supporto.

12. (Facoltativo) Se disponi di un piano di Support Business, Enterprise On-Ramp o Enterprise, viene visualizzata l'opzione Additional contacts (Contatti aggiuntivi). È possibile inserire gli indirizzi e-mail delle persone a cui inviare una notifica quando lo stato del caso cambia. Se hai effettuato l'accesso come utente IAM, includi il tuo indirizzo e-mail. Se hai effettuato l'accesso con l'indirizzo e-mail e la password dell'account root, non è necessario includere il proprio indirizzo e-mail

    > **Note**
    >
    > Se hai sottoscritto un piano di supporto Basic, l'opzione Additional contacts (Contatti aggiuntivi) non è disponibile. Tuttavia, il contatto operativo specificato nella sezione Contatti alternativi della pagina My Account riceve copie della corrispondenza dei casi, ma solo per tipi di casi specifici di account, fatturazione e tecnici.

13. Rivedi i dettagli del caso e scegli Submit (Invia). Vengono visualizzati il numero di ID caso e il riepilogo.

Descrizione del problema

La descrizione dovrebbe essere quanto più dettagliata possibile e includere informazioni sulle risorse rilevanti, oltre a qualsiasi altra informazione che potrebbe esserci utile per capire il tuo problema. Ad esempio, per la risoluzione dei problemi relativi alle prestazioni, includi time stamp e log. Per la richiesta di caratteristiche o di informazioni generali, includi una descrizione dell'ambiente e dello scopo. In tutti i casi, segui le Description Guidance (Linee guida per la descrizione) visualizzate sul modulo per l'invio del caso.

Fornendo il maggior numero di dettagli possibile, aumenti le probabilità che il tuo caso venga risolto in modo rapido.

Scelta del livello di gravità

Potresti essere incline a creare sempre un caso di supporto con la massima severità consentita dal tuo piano di supporto. Tuttavia, si consiglia di scegliere i livelli di gravità più elevati per i casi che non possono essere risolti o che influiscono direttamente sulle applicazioni di produzione. Per informazioni su come creare servizi in modo che la perdita di singole risorse non abbia conseguenze sulla tua applicazione, consulta il documento tecnico sulla Creazione di applicazioni con tolleranza ai guasti in AWS.

Nella tabella seguente sono elencati i livelli di gravità, i tempi di risposta e i problemi di esempio.

> **Note**
>
> - Non è possibile modificare il codice di gravità per un caso di supporto dopo averne creato uno. Se la situazione cambia, collabora con l' AWS Support agente responsabile della tua richiesta di assistenza.
> - Per ulteriori informazioni sul livello di gravità, consulta la Documentazione di riferimento dell'API AWS Support.

Gravità	Codice di livello di gravità	Tempo della prima risposta	Descrizione e piano di supporto
Informazioni generali	`low`	24 ore	Hai una domanda generale relativa allo sviluppo o desideri richiedere una caratteri stica. (*Piano di supporto Developer, Business, Enterprise On-Ramp o Enterprise)
Sistema impattato	`normal`	12 ore	Funzioni non critiche della tua applicazione mostrano un comportamento anomalo o hai una domanda relativa allo sviluppo legata al fattore tempo. (*Piano di supporto Developer, Business, Enterprise On-Ramp o Enterprise)
Sistema di produzione impattato	`high`	4 ore	Funzioni importanti della tua applicazione sono danneggiate o mostrano un deterioramento. (Piano di supporto Business, Enterprise On-Ramp o Enterprise)
Sistema di produzione spento	`urgent`	1 ora	L'impatto sulla tua attività è notevole. Funzioni importanti della tua applicazione non sono disponibili. (Piano di supporto Business, Enterprise On-Ramp o Enterprise)
Sistema business-critical spento	`critical`	15 minuti	La tua attività è a rischio. Funzioni critiche della tua applicazione non sono disponibili (piano di supporto Enterprise). Sono 30 minuti per il piano di supporto Enterprise On-Ramp.

Tempi di risposta

Compiamo ogni ragionevole sforzo per rispondere alle richieste iniziali nei tempi indicati. Per informazioni sull'ambito del supporto per ogni AWS Support piano, consulta AWS Support le funzionalità.

Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, puoi accedere al Support tecnico 24 ore su 24, 7 giorni su 7. *Per il piano di supporto Developer, i tempi di risposta per i casi di supporto sono calcolati in base agli orari lavorativi. L'orario lavorativo va generalmente dalle 8:00 alle 18:00 secondo il fuso orario del cliente, festività e fine settimana esclusi. Tali orari possono variare nei paesi con più fusi orari. Queste informazioni per il paese del cliente vengono visualizzate nella sezione Informazioni di contatto della pagina Il mio account in AWS Management Console.

Note

Se scegli il giapponese come lingua di contatto preferita per i casi di supporto, l'assistenza in giapponese potrebbe essere disponibile con le seguenti modalità:

- Se hai bisogno del servizio clienti per casi di supporto non tecnico o se disponi di un piano Developer Support e hai bisogno di supporto tecnico, l'assistenza in giapponese è disponibile durante l'orario lavorativo in Giappone, definito dalle 09:00 alle 18:00 del Japan Standard Time (GMT+9), esclusi i giorni festivi e i fine settimana.
- Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, il Supporto tecnico giapponese è disponibile 24 ore su 24, 7 giorni su 7.

Se scegli il cinese come lingua di contatto preferita per i casi di supporto, l'assistenza in cinese potrebbe essere disponibile con le seguenti modalità:

- Se hai bisogno del servizio clienti per casi di supporto non tecnico, l'assistenza in cinese è disponibile dalle 09:00 alle 18:00 (GMT+8), esclusi i giorni festivi e i fine settimana.
- Se disponi di un piano Developer Support, il supporto tecnico in cinese è disponibile durante l'orario lavorativo, generalmente definito dalle 8:00 alle 18:00 del tuo Paese, come stabilito in Il mio account, esclusi i giorni festivi e i fine settimana. Tali orari possono variare nei paesi con più fusi orari.
- Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, il supporto tecnico in cinese è disponibile 24 ore su 24, 7 giorni su 7.

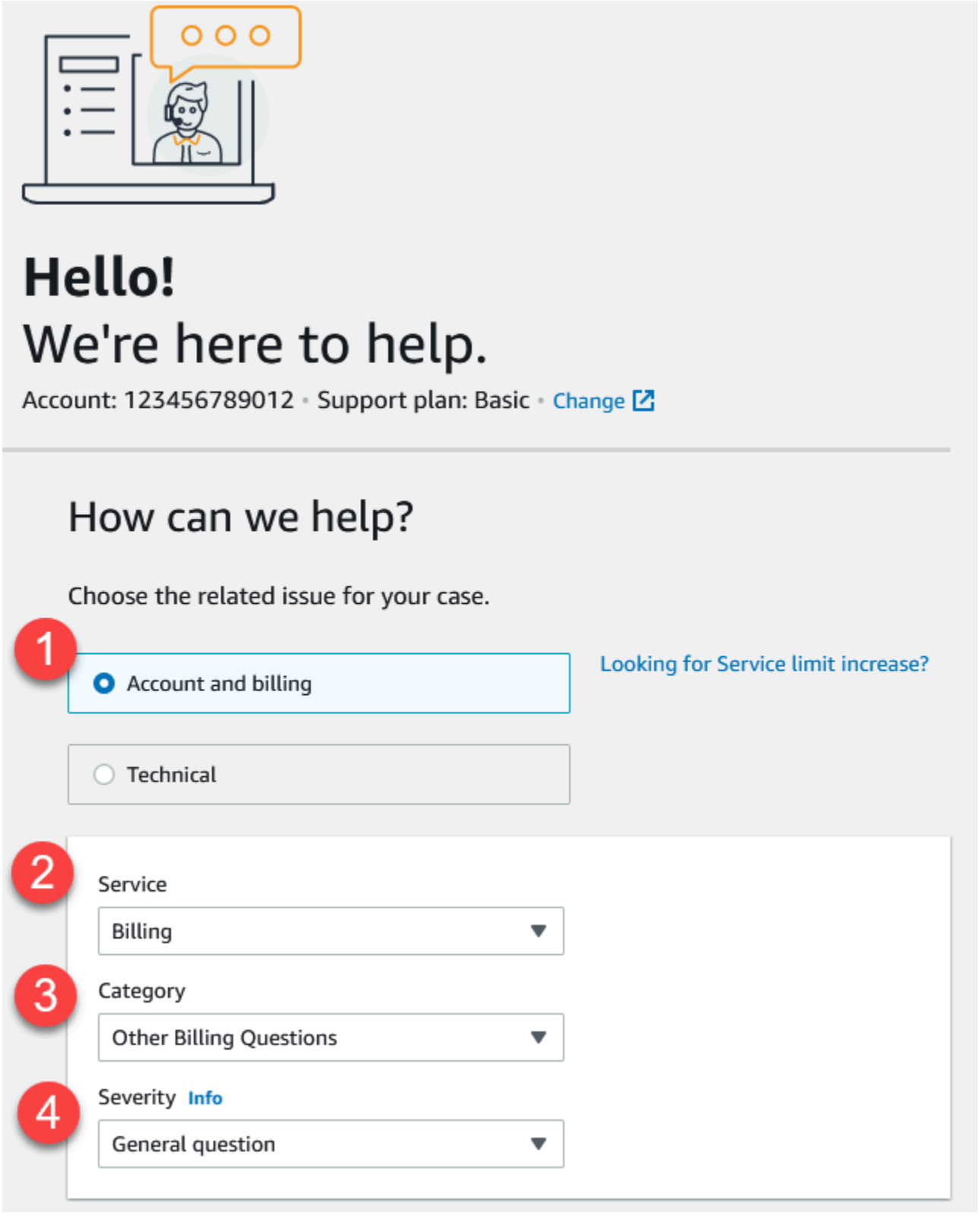
Se scegli il coreano come lingua di contatto preferita per i casi di supporto, l'assistenza in coreano potrebbe essere disponibile con le seguenti modalità:

- Se hai bisogno del servizio clienti per casi di supporto non tecnico, l'assistenza in coreano è disponibile durante l'orario lavorativo in Corea, definito dalle 09:00 alle 18:00 Korean Standard Time (GMT+9), esclusi i giorni festivi e i fine settimana.

- Se disponi di un piano Developer Support, il supporto tecnico in corenao è disponibile durante l'orario lavorativo, generalmente definito dalle 8:00 alle 18:00 del tuo Paese, come stabilito in Il mio account, esclusi i giorni festivi e i fine settimana. Tali orari possono variare nei paesi con più fusi orari.
- Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, il Supporto tecnico coreano è disponibile 24 ore su 24, 7 giorni su 7.

Esempio: crea un caso di supporto per account e fatturazione

L'esempio seguente è un caso di supporto per un problema di fatturazione e account.



1. Crea un caso: scegli il tipo di caso da creare. In questo esempio, il tipo di caso è Account e fatturazione.

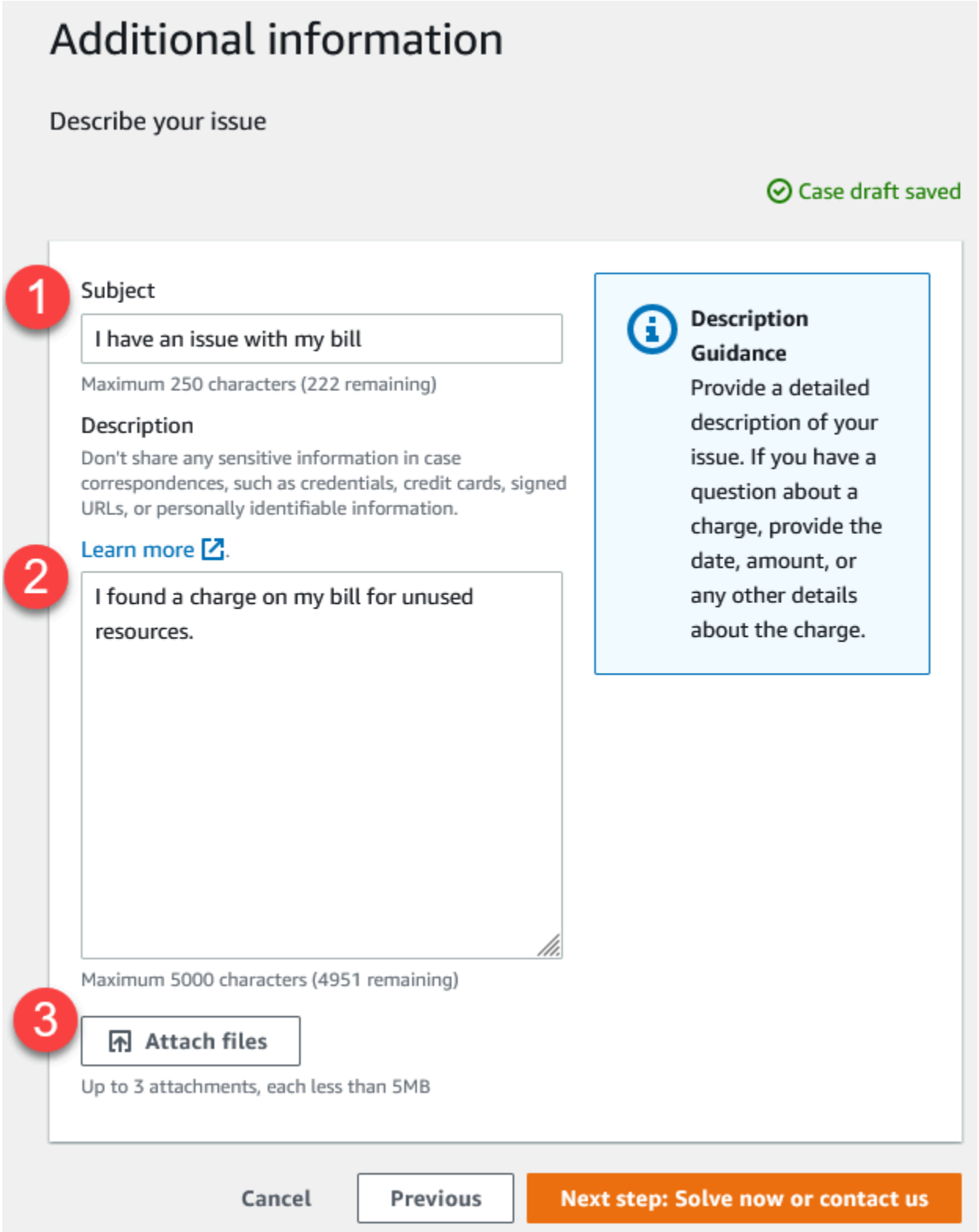
> **Note**
>
> Se hai sottoscritto un piano di supporto Basic, non puoi creare un caso di supporto tecnico.

2. Servizio – Se la tua domanda interessa più servizi, scegli il servizio a cui si applica maggiormente.
3. Categoria – Scegli la categoria che meglio si adatta al tuo caso d'uso. Quando selezioni una categoria, i collegamenti alle informazioni che potrebbero aiutarti a risolvere il problema appaiono sotto.
4. Gravità – Tutti i clienti che hanno sottoscritto un piano di supporto a pagamento possono selezionare il livello di gravità Linee guida generali (tempo di risposta di 1 giorno) o Sistema compromesso (tempo di risposta di 12 ore). I clienti che hanno sottoscritto un piano di supporto Business possono scegliere anche l'opzione Sistema di produzione compromesso (risposta in 4 ore) o Arresto del sistema di produzione (risposta in 1 ora). I clienti con un piano di supporto Enterprise On-Ramp o Enterprise possono scegliere Business-critical system down (Sistema business-critical spento) (risposta di 15 minuti per il supporto Enterprise e risposta di 30 minuti per Enterprise On-Ramp).

   I tempi di risposta sono per la prima risposta da AWS Support. Questi tempi di risposta non sono applicabili alle risposte successive. Per problemi relativi a terze parti, i tempi di risposta possono essere più lunghi, a seconda della disponibilità di personale specializzato. Per ulteriori informazioni, consulta Scelta del livello di gravità.

   > **Note**
   >
   > In base alla categoria scelta, potresti ricevere una richiesta di ulteriori informazioni.

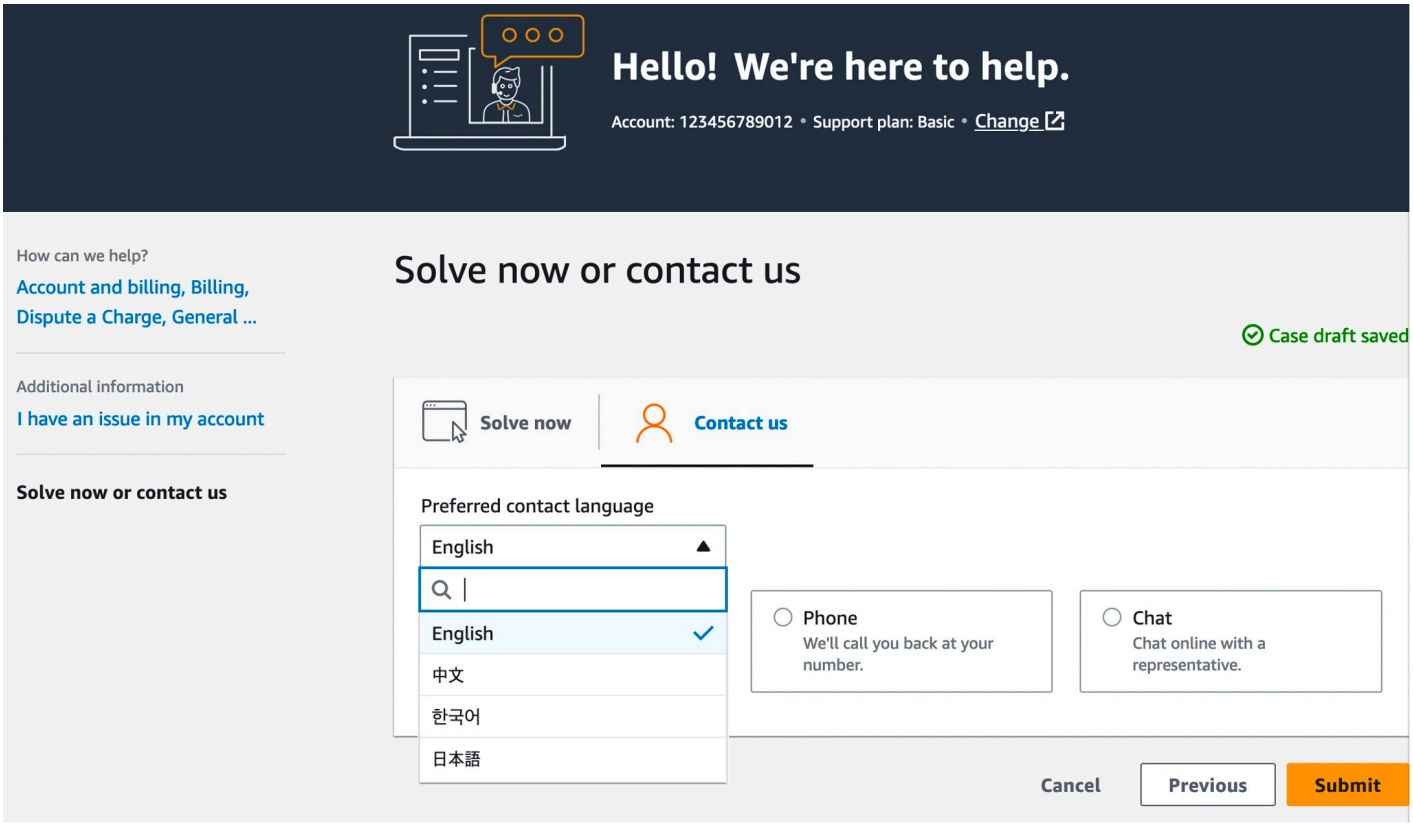
Dopo aver specificato il tipo di caso e la classificazione, puoi specificare la descrizione e il modo in cui vuoi essere contattato.



1. Oggetto – Inserisci un titolo che descriva brevemente il problema.

2. Descrizione – Descrivi il caso di supporto. Si tratta dell'informazione più importante che fornisci a AWS Support. Per alcune combinazioni di servizio e categoria, viene visualizzata una richiesta con le informazioni correlate. Usa questi link per aiutarti a risolvere il problema. Per ulteriori informazioni, consulta Descrizione del problema.
3. Allegati – Screenshot e altri allegati possono aiutare gli agenti di supporto a risolvere il tuo caso più rapidamente. Puoi allegare fino a tre file. Ogni file può essere fino a 5 MB.

Dopo aver aggiunto i dettagli del caso, puoi scegliere come vuoi essere contattato.



1. Impostazioni lingua preferita: scegli la lingua preferita. Al momento, puoi scegliere tra il cinese, l'inglese, il giapponese o il coreano. Le opzioni di contatto personalizzate nella tua lingua preferita verranno mostrate dal tuo piano di supporto.
2. Scegli un metodo di contatto. Le opzioni di contatto che appaiono dipendono dal tipo di caso e dal piano di supporto.
   - Se scegli Web, puoi monitorare il progresso del caso e rispondere nel Centro assistenza.
   - Scegli Chat o Phone (Telefono). Se selezioni Phone (Telefono), ti verrà richiesto di fornire un numero di richiamata.

3. Scegli Submit (Invia) quando le tue informazioni sono complete e il caso è pronto per essere creato.

> **Note**
>
> Se scegli il giapponese come lingua di contatto preferita per i casi di supporto, l'assistenza in giapponese potrebbe essere disponibile con le seguenti modalità:
>
> - Se hai bisogno del servizio clienti per casi di supporto non tecnico o se disponi di un piano Developer Support e hai bisogno di supporto tecnico, l'assistenza in giapponese è disponibile durante l'orario lavorativo in Giappone, definito dalle 09:00 alle 18:00 del Japan Standard Time (GMT+9), esclusi i giorni festivi e i fine settimana.
> - Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, il Supporto tecnico giapponese è disponibile 24 ore su 24, 7 giorni su 7.
>
> Se scegli il cinese come lingua di contatto preferita per i casi di supporto, l'assistenza in cinese potrebbe essere disponibile con le seguenti modalità:
>
> - Se hai bisogno del servizio clienti per casi di supporto non tecnico, l'assistenza in cinese è disponibile dalle 09:00 alle 18:00 (GMT+8), esclusi i giorni festivi e i fine settimana.
> - Se disponi di un piano Developer Support, il supporto tecnico in cinese è disponibile durante l'orario lavorativo, generalmente definito dalle 8:00 alle 18:00 del tuo Paese, come stabilito in Il mio account, esclusi i giorni festivi e i fine settimana. Tali orari possono variare nei paesi con più fusi orari.
> - Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, il supporto tecnico in cinese è disponibile 24 ore su 24, 7 giorni su 7.
>
> Se scegli il coreano come lingua di contatto preferita per i casi di supporto, l'assistenza in coreano potrebbe essere disponibile con le seguenti modalità:
>
> - Se hai bisogno del servizio clienti per casi di supporto non tecnico, l'assistenza in coreano è disponibile durante l'orario lavorativo in Corea, definito dalle 09:00 alle 18:00 Korean Standard Time (GMT+9), esclusi i giorni festivi e i fine settimana.
> - Se disponi di un piano Developer Support, il supporto tecnico in corenao è disponibile durante l'orario lavorativo, generalmente definito dalle 8:00 alle 18:00 del tuo Paese, come

stabilito in Il mio account, esclusi i giorni festivi e i fine settimana. Tali orari possono variare nei paesi con più fusi orari.

- Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, il Supporto tecnico coreano è disponibile 24 ore su 24, 7 giorni su 7.

Risoluzione dei problemi

Se riscontri problemi durante la creazione o la gestione del caso di supporto, consulta le informazioni seguenti sulla risoluzione dei problemi.

Desidero riaprire una chat dal vivo per il mio caso

Puoi rispondere al caso di supporto esistente per aprire un'altra finestra della chat. Per ulteriori informazioni, consulta Aggiornamento di un caso di supporto esistente.

Non riesco a connettermi a una chat dal vivo

Se hai scelto l'opzione Chat ma non riesci a connetterti alla finestra della chat, esegui prima i seguenti controlli:

- Assicurati di aver configurato il tuo browser per consentire le finestre a comparsa nel Centro assistenza.

  > **Note**
  >
  > Controlla le impostazioni del tuo browser. Per ulteriori informazioni, consulta i siti Web Chrome Help (Guida di Chrome) e Firefox Support (Supporto Firefox).

- Assicurati di aver configurato la tua rete in modo da poter utilizzare AWS Support:
  - La tua rete può accedere all'endpoint `*.connect.us-east-1.amazonaws.com`.

    > **Note**
    >
    > Per AWS GovCloud (US), l'endpoint è `*.connect-fips.us-east-1.amazonaws.com`.

  - Il firewall supporta le connessioni Web socket.

Tuttavia, se non riesci ancora a connetterti alla finestra della chat, contatta AWS Support utilizzando le opzioni di contatto tramite e-mail o telefono.

Creazione di un aumento delle quote di servizio

Per migliorare le prestazioni del servizio, richiedere l'aumento delle quote di servizio (precedentemente denominate limiti).

> **Note**
>
> Puoi anche utilizzare il servizio Service Quotas per richiedere direttamente un aumento per i servizi. Attualmente, Service Quotas non supporta le quote di servizio per tutti i servizi. Per ulteriori informazioni, consulta Cos'è Service Quotas? nella Guida per l'utente di Service Quotas.

Per creare un caso di supporto per un aumento delle quote di servizio

1. Accedere alla AWS Support Center Console.

   > **Tip**
   >
   > Nella AWS Management Console, puoi anche scegliere l'icona del punto interrogativo () e quindi scegli Support Center (Centro assistenza).

2. Scegli Create case (Crea caso).
3. Scegli Looking for service limit increases? (Stai cercando un aumento dei limiti di servizio?)
4. Per richiedere un aumento, segui le istruzioni. Le opzioni possibili sono le seguenti:

   - Tipo di limite
   - Gravità

   > **Note**
   >
   > In base alla categoria scelta, le istruzioni potrebbero richiedere ulteriori informazioni.

5. Per Requests (Richieste), scegli Region (Regione).

6. Per Limit (Limite), scegli il tipo di limite di servizio.
7. Per New limit value (Nuovo valore limite), immetti il valore desiderato.
8. (Facoltativo) Per richiedere un altro aumento, scegli Add another request (Aggiungi un'altra richiesta).
9. Per Case description (Descrizione del caso), descrivi il caso di supporto.
10. Per la pagina Opzioni di contatto, scegli la lingua preferita e il modo in cui vuoi essere contattato. Puoi scegliere una delle seguenti opzioni:
    - Web: ricevi una risposta nel Centro di Support.
    - Chat: avvia una live chat con un agente dell'assistenza. In caso di mancata connessione a una chat, consulta Risoluzione dei problemi.
    - Telefono – Ricevi una telefonata da un operatore di supporto. Se si sceglie questa opzione, immetti le informazioni riportate di seguito:
      - Paese/regione
      - Numero di telefono
      - (Facoltativo) Estensione
11. Scegli Submit (Invia). Vengono visualizzati il numero di ID caso e il riepilogo.

Aggiornamento, risoluzione e riapertura del caso

Dopo aver creato il caso di supporto, puoi monitorare lo stato del caso nel Centro assistenza. Un nuovo caso inizia con lo stato Non assegnato. Quando un operatore di supporto inizia a lavorare a un caso, lo stato viene modificato in Analisi in corso. L'operatore di supporto potrebbe rispondere al caso chiedendoti ulteriori informazioni (In attesa di un'operazione da parte del cliente) o per informarti che il caso è in fase di esame (In attesa di un'operazione da parte di Amazon).

Quando il tuo caso viene aggiornato, riceverai un'e-mail con la relativa corrispondenza e un link al Centro assistenza. Utilizza il link nel messaggio e-mail per accedere al caso di supporto. Non puoi rispondere alla corrispondenza relativa al caso tramite e-mail.

> **Note**
>
> - Devi accedere all'Account AWS che ha inviato la richiesta relativa al caso di supporto. Se accedi come utente AWS Identity and Access Management (IAM), devi disporre delle

autorizzazioni necessarie per visualizzare i casi di supporto. Per ulteriori informazioni, consulta Gestisci l'accesso al AWS Support Centro.

- Se non viene data una risposta al caso entro pochi giorni, il caso viene automaticamente risolto da AWS Support.
- I casi di supporto in stato risolto per più di 14 giorni non possono essere riaperti. Se si riscontra un problema simile relativo al caso risolto, è possibile creare un caso correlato. Per ulteriori informazioni, consulta Creazione di un caso correlato.

Argomenti

Aggiornamento di un caso di supporto esistente

Puoi aggiornare il caso per fornire maggiori informazioni all'operatore di supporto. Ad esempio, puoi rispondere alle corrispondenze, avviare un'altra chat dal vivo, aggiungere altri destinatari e-mail e così via. Tuttavia, non puoi aggiornare la gravità di un caso dopo averlo creato. Per ulteriori informazioni, consulta Scelta del livello di gravità.

Aggiornamento di un caso di supporto esistente

1. Accedere alla AWS Support Center Console.

   > **Tip**
   >
   > Nella AWS Management Console, puoi anche scegliere l'icona del punto interrogativo ( ) e quindi scegli Support Center (Centro assistenza).

2. Alla voce Casi di supporto aperti, seleziona l'Oggetto del caso di supporto.
3. Scegli Rispondi. Nella sezione Corrispondenza, puoi anche effettuare una qualsiasi delle seguenti modifiche:

- Fornire le informazioni richieste dall'operatore di supporto
- Caricare allegati
- Modificare il metodo di contatto preferito
- Aggiungere indirizzi e-mail per ricevere aggiornamenti sui casi

4. Scegli Submit (Invia).

> **Tip**
>
> Se hai chiuso la finestra della chat e vuoi avviare un'altra chat dal vivo, aggiungi una Reply (Risposta) al tuo caso di supporto, scegli Chat e quindi scegli Submit (Invia). Si apre una nuova finestra a comparsa della chat.

Risoluzione di un caso di supporto

Se la risposta è esaustiva o il problema è stato risolto, è possibile risolvere il caso nel Centro assistenza.

Risolvere un caso di supporto

1. Accedere alla AWS Support Center Console.

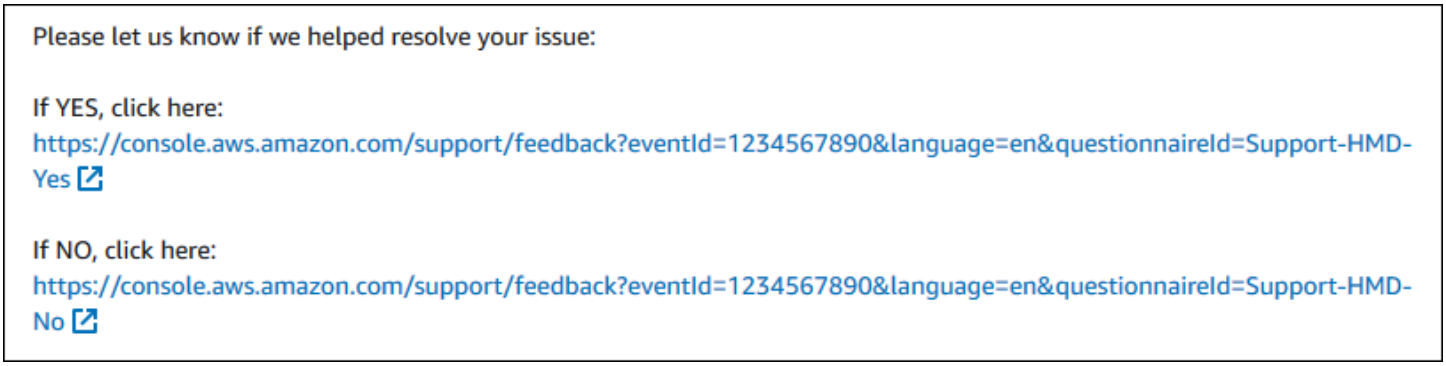
   > **Tip**
   >
   > Nella AWS Management Console, puoi anche scegliere l'icona del punto interrogativo ( ) e quindi scegli Support Center (Centro assistenza).

2. Alla voce Casi di supporto aperti, seleziona l'Oggetto del caso di supporto che desideri risolvere.
3. (Facoltativo) Seleziona Rispondi e nella sezione Corrispondenza, digita il motivo per cui si sta risolvendo il caso, quindi scegli Invia. Ad esempio, è possibile inserire informazioni su come è stato risolto autonomamente il problema, nel caso in cui queste informazioni siano necessarie per un riferimento futuro.
4. Seleziona Risolvi caso.
5. Nella finestra di dialogo, seleziona Ok per risolvere il caso.

> **Note**
>
> Se il caso è stato risolto da AWS Support è possibile utilizzare il link di feedback per fornire maggiori informazioni sulla tua esperienza con AWS Support.

Example : Link di feedback

Lo screenshot seguente mostra i link del feedback nella corrispondenza di un caso nel Centro assistenza.



Riapertura di un caso risolto

Se si verifica di nuovo lo stesso problema, è possibile riaprire il caso originale. Fornisci dettagli su quando si è verificato nuovamente il problema e quali procedure di risoluzione dei problemi sono state effettuate. Includi eventuali numeri di caso correlati in modo che l'operatore di supporto possa fare riferimento alle corrispondenze precedenti.

> **Note**
>
> - Puoi riaprire il caso di supporto fino a 14 giorni dalla risoluzione del problema. Tuttavia, non è possibile riaprire un caso inattivo da più di 14 giorni. È possibile creare un nuovo caso o un caso correlato. Per ulteriori informazioni, consulta Creazione di un caso correlato.
> - Se viene riaperto un caso esistente con informazioni diverse da quelle del problema attuale, l'operatore di supporto potrebbe chiederti di creare un nuovo caso.

Riaprire un caso risolto

1. Accedere alla AWS Support Center Console.

> **Tip**
>
> Nella AWS Management Console, puoi anche scegliere l'icona del punto interrogativo () e quindi scegli Support Center (Centro assistenza).

2. Seleziona Visualizza tutti i casi, quindi seleziona l'Oggetto o l'ID del caso del caso di supporto che si intende riaprire.
3. Seleziona Riapri il caso.
4. Alla voce Corrispondenza, nel campo Rispondi, inserisci i dettagli del caso.
5. (Facoltativo) Seleziona Scegli file per allegare file al tuo caso. Puoi allegare fino a 3 file.
6. Nella sezione Metodi di contatto, scegli una delle seguenti opzioni:
   - Web – Ricevi una notifica via e-mail e tramite il Centro assistenza.
   - Chat – Chatta online con un operatore di supporto.
   - Telefono – Ricevi una telefonata da un operatore di supporto.
7. (Facoltativo) Per la sezione Contatti aggiuntivi, inserisci gli indirizzi e-mail per gli altri destinatari a cui desideri inviare le corrispondenze del caso.
8. Rivedi i dettagli del caso e seleziona Invia.

Creazione di un caso correlato

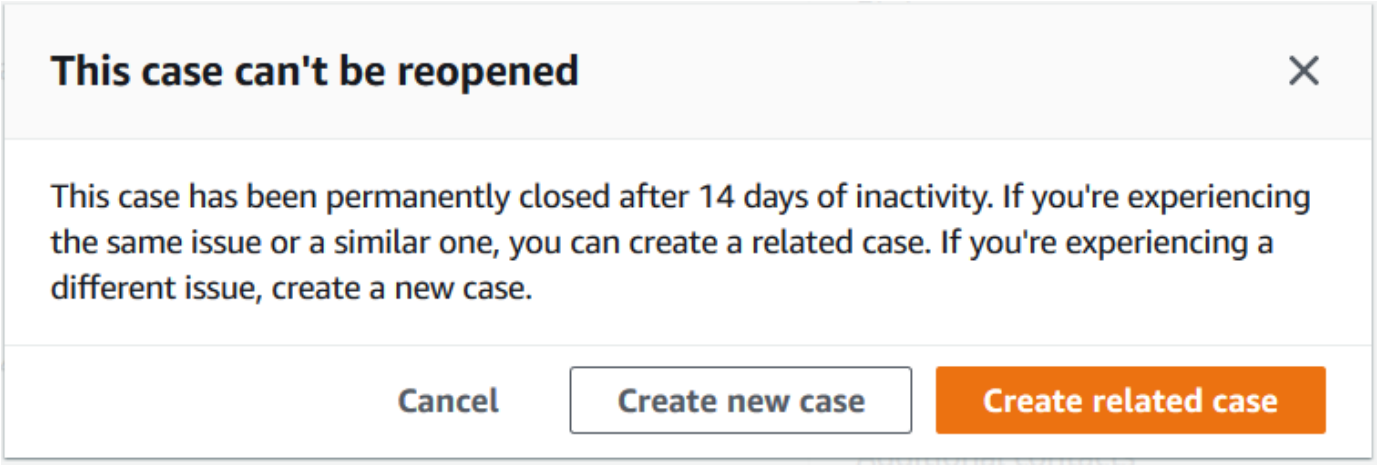
Dopo 14 giorni di inattività, non è possibile riaprire un caso risolto. Se si riscontra un problema simile relativo al caso risolto, è possibile creare un caso correlato. Questo caso correlato includerà un link al caso risolto in precedenza, in modo che l'operatore di supporto possa esaminare i dettagli e le corrispondenze precedenti del caso. Se riscontri un problema diverso, ti suggeriamo di creare un nuovo caso.

Creare un caso correlato

1. Accedere alla AWS Support Center Console.

> **Tip**
>
> Nella AWS Management Console, puoi anche scegliere l'icona del punto interrogativo ( ) e quindi scegli Support Center (Centro assistenza).

2. Seleziona Visualizza tutti i casi, quindi seleziona l'Oggetto o l'ID del caso del caso di supporto che si intende riaprire.
3. Seleziona Riapri il caso.
4. Nella finestra di dialogo, seleziona Crea caso correlato. Le informazioni sul caso precedente verranno aggiunte automaticamente al caso correlato. Se c'è un problema diverso, seleziona Crea un nuovo caso.

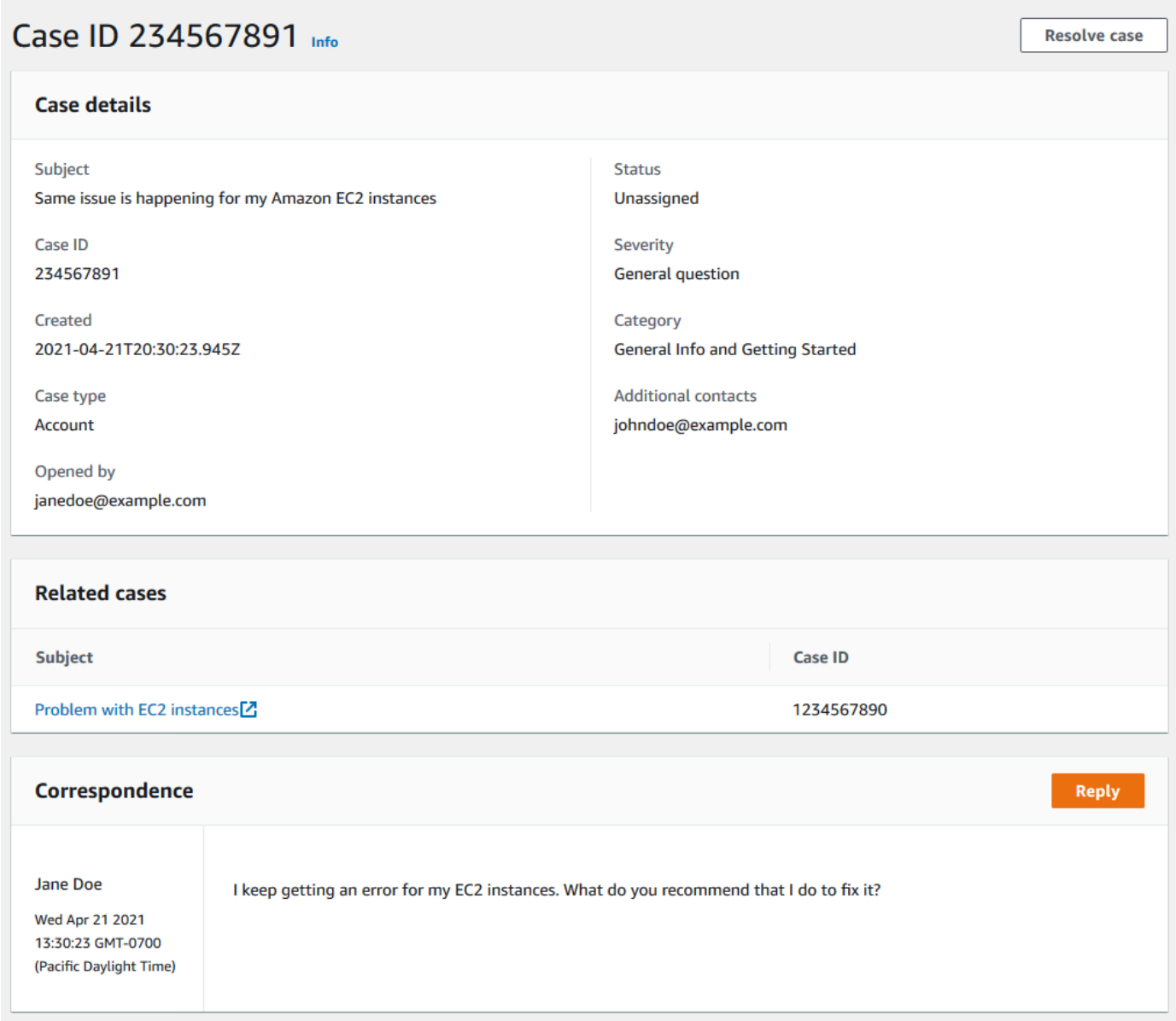


5. Per creare il caso, seguire la stessa procedura. Per informazioni, consultare Creazione di un caso di supporto.

> **Note**
>
> Per impostazione predefinita, il tuo caso correlato ha lo stesso Tipo, Categoria, e Gravità del caso precedente. È possibile aggiornare i dettagli del caso in base alle esigenze.

6. Rivedi i dettagli del caso e seleziona Invia.

Dopo aver creato il caso, il caso precedente viene visualizzato nella sezione Casi correlati, come nell'esempio seguente.



Cronologia dei casi

Puoi visualizzare le informazioni sulla cronologia dei casi fino a 24 mesi dopo la creazione di un caso.

AWS Support raccomandazioni

> **Note**
>
> AWS Support Recommendations viene fornito come «Servizio di anteprima» come definito dai Termini di AWS servizio. Il servizio di anteprima è soggetto a modifiche e cancellazioni. Ulteriori informazioni.

AWS Support Recommendations offre assistenza personalizzata per la risoluzione di problemi tecnici e relativi all'account durante il processo di creazione del caso nella console AWS Support Center. AWS Support Recommendations si basa sui dettagli del caso e sull'account connesso per rispondere con soluzioni personalizzate per risolvere il problema.

Per analizzare i problemi, AWS Support Recommendations richiede informazioni, come AccountID AWS , identificatori di risorse o il messaggio di errore, nell'ambito delle policy approvate e delle autorizzazioni utente. Ulteriori informazioni.

Argomenti

- Gestisci l'accesso ai AWS Support consigli
- Monitoraggio e registrazione dei consigli AWS Support

Gestisci l'accesso ai AWS Support consigli

> **Note**
>
> AWS Support Recommendations viene fornito come «Servizio di anteprima» come definito dai Termini di AWS servizio. Il servizio di anteprima è soggetto a modifiche e cancellazioni. Ulteriori informazioni.

Puoi utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso a AWS Support Recommendations nella console AWS Support Center durante il flusso di creazione del caso.

Argomenti

- AWS Support Consigli e azioni

- Esempi di politiche IAM per Recommendations AWS Support

AWS Support Consigli e azioni

È possibile specificare le azioni AWS Support Recommendations in una policy IAM per fornire l'accesso completo, negare l'accesso completo o fornire/negare l'accesso ad azioni specifiche.

Azione	Descrizione
`StartSupportTroubleshooting`	Avvia una sessione guidata di risoluzione dei problemi per diagnosticare e risolvere problemi tecnici o relativi all'account durante il flusso di creazione dei casi nella console Center. AWS Support
`GetSupportTroubleshootingResponse`	Recupera lo stato e l'output correnti da una sessione di risoluzione dei problemi iniziata con. StartSupportTroubleshooting Include richieste interattive per ulteriori informazioni e consigli per la risoluzione del problema in base alle risposte precedenti.

Esempi di politiche IAM per Recommendations AWS Support

Puoi utilizzare le seguenti politiche di esempio per gestire l'accesso a AWS Support Recommendations.

Accesso completo a AWS Support Recommendations

La seguente politica consente agli utenti l'accesso completo a AWS Support Recommendations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportrecommendations:StartSupportTroubleshooting",
                "supportrecommendations:GetSupportTroubleshootingResponse"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Negare l'accesso a Recommendations AWS Support

La seguente politica non consente agli utenti di accedere a AWS Support Recommendations.

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

Monitoraggio e registrazione dei consigli AWS Support

> **Note**
>
> AWS Support Recommendations viene fornito come «Servizio di anteprima» come definito dai Termini di AWS servizio. Il servizio di anteprima è soggetto a modifiche e cancellazioni. Ulteriori informazioni.

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Support Recommendations e delle altre AWS soluzioni. AWS fornisce il seguente strumento di monitoraggio per guardare AWS Support Recommendations, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon 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 chiamate AWS Support Recommendations con AWS CloudTrail

> **Note**
>
> AWS Support Recommendations viene fornito come «Servizio di anteprima», come definito dai Termini di servizio. AWS Il servizio di anteprima è soggetto a modifiche e cancellazioni. Ulteriori informazioni.

AWS Support Recommendations è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio. CloudTrail acquisisce le chiamate API per AWS Support Recommendations come eventi. Le chiamate acquisite includono chiamate dalla console AWS Support Center e chiamate in codice verso AWS Support Recommendations.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per Recommendations. AWS Support Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a AWS Support Recommendations, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

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

AWS Support Informazioni sui consigli 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 Support Recommendations, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS 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 cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per AWS Support Recommendations, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket

Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS . Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

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

Tutte le chiamate AWS Support Recommendations vengono registrate da CloudTrail. Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

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

Comprensione delle voci dei file di registro di AWS Support Re

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 da un'origine. Include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia dello stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Example : voce di registro per **`StartSupportTroubleshooting`**

L'esempio seguente mostra una voce di CloudTrail registro per l'`StartSupportTroubleshooting`operazione.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "StartSupportTroubleshooting",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "message": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : voce di registro per **`GetSupportTroubleshootingResponse`**

L'esempio seguente mostra una voce di CloudTrail registro per l'`GetSupportTroubleshootingResponse`operazione.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "GetSupportTroubleshootingResponse",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "conversationId": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Utilizzo AWS Support con un AWS SDK

AWS I kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK for C++	AWS SDK for C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK for Go	AWS SDK for Go esempi di codice
AWS SDK for Java	AWS SDK for Java esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK for JavaScript	AWS SDK for JavaScript esempi di codice
SDK AWS for Kotlin	SDK AWS for Kotlin esempi di codice
AWS SDK for .NET	AWS SDK for .NET esempi di codice
AWS SDK for PHP	AWS SDK for PHP esempi di codice
AWS Tools for PowerShell	Strumenti per esempi di PowerShell codice
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) esempi di codice
AWS SDK for Ruby	AWS SDK for Ruby esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS per Swift esempi di codice

Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Informazioni sull'API di AWS Support

L'API AWS Support fornisce l'accesso ad alcune delle funzionalità del Centro di supporto AWS.

L'API offre due diversi gruppi di operazioni:

- operazioni Gestione dei casi di supporto per la gestione dell'intero ciclo di vita dei casi di supporto AWS, dalla creazione di un caso alla sua risoluzione
- operazioni AWS Trusted Advisor per accedere ai controlli AWS Trusted Advisor

> **Note**
>
> È necessario disporre di un piano di supporto Business, Enterprise On-Ramp o Enterprise per utilizzare l'API AWS Support. Per ulteriori informazioni, consulta AWS Support.

Per ulteriori informazioni sulle operazioni e sui tipi di dati forniti da AWS Support, consulta la Documentazione di riferimento API AWS Support.

Argomenti

Gestione dei casi di supporto

Puoi utilizzare l'API per eseguire le attività seguenti:

- Aprire un caso di supporto
- Ottenere un elenco e informazioni dettagliate su casi di supporto recenti
- Filtrare la ricerca di casi di supporto per date e identificatori dei casi, inclusi i casi che sono stati risolti
- Aggiungi comunicazioni e allegati ai casi e aggiungi destinatari alle e-mail per corrispondenze di caso. Puoi allegare fino a tre file. Ogni file può pesare fino a 5 MB

- Risolvere i tuoi casi

L'AWS SupportAPI supporta la CloudTrail registrazione per le operazioni di gestione dei casi di supporto. Per ulteriori informazioni, consulta Registrazione delle chiamate API AWS Support con AWS CloudTrail.

Per alcuni esempi di codici che dimostrano come gestire l'intero ciclo di vita di un caso di supporto, consulta Esempi di codici per AWS Support utilizzando SDK AWS.

AWS Trusted Advisor

Puoi utilizzare le operazioni Trusted Advisor per eseguire le attività seguenti:

- Ottenere nomi e identificatori per i controlli Trusted Advisor
- Richiedere che un controllo Trusted Advisor venga eseguito sul tuo account AWS e sulle tue risorse
- Ottenere riepiloghi e informazioni dettagliate per i risultati del controllo Trusted Advisor
- Aggiornare i controlli Trusted Advisor
- Ottenere lo stato di ogni controllo Trusted Advisor

L'AWS SupportAPI supporta la CloudTrail registrazione delle operazioni. Trusted Advisor Per ulteriori informazioni, consulta Informazioni di AWS Trusted Advisor nella registrazione di CloudTrail.

Puoi utilizzare Amazon CloudWatch Events per monitorare le modifiche ai risultati del controllo diTrusted Advisor. Per ulteriori informazioni, consulta Monitoraggio dei risultati dei AWS Trusted Advisor controlli con Amazon EventBridge.

Per un esempio di codice Java che dimostra come utilizzare le operazioni Trusted Advisor, consulta Utilizzo Trusted Advisor come servizio web.

Endpoints

AWS Support è un servizio globale. Ciò implica che qualunque endpoint utilizzato aggiornerà i tuoi casi di supporto nella console del Centro assistenza.

Ad esempio, se utilizzi l'endopoint Stati Uniti orientali (Virginia settentrionale) per creare un caso, puoi utilizzare l'endpoint Stati Uniti occidentali (Oregon) o Europa (Irlanda) per aggiungere una corrispondenza allo stesso caso.

Puoi utilizzare gli endpoint seguenti per accedere all'API AWS Support:

- Stati Uniti orientali (Virginia settentrionale): https://support.us-east-1.amazonaws.com
- Stati Uniti occidentali (Oregon): https://support.us-west-2.amazonaws.com
- Europa (Irlanda): https://support.eu-west-1.amazonaws.com

> **Important**
>
> - Se chiami l'CreateCaseoperazione per creare casi di supporto ai test, ti consigliamo di includere un oggetto, ad esempio TEST CASE-please ignore. Al termine del test support case, chiama l'ResolveCaseoperazione per risolverlo.
> - Per invocare le operazioni AWS Trusted Advisor nell'API AWS Support, devi utilizzare l'endpoint Stati Uniti orientali (Virginia settentrionale). Attualmente, gli endopoint Stati Uniti occidentali (Oregon) ed Europa (Irlanda) non supportano le operazioni Trusted Advisor.

Per ulteriori informazioni sugli endpoint AWS, consulta la sezione Endpoint e quote di AWS Support nella Riferimenti generali di Amazon Web Services.

Supporto sugli SDK AWS

La AWS Command Line Interface (AWS CLI) e i kit di sviluppo dei software (Software Development Kit, SDK) AWS includono il supporto per l'API AWS Support.

Per un elenco delle lingue che supportano l'AWS SupportAPI, scegli il nome di un'operazione, ad esempio CreateCase, e nella sezione Vedi anche, scegli la tua lingua preferita.

AWS Support Piani

Puoi modificare AWS Support i piani per il tuo account in base alle tue esigenze aziendali.

Argomenti

Caratteristiche dei AWS Support piani

AWS Support offre cinque piani di supporto:

- Base
- Developer
- Business
- Enterprise On-Ramp
- Enterprise

Il piano di supporto Basic offre supporto per domande relative all'account e alla fatturazione, oltre che per l'aumento della quota di servizio. Gli altri piani offrono una serie di casi di supporto tecnico con pay-by-the-month prezzi e senza contratti a lungo termine.

Tutti i AWS clienti hanno automaticamente accesso 24 ore su 24, 7 giorni su 7 a queste funzionalità di Basic Support:

- O ne-on-one risposte alle domande relative all'account e alla fatturazione
- Forum di supporto
- Controlli dello stato del servizio
- Documentazione, documentazione tecnica e guide alle best practice

I clienti che hanno sottoscritto un piano di supporto Developer hanno accesso alle seguenti caratteristiche aggiuntive:

- Guida alle best practice

- Strumenti di diagnostica dal lato del cliente
- Supporto per l'architettura a blocchi: linee guida su come utilizzare insieme AWS prodotti, funzionalità e servizi
- Supporta un numero illimitato di casi di supporto che possono essere aperti da qualsiasi utente con autorizzazioni.

Inoltre, i clienti che hanno sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise hanno accesso alle seguenti caratteristiche aggiuntive:

- Guida ai casi d'uso: quali AWS prodotti, funzionalità e servizi utilizzare per soddisfare al meglio le tue esigenze specifiche.
- AWS Trusted Advisor— Una funzionalità di AWS Support, che ispeziona gli ambienti dei clienti e identifica le opportunità per risparmiare denaro, colmare le lacune di sicurezza e migliorare l'affidabilità e le prestazioni del sistema. Puoi accedere a tutti i controlli. Trusted Advisor
- L' AWS Support API per interagire con Support Center e Trusted Advisor. È possibile utilizzare l'API AWS Support per automatizzare la gestione dei casi di supporto e le operazioni Trusted Advisor .
- Supporto per software di terze parti – guida per la configurazione e i sistemi operativi dell'istanza Amazon Elastic Compute Cloud (Amazon EC2). Inoltre, aiuta a migliorare le prestazioni dei componenti software di terze parti più diffusi su AWS. Il supporto per il software di terze parti non è disponibile per i clienti con piani di supporto Basic o Developer.
- Supporta un numero illimitato di utenti AWS Identity and Access Management (IAM) che possono aprire casi di supporto tecnico.

Inoltre, i clienti che hanno sottoscritto un piano di supporto Enterprise On-Ramp o Enterprise hanno accesso alle seguenti caratteristiche aggiuntive:

- Linee guida per l'architettura dell'applicazione – Linee guida consultive sull'uso dei servizi in sinergia, in base a casi d'uso, applicazioni o carichi di lavoro specifici.
- Gestione degli eventi dell'infrastruttura – Impegno a breve temine con AWS Support per ottenere informazioni dettagliate del caso d'uso. Dopo l'analisi, fornisci le indicazioni sull'architettura e sul dimensionamento per un evento.
- Technical account manager – Lavora con un technical account manager (TAM) per applicazioni e casi d'uso specifici.
- Trattamento su misura dei casi.

- Analisi delle attività di gestione.

Per ulteriori informazioni sulle funzionalità e sui prezzi di ciascun piano di supporto, consulta AWS Supporte Confronta AWS Support i piani. Alcune funzionalità, ad esempio il supporto telefonico 24 ore su 24, 7 giorni su 7 e il supporto tramite chat, non sono disponibili in tutte le lingue.

Modifica AWS Support dei piani

Puoi utilizzare la console AWS Support Plans per modificare il piano di supporto per i tuoi Account AWS. Per modificare il piano di supporto, devi disporre delle autorizzazioni AWS Identity and Access Management (IAM) o accedere al tuo account come utente root. Per ulteriori informazioni, consulta Gestisci l'accesso ai piani AWS Support e AWS politiche gestite per AWS Support Plans.

Per modificare il piano di supporto

1. Accedi alla console AWS Support Plans all'indirizzo https://console.aws.amazon.com/support/plans/home.
2. (Facoltativo) Nella pagina Piani di AWS Support , confronta i piani di supporto. Per ulteriori informazioni sui prezzi, consulta la pagina Dettagli dei prezzi.
3. (Facoltativo) In Esempio di prezzi di AWS Support , scegli Vedi gli esempi, quindi seleziona una delle opzioni del piano di supporto per visualizzare il costo stimato.
4. Una volta che hai deciso quale piano desideri, scegli Review downgrade (Esamina il downgrade) o Review upgrade (Esamina l'upgrade) per il piano desiderato.

   > **Note**
   >
   > - Se ti iscrivi a un piano di supporto a pagamento, sarai vincolato con un abbonamento a AWS Support per un minimo di un mese. Per ulteriori informazioni, consulta le domande frequenti su AWS Support.
   > - Se hai un piano di supporto Enterprise On-Ramp o Enterprise, nella finestra di dialogo Change plan confirmation (Conferma della modifica del piano), contatta AWS Support per modificare il piano di supporto.

5. Nella finestra di dialogo Change plan confirmation (Conferma della modifica del piano), puoi espandere gli elementi di supporto per visualizzare le funzionalità che desideri aggiungere o rimuovere dal tuo account.

In Pricing (Prezzi), puoi visualizzare i costi una tantum previsti per il nuovo piano di supporto.

6. Scegli Accept and agree (Conferma e accetta).

Informazioni correlate

Per ulteriori informazioni sui AWS Support piani, consulta le AWS Support domande frequenti. Inoltre, è possibile scegliere Contact us (Contattaci) dalla console dei piani di supporto.

Per chiudere l'account, consulta la sezione Chiusura dell'account nella AWS Billing Guida per l'utente.

AWS Trusted Advisor

Trusted Advisor si basa sulle migliori pratiche apprese servendo centinaia di migliaia di AWS clienti. Trusted Advisor ispeziona l' AWS ambiente e quindi formula raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza.

Se disponi di un piano Basic o Developer Support, puoi utilizzare la Trusted Advisor console per accedere a tutti i controlli nella categoria Service Limits e a sei controlli nella categoria Security.

Se disponi di un piano Business, Enterprise On-Ramp o Enterprise Support, puoi utilizzare la Trusted Advisor console e l'AWS Trusted Advisor API per accedere a tutti i Trusted Advisor controlli. Puoi anche utilizzare Amazon CloudWatch Events per monitorare lo stato dei Trusted Advisor controlli. Per ulteriori informazioni, consulta Monitoraggio dei risultati dei AWS Trusted Advisor controlli con Amazon EventBridge.

Puoi accedere Trusted Advisor in AWS Management Console. Per ulteriori informazioni sul controllo dell'accesso alla Trusted Advisor console, vedereGestisci l'accesso a AWS Trusted Advisor.

Per ulteriori informazioni, consulta Trusted Advisor.

Argomenti

Come iniziare con Consigli per Trusted Advisor

Puoi utilizzare la pagina Trusted Advisor Consigli della Trusted Advisor console per esaminare i risultati dei controlli relativi al tuo computer Account AWS e quindi seguire i passaggi consigliati per risolvere eventuali problemi. Ad esempio: Trusted Advisor suggerisce di eliminare le risorse non utilizzate per ridurre la fattura mensile, come un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

Puoi anche utilizzare l' AWS Trusted Advisor API per eseguire operazioni sui tuoi Trusted Advisor controlli. Per ulteriori informazioni, consulta l'AWS Trusted Advisor API Reference

Argomenti

Accedi alla Trusted Advisor console

Puoi visualizzare i controlli e lo stato di ogni controllo nella Trusted Advisor console.

> **Note**
>
> È necessario disporre delle autorizzazioni AWS Identity and Access Management (IAM) per accedere alla Trusted Advisor console. Per ulteriori informazioni, consulta Gestisci l'accesso a AWS Trusted Advisor.

Per accedere alla console Trusted Advisor

1. Accedere alla Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.

2. Nella pagina Consigli per Trusted Advisor , visualizza il riepilogo per ogni categoria di controllo:

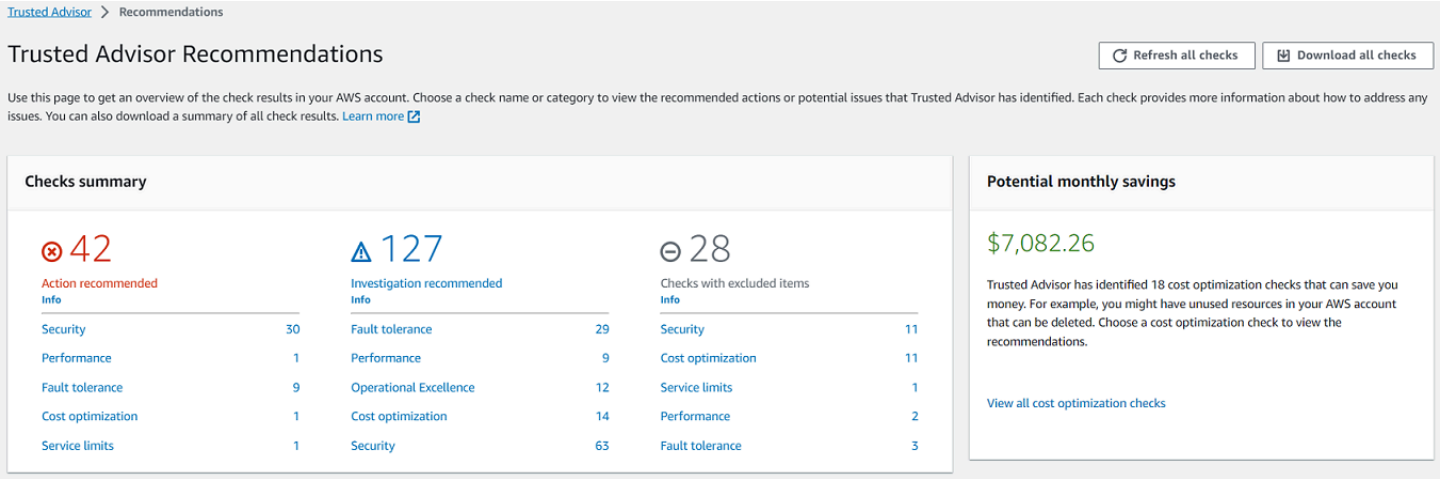
   - Azione consigliata (rosso): Trusted Advisor consiglia un'azione per il controllo. Ad esempio, un controllo che rileva un problema di sicurezza per le risorse IAM potrebbe suggerire di effettuare passaggi urgenti.
   - Indagine suggerita (giallo) – Trusted Advisor rileva un possibile problema per il controllo. Ad esempio, un controllo che raggiunge una quota per una risorsa potrebbe consigliare modi per eliminare le risorse inutilizzate.
   - Checks with excluded items (gray) (Controlli con elementi esclusi (grigio): il numero di controlli con elementi esclusi, ad esempio risorse che devono essere ignorate da un controllo. Ad esempio, potrebbe trattarsi di istanze Amazon EC2 che non si desidera sottoporre al controllo.

3. Puoi effettuare le operazioni seguenti nella pagina Consigli per Trusted Advisor :

   - Per aggiornare tutti i controlli nel tuo account, scegli Aggiorna tutti i controlli.
   - Per creare un file .xls che include tutti i risultati del controllo, seleziona Scarica tutti i controlli.
   - Alla voce Checks summary (Riepilogo controlli), seleziona una categoria di controllo, ad esempio Security (Sicurezza) per visualizzare i risultati.
   - Alla voce Potential monthly savings (Possibili risparmi mensili) è possibile visualizzare quanto è possibile risparmiare per il proprio account e i controlli di ottimizzazione dei costi per i suggerimenti.
   - Alla voce Modifiche recenti è possibile visualizzare le modifiche per controllare gli stati negli ultimi 30 giorni. Scegli un nome di controllo per visualizzare i risultati più recenti per tale controllo o seleziona l'icona a forma di freccia per visualizzare la pagina successiva.

Example : Trusted Advisor Raccomandazioni

L'esempio seguente mostra un riepilogo dei risultati del controllo per un Account AWS.



Visualizza le categorie di controllo

È possibile visualizzare le descrizioni dei controlli e i risultati delle seguenti categorie di controllo:

- Ottimizzazione dei costi – Suggerimenti per ottenere potenziali risparmi. Questi controlli evidenziano le risorse inutilizzate e le opportunità per ridurre la fattura.
- Prestazioni – Suggerimenti che consentono di migliorare la velocità e la reattività delle applicazioni.
- Sicurezza: consigli per le impostazioni di sicurezza che possono rendere la AWS soluzione più sicura.
- Tolleranza ai guasti: raccomandazioni che aiutano ad aumentare la resilienza della AWS soluzione. Questi controlli evidenziano le carenze in termini di ridondanza e l'utilizzo eccessivo delle risorse.
- Limiti del servizio – Controlla l'utilizzo del tuo account e verifica se il tuo account si avvicina o supera il limite (noto anche come quote) per i servizi e le risorse AWS .
- Eccellenza operativa: raccomandazioni per aiutarvi a gestire AWS l'ambiente in modo efficace e su larga scala.

Per visualizzare le categorie di controllo

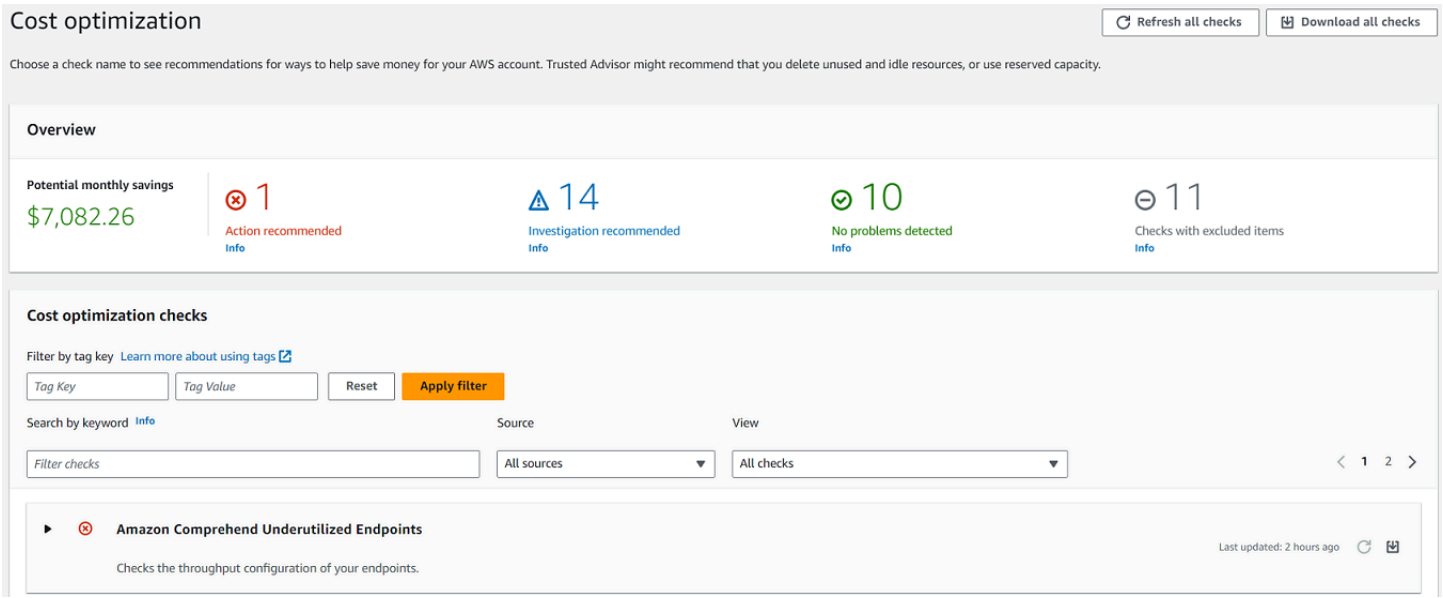
1. Accedi alla Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nel pannello di navigazione, scegli la categoria di controllo.
3. Nella pagina della categoria, visualizza il riepilogo per ogni categoria di controllo:
   - Azione consigliata (rosso): Trusted Advisor consiglia un'azione per il controllo.
   - Indagine suggerita (giallo) – Trusted Advisor rileva un possibile problema per il controllo.

- Nessun problema rilevato (verde): Trusted Advisor non rileva alcun problema per il controllo.
- Elementi esclusi (grigio) – Il numero di controlli che hanno escluso degli elementi, come ad esempio delle risorse che non si desidera sottoporre a un controllo.

4. Per ogni controllo, seleziona l'icona di aggiornamento
   ( )
   per aggiornare questo controllo.
5. Scegli l'icona di download
   ( )
   per creare un file .xls che includa i risultati di questo controllo.

Example : Categoria Ottimizzazione dei costi

L'esempio seguente mostra 10 controlli (verdi) che non presentano problemi.



Visualizza controlli specifici

Espandi un controllo per visualizzare la descrizione completa del controllo, le risorse interessate, i passaggi consigliati e i collegamenti a ulteriori informazioni.

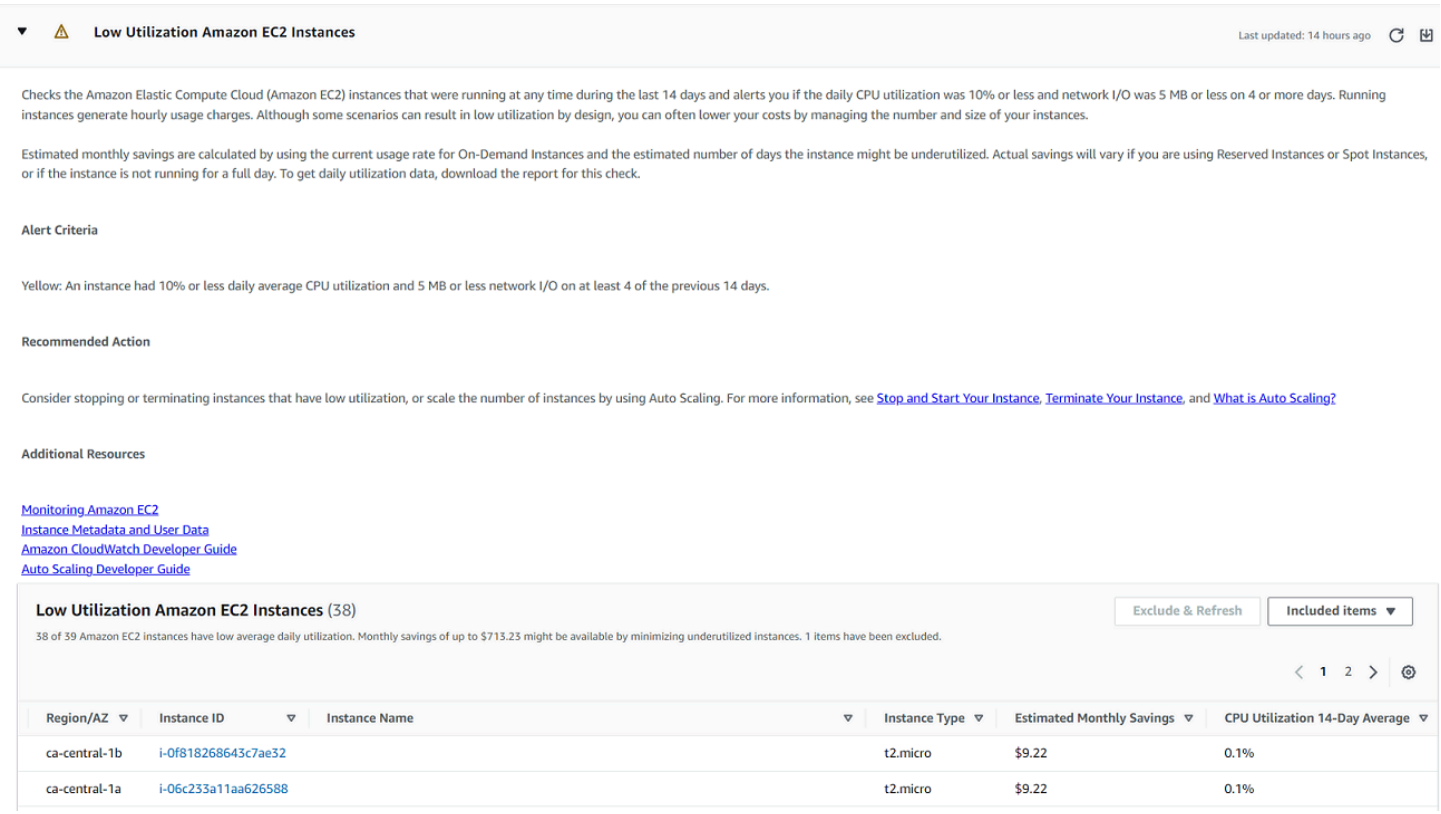
Per visualizzare un controllo specifico

1. Accedi alla Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.

2. Nel pannello di navigazione, seleziona una categoria di controllo.
3. Scegli il nome del controllo per visualizzare la descrizione e i seguenti dettagli:
   - Criteri di avviso – Descrive la soglia oltre cui un controllo cambierà lo stato.
   - Operazione consigliata – Descrive le azioni consigliate per questo controllo.
   - Risorse aggiuntive – Elenca la documentazione AWS correlata.
   - Tabella che elenca gli elementi interessati nell'account. È possibile includere o escludere questi elementi dai risultati del controllo.
4. (Facoltativo) Per escludere gli elementi in modo che non vengano visualizzati nei risultati del controllo:
   a. Seleziona un elemento e scegli Escludi e aggiorna.
   b. Per visualizzare tutti gli elementi esclusi, seleziona Elementi esclusi.
5. (Facoltativo) Per includere gli elementi in modo che il controllo li valuti nuovamente:
   a. Seleziona Elementi esclusi, seleziona un elemento, quindi scegli Includi e Aggiorna.
   b. Per visualizzare tutti gli elementi inclusi, seleziona Elementi inclusi.
6. Seleziona l'icona relativa alle impostazioni
   ().
   Nella finestra di dialogo Preferences (Preferenze) puoi specificare il numero di elementi o le proprietà da visualizzare, quindi scegli Confirm (Conferma).

Example : Controllo Ottimizzazione dei costi

Il seguente controllo Istanze Amazon EC2 con utilizzo ridotto elenca le istanze interessate nell'account. Questo controllo individua 38 istanze Amazon EC2 che hanno un utilizzo ridotto e consiglia di interrompere o terminare le risorse.



Filtra i controlli

Nelle pagine delle categorie di controllo è possibile specificare i risultati del controllo che desideri visualizzare. Ad esempio, puoi filtrare in base ai controlli che hanno rilevato errori nel tuo account, in modo da poter esaminare prima i problemi urgenti.

Se disponi di controlli che valutano gli elementi presenti nel tuo account, ad esempio le AWS risorse, puoi utilizzare i filtri per i tag per mostrare solo gli elementi che hanno il tag specificato.

Per filtrare i controlli

1. Accedi alla Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nel riquadro di navigazione o nella pagina Consigli per Trusted Advisor , scegli la categoria di controllo.
3. Per Ricerca per parola chiave, inserisci una parola chiave dal nome o dalla descrizione del controllo per filtrare i risultati.
4. Per la lista Visualizzazione, specifica quali controlli visualizzare:

   - All checks (Tutti i controlli): elenca tutti i controlli per questa categoria.

- Operazione consigliata – Elenca i controlli che consigliano di intraprendere un'azione. Questi controlli sono evidenziati in rosso.
- Indagine consigliata – Elenca i controlli che consigliano di eseguire un'azione. Questi controlli sono evidenziati in giallo.
- Nessun problema rilevato – Elenca i controlli che non presentano problemi. Questi controlli sono evidenziati in verde.
- Controlli con elementi esclusi – Elenca i controlli specificati per escludere gli elementi dai risultati del controllo.

5. Se hai aggiunto tag alle tue AWS risorse, come istanze o AWS CloudTrail trail di Amazon EC2, puoi filtrare i risultati in modo che i controlli mostrino solo gli elementi con il tag specificato.

   Per Filtrare per tag, inserisci una chiave e un valore di tag, quindi scegli Applica filtro.
6. Nella tabella per il controllo, i risultati del controllo mostrano solo gli elementi con la chiave e il valore specificati.
7. Per cancellare il filtro in base ai tag, seleziona Reimposta.

Informazioni correlate

Per ulteriori informazioni sull'etichettatura per Trusted Advisor, consulta i seguenti argomenti:

- AWS Support abilita le funzionalità di etichettatura per Trusted Advisor
- Tagging delle risorse in AWS nella Riferimenti generali di AWS

Aggiorna i risultati di controllo

Puoi aggiornare i controlli per ottenere i risultati più recenti per il tuo account. Se hai un piano Developer o Basic Support, puoi accedere alla Trusted Advisor console per aggiornare i controlli. Se hai un piano Business, Enterprise On-Ramp o Enterprise Support, aggiorna Trusted Advisor automaticamente gli assegni nel tuo account su base settimanale.

Per aggiornare i controlli Trusted Advisor

1. Accedi alla AWS Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor.
2. Nella pagina Trusted Advisor Consigli o nella categoria di controlli, scegli Aggiorna tutti i controlli.

È inoltre possibile aggiornare controlli specifici nei modi seguenti:

- Seleziona l'icona di aggiornamento
  ()
  per un controllo individuale.
- Usa l'operazione API RefreshTrustedAdvisorCheck.

> **Note**
>
> - Trusted Advisor aggiorna automaticamente alcuni controlli più volte al giorno, ad esempio i problemi AWS Well-Architected ad alto rischio per il controllo dell'affidabilità. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate nell'account. Per questi controlli aggiornati automaticamente, non puoi scegliere l'icona di aggiornamento
>   ()
>   per aggiornare manualmente i risultati.
> - Se hai abilitato AWS Security Hub il tuo account, non puoi usare la Trusted Advisor console per aggiornare i controlli del Security Hub. Per ulteriori informazioni, consulta Aggiorna i risultati del Security Hub.

Scarica i risultati del controllo

Puoi scaricare i risultati dei controlli per avere una panoramica del Trusted Advisor tuo account. È possibile scaricare i risultati di tutti i controlli o di un controllo specifico.

Per scaricare i risultati dei controlli da Trusted Advisor Recommendations

1. Accedi alla AWS Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor.
   - Per scaricare tutti i risultati dei controlli, nella pagina Consigli per Trusted Advisor o nella pagina di una categoria di controllo, scegli Scarica tutti i controlli.
   - Per scaricare un risultato di controllo per un controllo specifico, seleziona il nome del controllo, poi seleziona l'icona di download
     ().

2. Salva o apri il file .xls. Il file contiene le stesse informazioni di riepilogo della console Trusted Advisor , ad esempio il nome del controllo, la descrizione, lo stato, le risorse interessate e così via.

Visualizzazione organizzativa

Puoi configurare la funzionalità di visualizzazione organizzativa per creare un rapporto per tutti gli account membri AWS dell'organizzazione. Per ulteriori informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor.

Preferenze

Nella pagina Gestisci Trusted Advisor, puoi disabilitare Trusted Advisor.

Sulla pagina delle Notifiche, è possibile configurare i messaggi e-mail settimanali per il riepilogo delle verifiche. Per informazioni, consulta Configura le preferenze di notifica.

Nella pagina La tua organizzazione, puoi abilitare o disabilitare l'accesso affidabile con AWS Organizations. Ciò è necessario per la funzionalità Visualizzazione organizzativa per AWS Trusted Advisor, Trusted Advisor Priority e Trusted Advisor Engage.

Configura le preferenze di notifica

Specificate chi può ricevere i messaggi Trusted Advisor e-mail settimanali per i risultati dei controlli e la lingua. Riceverai una notifica via e-mail relativa al riepilogo dei controlli relativi a Trusted Advisor Recommendations una volta alla settimana.

Le notifiche e-mail per Trusted Advisor Recommendations non includono i risultati per Trusted Advisor Priority. Per ulteriori informazioni, consulta Gestione delle notifiche di Trusted Advisor Priority.

Configura le preferenze di notifica

1. Accedi alla Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nel riquadro di navigazione, in Preferences (Preferenze) scegli Notifications (Notifiche).
3. Per Recommendations (Suggerimenti), seleziona i destinatari della notifica per i risultati del controllo. Puoi aggiungere e rimuovere contatti dalla pagina Impostazioni account della AWS Billing and Cost Management console.

4. Per la Lingua, seleziona la lingua del messaggio di posta elettronica.
5. Scegli Save your preferences (Salva preferenze).

Configura la visualizzazione organizzativa

Se configuri il tuo account con AWS Organizations, puoi creare report per tutti gli account dei membri della tua organizzazione. Per ulteriori informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor.

Disabilita Trusted Advisor

Quando disabiliti questo servizio, Trusted Advisor non eseguirà alcun controllo sul tuo account. Chiunque tenti di accedere alla Trusted Advisor console o utilizzare le operazioni API riceverà un messaggio di errore di accesso negato.

Per disabilitare Trusted Advisor

1. Accedi alla Trusted Advisor console all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nel riquadro di navigazione, in Preferenze, scegli Gestisci Trusted Advisor.
3. In Trusted Advisor, disattiva Enabled (Abilitato). Questa azione disabilita tutti Trusted Advisor i controlli sul tuo account.
4. Puoi quindi eliminare manualmente il dal tuo account. Per ulteriori informazioni, consulta Eliminazione di un ruolo collegato ai servizi per Trusted Advisor.

Informazioni correlate

Per ulteriori informazioni su Trusted Advisor, consulta i seguenti argomenti:

- Come posso iniziare a usare Trusted Advisor?
- AWS Trusted Advisor verifica riferimento

Inizia a usare l' Trusted Advisor API

L' AWS Trusted Advisor API Reference è destinato ai programmatori che necessitano di informazioni dettagliate sulle operazioni dell' Trusted Advisor API e sui tipi di dati. Questa API fornisce l'accesso

ai Trusted Advisor consigli per il tuo account o per tutti gli account all'interno della tua AWS organizzazione. L' Trusted Advisor API utilizza metodi HTTP che restituiscono risultati in formato JSON.

> **Note**
>
> - È necessario disporre di un piano Business, Enterprise On-Ramp o Enterprise Support per utilizzare l'API Trusted Advisor
> - Se chiami l' AWS Trusted Advisor API da un account che non dispone di un piano Business, Enterprise On-Ramp o Enterprise Support, ricevi un'eccezione Access Denied. Per ulteriori informazioni sulla modifica del piano di supporto, consulta AWS Support.

Puoi utilizzare l' AWS Trusted Advisor API per ottenere un elenco di controlli e le relative descrizioni, consigli e risorse per i consigli. Puoi anche aggiornare il ciclo di vita dei consigli. Per gestire i consigli, utilizza le seguenti operazioni API:

- Utilizza le operazioni ListChecksListRecommendations, GetRecommendation, e ListRecommendationResourcesAPI per visualizzare i consigli e gli account e le risorse corrispondenti.
- Utilizza l'operazione UpdateRecommendationLifecycleAPI per aggiornare il ciclo di vita di una raccomandazione gestita da Trusted Advisor Priority.
- Utilizza l'operazione BatchUpdateRecommendationResourceExclusionAPI per includere o escludere una o più risorse dai risultati. Trusted Advisor
- Le chiamate ListOrganizationRecommendationsGetOrganizationRecommendation, ListOrganizationRecommendationResources, ListOrganizationRecommendationAccounts, e UpdateOrganizationRecommendationLifecycleAPI supportano solo i consigli gestiti da Trusted Advisor Priority. Queste raccomandazioni vengono anche chiamate raccomandazioni prioritarie. Puoi visualizzare e gestire i consigli con priorità da un account di gestione o amministratore delegato se hai attivato Trusted Advisor Priority. Se Priority non è attivata, riceverai un'eccezione di accesso negato quando effettui delle richieste.

Per ulteriori informazioni, consulta AWS Trusted Advisor la AWS Support User Guide.

Per l'autenticazione delle richieste, consulta il processo di firma della versione 4 di Signature.

Utilizzo Trusted Advisor come servizio web

> **Note**
>
> Trusted Advisor le operazioni non saranno supportate dall'API AWS Trusted Advisor Support nel 2024. Utilizza la nuova AWS Trusted Advisor API per accedere in modo programmatico ai controlli e ai consigli sulle migliori pratiche.

Il AWS Support servizio consente di scrivere applicazioni che interagiscono con. AWS Trusted Advisor In questo argomento viene illustrato come ottenere un elenco di Trusted Advisor controlli, aggiornarne uno e quindi ottenere i risultati dettagliati del controllo. Queste attività sono illustrate in Java. Per informazioni sul supporto di altre lingue, consulta la pagina relativa agli strumenti per Amazon Web Services.

Argomenti

Visualizza l'elenco dei controlli disponibili Trusted Advisor

Il seguente frammento di codice Java crea un'istanza di un AWS Support client che puoi utilizzare per chiamare tutte le operazioni Trusted Advisor API. Successivamente, il codice ottiene l'elenco dei Trusted Advisor controlli e i `CheckId` valori corrispondenti chiamando l'operazione DescribeTrustedAdvisorChecksAPI. Puoi utilizzare queste informazioni per creare interfacce utente che consentano agli utenti di selezionare il controllo che desiderano eseguire o aggiornare.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
```

```
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

Aggiorna l'elenco dei controlli disponibili Trusted Advisor

Il seguente frammento di codice Java crea un'istanza di un AWS Support client che è possibile utilizzare per aggiornare i dati. Trusted Advisor

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

Esegui un Trusted Advisor sondaggio per verificare le modifiche allo stato

Dopo aver inviato la richiesta di eseguire un Trusted Advisor controllo per generare i dati di stato più recenti, si utilizza l'operazione DescribeTrustedAdvisorCheckRefreshStatusesAPI per richiedere lo stato di avanzamento dell'esecuzione del controllo e quando i nuovi dati sono pronti per il controllo.

Il seguente frammento di codice Java ottiene lo stato del controllo richiesto nella sezione seguente utilizzando il valore corrispondente nella variabile `CheckId`. Inoltre, il codice illustra diversi altri usi del Trusted Advisor servizio:

1. Puoi richiamare `getMillisUntilNextRefreshable` ricorrendo agli oggetti contenuti nell'istanza `DescribeTrustedAdvisorCheckRefreshStatusesResult`. Puoi utilizzare il valore restituito per verificare se desideri che il codice esegua l'aggiornamento del controllo.
2. Se `timeUntilRefreshable` è uguale a zero, puoi richiedere l'aggiornamento del controllo.
3. Utilizzando lo stato restituito, puoi continuare a sollecitare cambiamenti di stato; il frammento di codice imposta l'intervallo di polling sul valore consigliato di dieci secondi. Se lo stato è `enqueued` o `in_progress`, il ciclo ricomincia e viene richiesto un altro stato. Se la chiamata restituisce `successful`, il ciclo viene terminato.
4. Infine, il codice restituisce un'istanza di un tipo di dati `DescribeTrustedAdvisorCheckResultResult` che puoi utilizzare per ricorrere alle informazioni prodotte per il controllo.

Note: utilizza una richiesta di aggiornamento singola prima di eseguire il polling dello stato della richiesta.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
```

```
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Richiedi il risultato di un Trusted Advisor controllo

Dopo aver selezionato il controllo per i risultati dettagliati che desideri, invii una richiesta utilizzando l'operazione DescribeTrustedAdvisorCheckResult API.

> **Tip**
>
> I nomi e le descrizioni Trusted Advisor dei controlli sono soggetti a modifiche. Si consiglia di specificare l'ID del controllo nel codice per identificare in modo univoco un controllo. È possibile utilizzare l'operazione DescribeTrustedAdvisorChecksAPI per ottenere l'ID dell'assegno.

Il seguente frammento di codice Java utilizza l'istanza `DescribeTrustedAdvisorChecksResult` a cui fa riferimento la variabile `result`, ottenuta nel precedente frammento di codice. Anziché definire un controllo in modo interattivo mediante un'interfaccia utente, dopo aver inviato al richiesta di esecuzione, il frammento invia semplicemente una richiesta di esecuzione per il primo check nell'elenco specificando un valore di indice 0 in ciascuna chiamata `result.getChecks().get(0)`. Quindi, il codice definisce un'istanza di `DescribeTrustedAdvisorCheckResultRequest`, che trasferisce a un'istanza di `DescribeTrustedAdvisorCheckResultResult` chiamata `checkResult`. Puoi utilizzare le strutture del membro di questo tipo di dati per visualizzare i risultati del controllo.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

Nota: la richiesta di un risultato del Trusted Advisor controllo non genera dati aggiornati sui risultati.

Mostra i dettagli di un controllo Trusted Advisor

Il seguente frammento di codice Java esegue un'iterazione sull'`DescribeTrustedAdvisorCheckResultResult`istanza restituita nella sezione precedente per ottenere un elenco di risorse contrassegnate dal controllo. Trusted Advisor

```
// Show ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

Visualizzazione organizzativa per AWS Trusted Advisor

La visualizzazione organizzativa consente di visualizzare i controlli Trusted Advisor per gli account nell'AWS Organizations. Dopo aver attivato questa funzionalità, è possibile creare report per aggregare i risultati dei controlli per tutti gli account membri dell'organizzazione. Il report include un riepilogo dei risultati dei controlli e informazioni sulle risorse interessate per ciascun account. Ad esempio, è possibile utilizzare i report per identificare gli account dell'organizzazione che utilizzano AWS Identity and Access Management (IAM) con il controllo IAM Utilizza o se hai consigliato azioni per i bucket Amazon Simple Storage Service (Amazon S3) con il controllo Autorizzazioni Bucket Amazon S3.

Argomenti

Prerequisiti

È necessario soddisfare i seguenti requisiti per abilitare la visualizzazione organizzativa:

- L'account deve essere un membro di un'Organizzazione AWS.
- L'organizzazione deve avere tutte le caratteristiche abilitate per Organizations. Per ulteriori informazioni, consulta la sezione Abilitazione di tutte le caratteristiche nell'organizzazione nella Guida per l'utente di AWS Organizations.
- L'account di gestione nell'organizzazione deve disporre di un piano di supporto Business, Enterprise On-Ramp o Enterprise. Puoi trovare il tuo piano di supporto dal Centro AWS Support o dalla pagina Piani di supporto. Consulta la sezione Confronta piani AWS Support.
- È necessario accedere come utente nell'account di gestione (o nel ruolo utilizzato equivalente). Che si acceda come utente IAM o come ruolo IAM, è comunque necessario disporre di una policy con le autorizzazioni richieste. Per informazioni, consultare Utilizzo delle policy IAM per consentire l'accesso alla visualizzazione organizzativa.

Abilita visualizzazione organizzativa

Dopo aver soddisfatto i prerequisiti, attieniti alla procedura seguente per abilitare la visualizzazione organizzativa. Dopo aver abilitato questa funzionalità, si verifica quanto segue:

- Trusted Advisor viene abilitato come servizio sicuro nell'organizzazione. Per ulteriori informazioni, consulta Abilitazione di un accesso sicuro con altri servizi AWS nella Guida per l'utente di AWS Organizations.
- Il ruolo collegato al servizio `AWSServiceRoleForTrustedAdvisorReporting` viene creato automaticamente nell'account di gestione dell'organizzazione. Questo ruolo include le autorizzazioni di cui Trusted Advisor necessita per richiamare Organizations per tuo conto. Questo ruolo collegato al servizio è bloccato e non è possibile eliminarlo manualmente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Trusted Advisor.

È possibile abilitare la visualizzazione organizzativa dalla console Trusted Advisor.

Per abilitare la visualizzazione organizzativa

1. Accedi come amministratore nell'account di gestione dell'organizzazione e apri la console AWS Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor.

2. Nel riquadro di navigazione, in Preferences (Preferenze), scegli Your organization (La tua organizzazione).
3. In Enable trusted access with AWS Organizations (Abilita accesso sicuro con), attiva Enabled (Abilitato).

> **Note**
>
> L'abilitazione della visualizzazione organizzativa per l'account di gestione non fornisce gli stessi controlli per tutti gli account membri. Ad esempio, se i tuoi account membri dispongono del Supporto base, questi account non avranno gli stessi controlli disponibili per il tuo account di gestione. Il piano AWS Support determina quali Trusted Advisor controlli sono disponibili per un account.

Aggiorna i controlli Trusted Advisor

Prima di creare un report per la tua organizzazione, è consigliabile aggiornare gli stati dei controlli Trusted Advisor. È possibile scaricare un report senza aggiornare i controlli Trusted Advisor, ma potrebbe non contenere le informazioni più recenti.

Se disponi di un piano di supporto Business, Enterprise On-Ramp o Enterprise, Trusted Advisor aggiorna in automatico i controlli nel tuo account settimanalmente.

> **Note**
>
> Se nell'organizzazione sono presenti account che dispongono di un piano di supporto Developer o Basic, è necessario che un utente per questi account acceda alla console Trusted Advisor per aggiornare i controlli. Non è possibile aggiornare i controlli per tutti gli account dall'account di gestione dell'organizzazione.

Per aggiornare i controlli Trusted Advisor

1. Passa alla console AWS Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor.
2. Nella pagina Suggerimenti per Trusted Advisor, seleziona Aggiorna tutti i controlli. In questo modo vengono aggiornati tutti i controlli nell'account.

È inoltre possibile aggiornare i controlli specifici nei modi seguenti:

- Utilizza l'operazione API RefreshTrustedAdvisorCheck.
- Scegli l'icona di aggiornamento
  ( )
  per un controllo individuale.

Creazione di report di visualizzazione organizzativa

Dopo aver abilitato la visualizzazione organizzativa, è possibile creare report in modo da poter visualizzare i risultati dei controlli Trusted Advisor per l'organizzazione.

Puoi creare fino a 50 report. Se si creano report oltre questa quota, Trusted Advisor elimina il report più datato. Non è possibile recuperare i report eliminati.

Per creare report di visualizzazione organizzativa

1. Accedi all'account di gestione dell'organizzazione e apri la console AWS Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor.
2. Nel riquadro di navigazione, seleziona Visualizzazione organizzativa.
3. Selezionare Create report (Crea report).
4. Per impostazione predefinita, il report include tutti gli stati delle Regioni, delle categorie di controllo e delle risorse AWS. Nella pagina Creazione di report puoi utilizzare le opzioni di filtro per personalizzare il report. Ad esempio, è possibile deselezionare l'opzione Tutte per Regione e specificare le singole Regioni da includere nel report.
   a. Inserisci un Nome per il report.
   b. Per l'opzione Formato, scegli JSON o CSV.
   c. Per l'opzione Regione, specifica le Regioni AWS o seleziona Tutte.
   d. Per l'opzione Categoria di controllo, seleziona la categoria di controllo o scegli Tutte.
   e. Per l'opzione Controlli, seleziona i controlli specifici per quella categoria o scegli Tutti.

> **Note**
>
> Il filtro Categoria di controllo sovrascrive il filtro Controlli. Ad esempio, selezionando la categoria Sicurezza e quindi selezionando un nome di controllo specifico, il report

include tutti i risultati del controllo per tale categoria. Per creare un report solo per controlli specifici, mantieni il valore predefinito Tutti per la Categoria di controllo e scegli i nomi dei controlli.

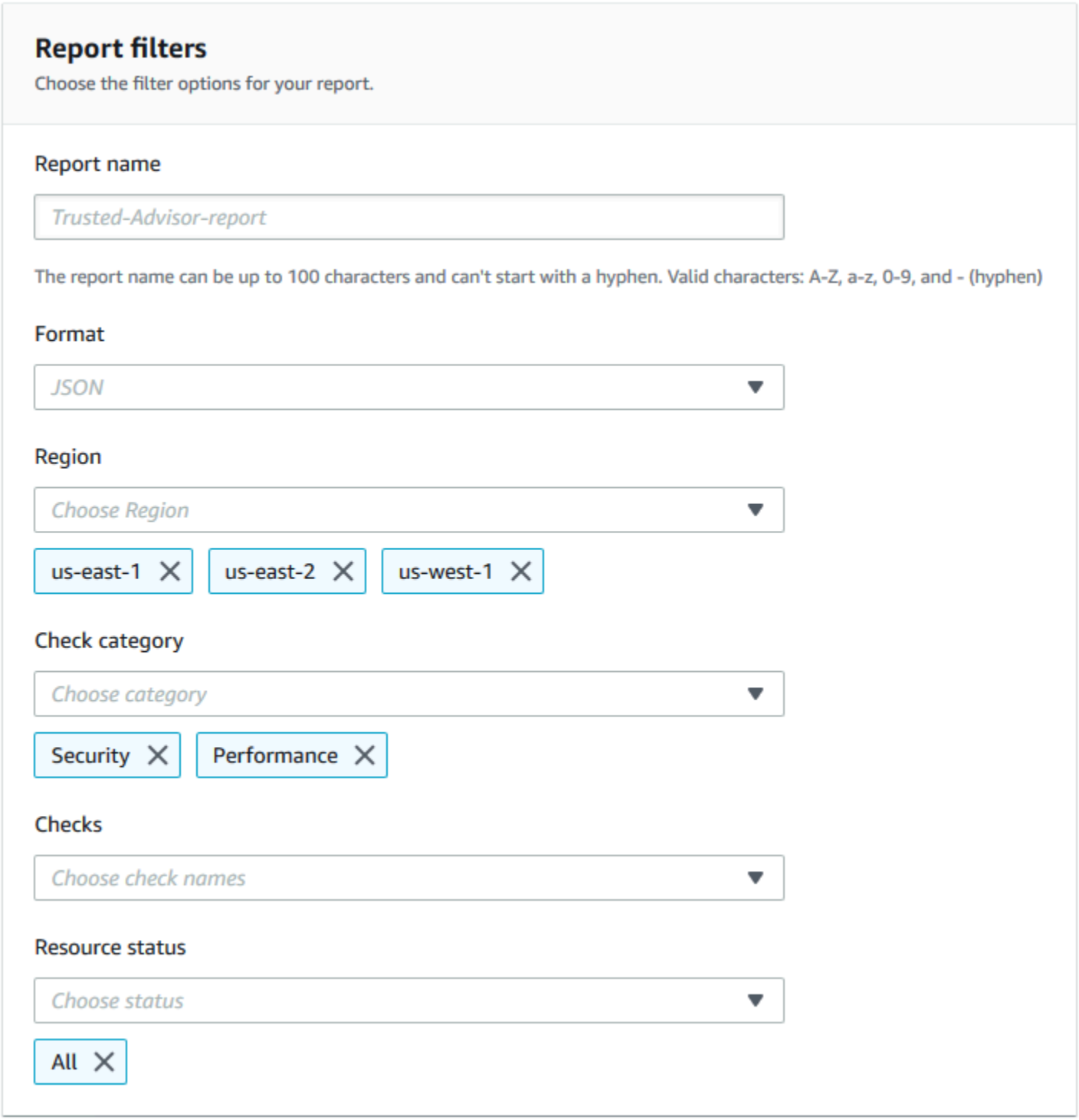
f. Per l'opzione Stato della risorsa, seleziona lo stato da filtrare, ad esempio Avviso, o seleziona Tutti.

5. Per l'opzione Organizzazione AWS, seleziona le unità organizzative (organizational unit, OU) da includere nel rapporto. Per ulteriori informazioni sulle OU, consulta la sezione Gestione delle unità organizzative nella Guida per l'utente di AWS Organizations.
6. Selezionare Create report (Crea report).

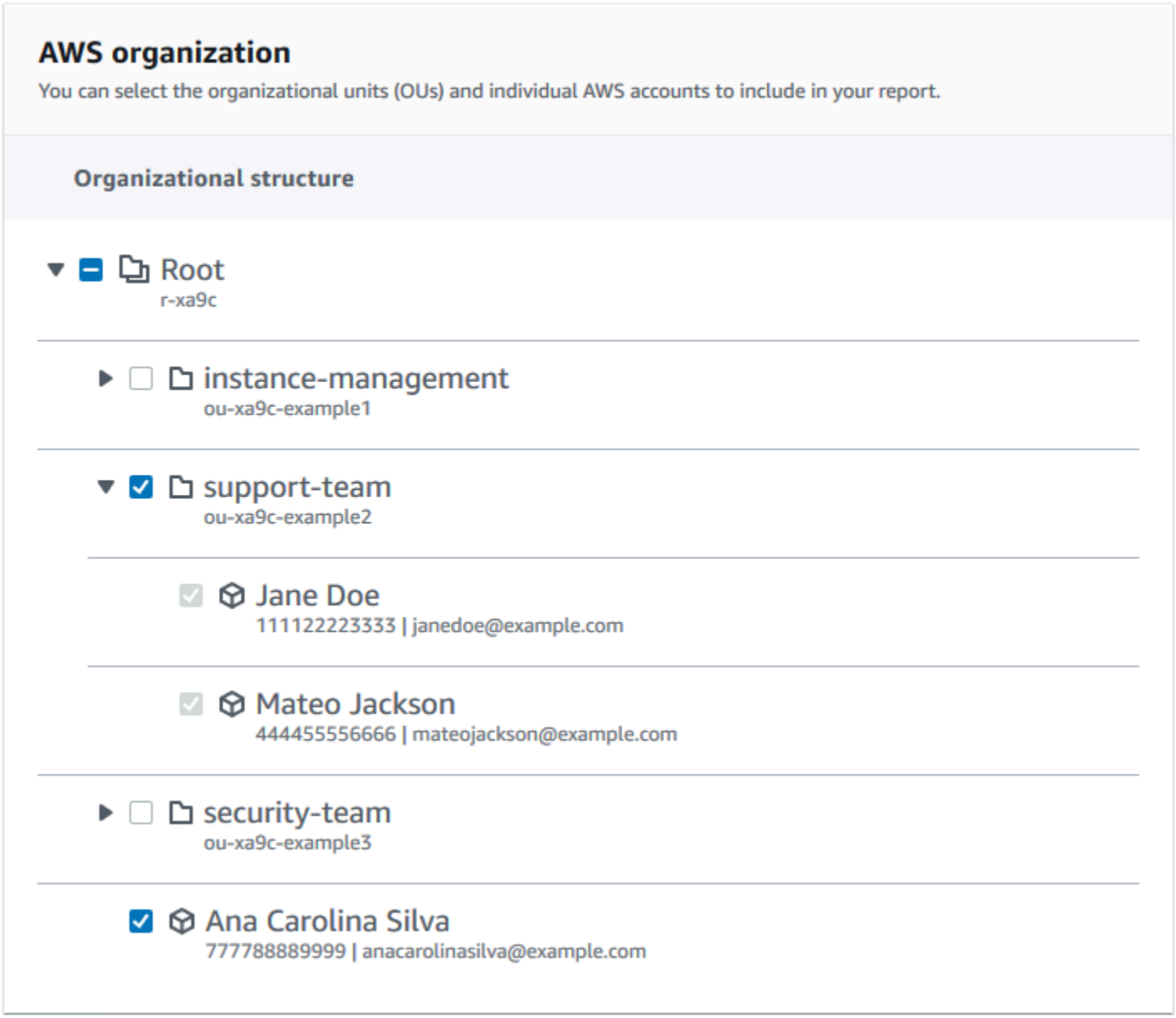
Example : Crea opzioni di filtri per report

L'esempio seguente crea un report JSON per i seguenti elementi:

- Tre Regioni AWS
- Tutti i controlli di Sicurezza e Prestazioni



Nell'esempio seguente, il report include l'OU support-team e un account AWS che fanno parte dell'organizzazione.



Note

- La quantità di tempo necessaria per creare il report dipende dal numero di account nell'organizzazione e dal numero di risorse in ciascun account.
- Non è possibile generare più di un report contemporaneamente, a meno che il report attuale non sia in esecuzione da più di 6 ore.
- Aggiorna la pagina se non vedi che il report viene visualizzato nella pagina.

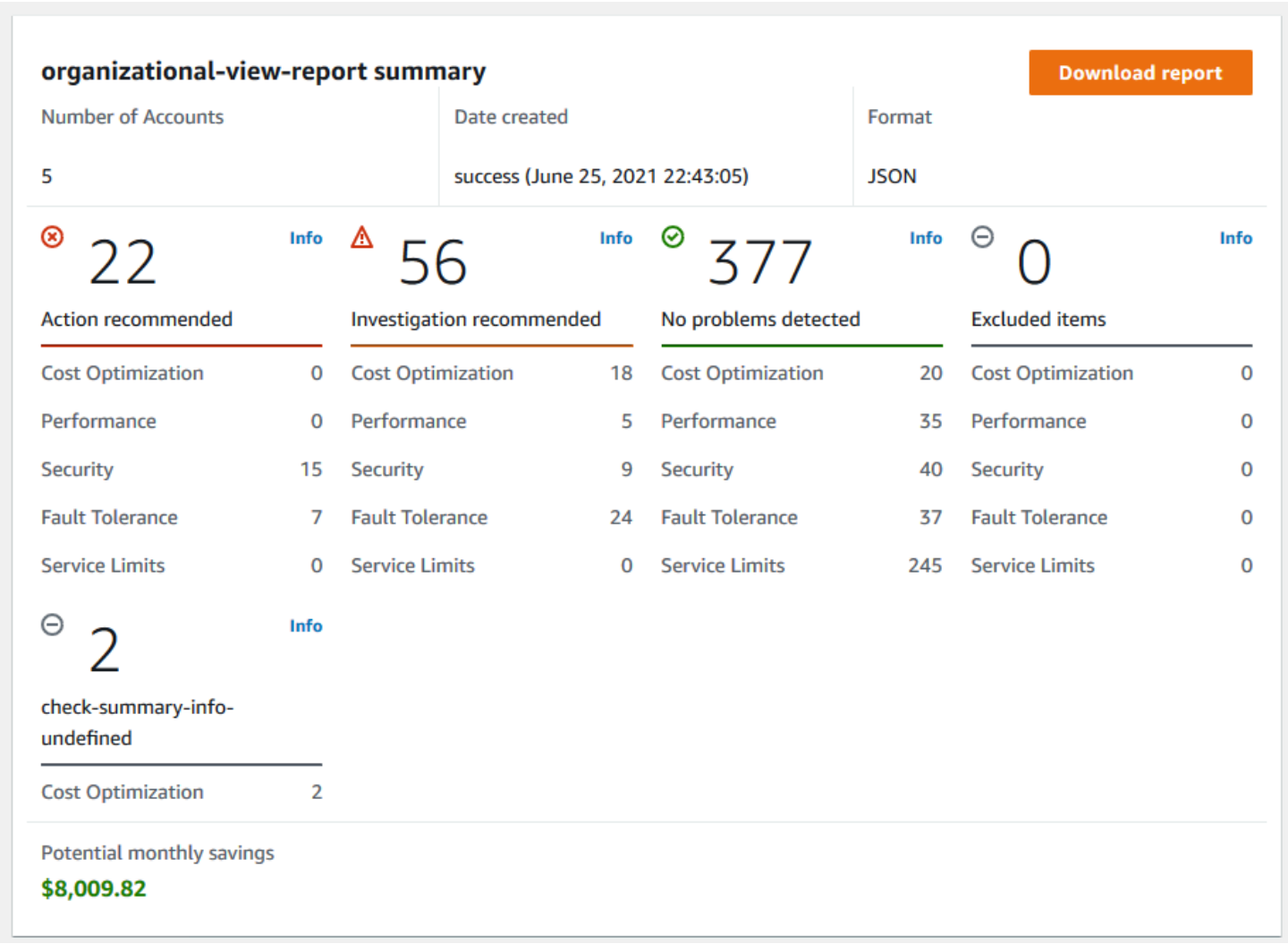
Esamina il riepilogo del report

Dopo che il report è pronto, è possibile visualizzare il riepilogo del report dalla console Trusted Advisor. In questo modo è possibile visualizzare rapidamente il riepilogo dei risultati dei controlli in tutta l'organizzazione.

Per visualizzare il riepilogo del report

1. Accedi all'account di gestione dell'organizzazione e apri la console AWS Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor.
2. Nel riquadro di navigazione, seleziona Visualizzazione organizzativa.
3. Scegli il nome del report.
4. Nella pagina Riepilogo, visualizza gli stati di controllo per ogni categoria. Puoi anche selezionare Scarica report.

Example : Riepilogo dei report per un'organizzazione



Scarica un report della visualizzazione organizzativa

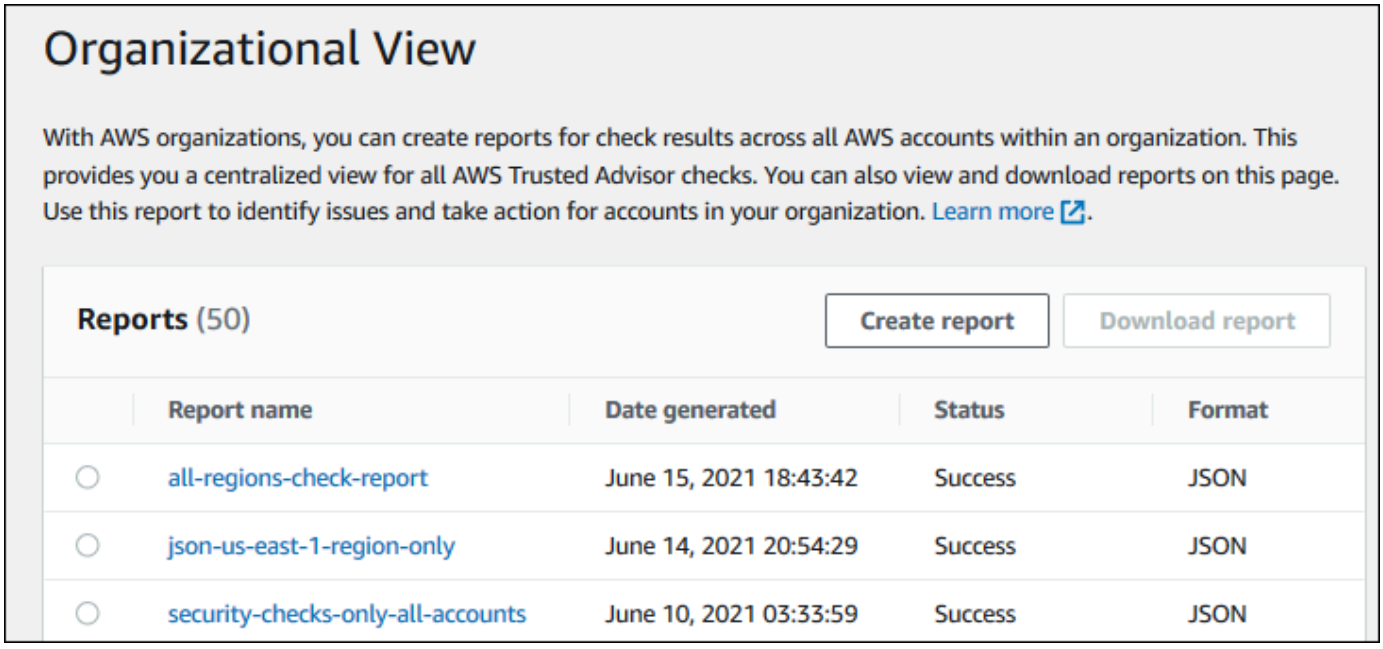
Dopo che il report è pronto, scaricalo dalla console Trusted Advisor. Il report è un file .zip contenente tre file:

- `summary.json`: Contiene un riepilogo dei risultati del controllo per ogni categoria di controllo.
- `schema.json`: Contiene lo schema dei controlli specificati nel report.
- Un file di risorse (.json o .csv): Contiene informazioni dettagliate sugli stati di controllo delle risorse dell'organizzazione.

Per scaricare un report della visualizzazione organizzativa

1. Accedi all'account di gestione dell'organizzazione e apri la console AWS Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor.
2. Nel riquadro di navigazione, seleziona Visualizzazione organizzativa.

   La pagina Visualizzazione organizzativa mostra i report disponibili per il download.
3. Seleziona un report, scegli Scarica report e salva il file. È possibile scaricare un solo report alla volta.



4. Decomprimere il file.
5. Utilizza un editor di testo per aprire il file `.json` o un'applicazione per fogli di calcolo per aprire il file `.csv`.

> **Note**
>
> Potresti ricevere più file se il report è di 5 MB o più grande.

Example : file summary.json

Il file `summary.json` mostra il numero di account nell'organizzazione e gli stati dei controlli in ciascuna categoria.

Trusted Advisor utilizza il seguente codice di colore per i risultati del controllo:

- `Green`: Trusted Advisor non rileva un problema per il controllo.
- `Yellow`: Trusted Advisor rileva un possibile problema per il controllo.
- `Red`: Trusted Advisor rileva un errore e consiglia un'azione per il controllo.
- `Blue`: Trusted Advisor non è in grado di determinare lo stato del controllo.

Nell'esempio seguente, due controlli sono `Red`, uno è `Green`, e uno è `Yellow`.


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
                    "count": 1
```

```
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : file schema.json

Il file `schema.json` include lo schema per i controlli nel report. Nell'esempio seguente sono inclusi gli ID e le proprietà per i controlli della Policy delle Password IAM (Yw2K9puPzl) e della rotazione delle chiavi IAM (DqdJqYeRm5).

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
        "Reason"
```

```
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : file resources.csv

Il file `resources.csv` include informazioni sulle risorse nell'organizzazione. In questo esempio vengono illustrate alcune colonne di dati che compaiono nel report, ad esempio le seguenti:

- L'ID dell'account interessato
- L'ID del controllo Trusted Advisor
- L'ID della risorsa
- Il timestamp del report
- Il nome completo del controllo Trusted Advisor
- La categoria del controllo Trusted Advisor
- L'ID dell'unità organizzativa (OU) padre o root

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7lgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

Il file delle risorse contiene voci solo se esiste un risultato di controllo a livello di risorsa. È possibile che non vengano visualizzati controlli nel report per i seguenti motivi:

- Alcuni controlli, come MFA nell'account Root, non dispongono di risorse e non compaiono nel report. I controlli senza risorse invece compaiono nel file `summary.json`.
- Alcuni controlli mostrano solo le risorse se sono `Red` o `Yellow`. Se tutte le risorse sono `Green`, potrebbero non comparire nel report.
- Se un account non è abilitato per un servizio che richiede il controllo, il controllo potrebbe non comparire nel report. Ad esempio, se non utilizzi istanze riservate Amazon Elastic Compute Cloud nell'organizzazione, il controllo Scadenza della locazione di istanze riservate Amazon EC2 non comparirà nel report.
- L'account non ha aggiornato i risultati degli assegni. Ciò può verificarsi quando gli utenti con un piano di supporto Basic o Developer accedono alla console Trusted Advisor per la prima volta. Se disponi di un piano di supporto Business, Enterprise On-Ramp o Enterprise, potrebbe essere necessaria più di una settimana dall'iscrizione dell'account affinché gli utenti possano visualizzare i risultati dei controlli. Per ulteriori informazioni, consulta Aggiorna i controlli Trusted Advisor.
- Se solo l'account di gestione dell'organizzazione ha abilitato i suggerimenti per i controlli, il report non includerà le risorse per gli altri account dell'organizzazione.

Per il file delle risorse, è possibile utilizzare software comuni come Microsoft Excel per aprire il formato di file csv. È possibile utilizzare il file .cvs per l'analisi unica di tutti i controlli in tutti gli account dell'organizzazione. Se si desidera utilizzare il report con un'applicazione, è possibile scaricare il report come file con estensione .json.

Il formato con estensione .json offre una maggiore flessibilità rispetto al formato .csv per casi d'uso avanzati quali aggregazione e analisi avanzate con più set di dati. Ad esempio, si può utilizzare un'interfaccia SQL con un sevizio AWS come Amazon Athena per eseguire query sui report. Si può anche utilizzare Amazon QuickSight per creare pannelli di controllo e visualizzare i tuoi dati. Per ulteriori informazioni, consulta Utilizzo di altri servizi AWS per visualizzare report Trusted Advisor.

Disattiva visualizzazione organizzativa

Segui questa procedura per disattivare la visualizzazione organizzativa. È necessario accedere all'account di gestione dell'organizzazione o assumere un ruolo con le autorizzazioni necessarie per disattivare questa funzionalità. Non è possibile disattivare questa funzionalità da un altro account nell'organizzazione.

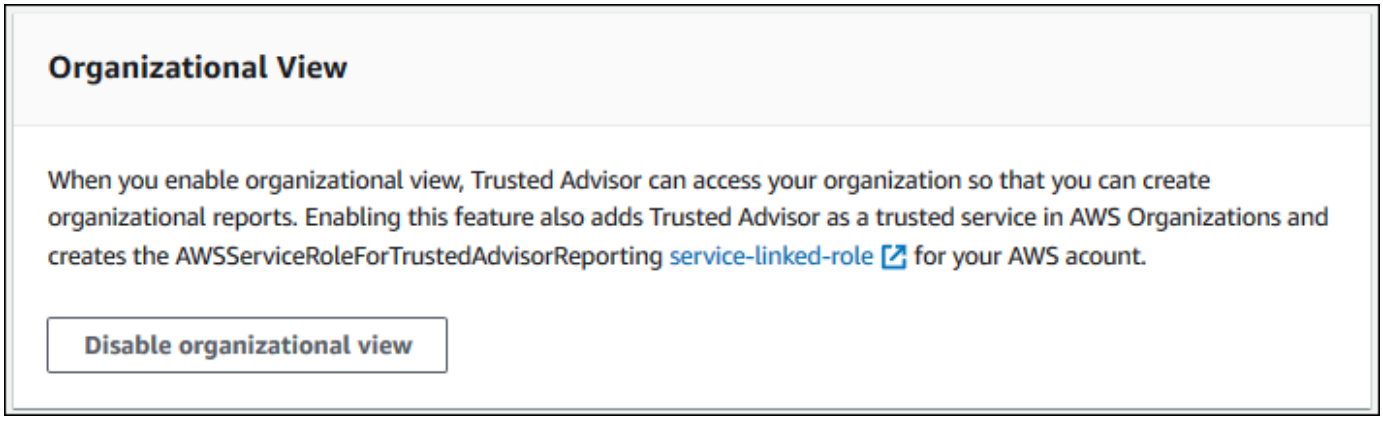
Dopo aver disattivato questa funzionalità, si verifica quanto segue:

- Trusted Advisor viene rimosso come servizio sicuro in Organizations.

- Il ruolo collegato al servizio `AWSServiceRoleForTrustedAdvisorReporting` viene sbloccato nell'account di gestione dell'organizzazione. Ciò significa che è possibile eliminarlo manualmente, se necessario.
- Non è possibile creare, visualizzare o scaricare report per l'organizzazione. Per accedere ai report creati in precedenza, è necessario riattivare la visualizzazione organizzativa dalla console Trusted Advisor. Per informazioni, consultare Abilita visualizzazione organizzativa.

Per disattivare la visualizzazione organizzativa per Trusted Advisor

1. Accedi all'account di gestione dell'organizzazione e apri la console AWS Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor.
2. Nel riquadro di navigazione, scegli Preferences (Preferenze).
3. Alla voce Visualizzazione organizzativa, seleziona Disattiva la visualizzazione organizzativa.



Dopo aver disattivato la visualizzazione organizzativa, Trusted Advisor non aggrega più controlli da altri account AWS nella tua organizzazione. Tuttavia, Il ruolo collegato al servizio `AWSServiceRoleForTrustedAdvisorReporting` rimane nell'account di gestione dell'organizzazione finché non viene eliminato tramite la console IAM, l'API IAM o la AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

> **Note**
>
> È possibile utilizzare altri servizi AWS per eseguire query e visualizzare i dati per i report di visualizzazione organizzativa. Per ulteriori informazioni, consulta le seguenti risorse :

- Visualizza suggerimenti di AWS Trusted Advisor su scala con AWS Organizations nel Blog AWS Management & Governance
- Utilizzo di altri servizi AWS per visualizzare report Trusted Advisor

Utilizzo delle policy IAM per consentire l'accesso alla visualizzazione organizzativa

È possibile utilizzare le policy AWS Identity and Access Management (IAM) seguenti per consentire agli utenti o ai ruoli dell'account di accedere alla visualizzazione organizzativa in AWS Trusted Advisor.

Example : Accesso completo alla visualizzazione organizzativa

La policy seguente consente l'accesso completo alla funzione di visualizzazione organizzativa. Un utente con queste autorizzazioni può eseguire le operazioni seguenti:

- Abilita e disabilita la visualizzazione organizzativa
- Crea, visualizza e scarica report

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
```

```
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : Accesso in modalità lettura alla visualizzazione organizzativa

La policy seguente consente l'accesso in sola lettura alla visualizzazione organizzativa per Trusted Advisor. Un utente con queste autorizzazioni può solo visualizzare e scaricare i report esistenti.

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

```
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

Puoi anche creare policy IAM personalizzate. Per ulteriori informazioni, consulta la sezione Creazione di policy IAM nella Guida per l'utente IAM.

> **Note**
>
> Se hai attivato AWS CloudTrail nel tuo account, i seguenti ruoli possono essere visualizzati nelle voci di log:
>
> - `AWSServiceRoleForTrustedAdvisorReporting`: Il ruolo collegato al servizio che Trusted Advisor utilizza per accedere agli account nell'organizzazione.
> - `AWSServiceRoleForTrustedAdvisor`: Il ruolo collegato al servizio che Trusted Advisor utilizza per accedere ai servizi nell'organizzazione.

Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo di ruoli collegati ai servizi per Trusted Advisor.

Utilizzo di altri servizi AWS per visualizzare report Trusted Advisor

Segui questo tutorial per caricare e visualizzare i dati utilizzando altri servizi AWS. In questo argomento, puoi creare un bucket Amazon Simple Storage Service (Amazon S3) per memorizzare il report e un modello AWS CloudFormation per creare risorse nell'account. Quindi, puoi utilizzare Amazon Athena per analizzare o eseguire query per il tuo report o Amazon QuickSight per visualizzare tali dati in un pannello di controllo.

Per informazioni ed esempi per la visualizzazione dei dati del report, consulta la sezione Suggerimenti di visualizzazione di AWS Trusted Advisor su scala con AWS Organizations nel Blog AWS Management & Governance.

Prerequisiti

Prima di iniziare il tutorial, assicurati di soddisfare i seguenti requisiti:

- Accedi come utente AWS Identity and Access Management (IAM) con autorizzazioni di amministratore.
- Utilizza la Regione AWS Stati Uniti orientali (Virginia settentrionale) per configurare rapidamente i servizi e le risorse AWS.
- Crea un account Amazon QuickSight. Per ulteriori informazioni, consulta la sezione Nozioni di base sull'analisi dei dati in Amazon QuickSight nella Guida per l'utente di Amazon QuickSight.

Carica il report su Amazon S3

Dopo aver scaricato il report `resources.json`, carica il file su Amazon S3. È necessario utilizzare un bucket nella Regione degli Stati Uniti orientali (Virginia settentrionale).

Per caricare i file in un bucket Amazon S3

1. Accedi all'AWS Management Console all'indirizzo https://console.aws.amazon.com/.
2. Utilizza il Selettore di Regione e seleziona la Regione Stati Uniti orientali (Virginia settentrionale).
3. Apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.

4. Dall'elenco dei bucket, scegli un bucket S3 e copia il nome. Il nome viene utilizzato nella procedura successiva.
5. Sulla pagina *bucket-name*, seleziona Crea cartella, inserisci il nome **folder1**, quindi scegli Salva.
6. Seleziona cartella1.
7. In cartella1, seleziona Caricamento e scegli il file `resources.json`.
8. Seleziona Avanti, mantieni le opzioni predefinite e scegli Carica.

> **Note**
>
> Se carichi un nuovo report in questo bucket, rinomina i file `.json` ogni volta che li carichi in modo da non sovrascrivere i report esistenti. Ad esempio, puoi aggiungere il timestamp a ciascun file, ad esempio `resources-timestamp.json`, `resources-timestamp2.json` e così via.

Creazione delle risorse utilizzando AWS CloudFormation

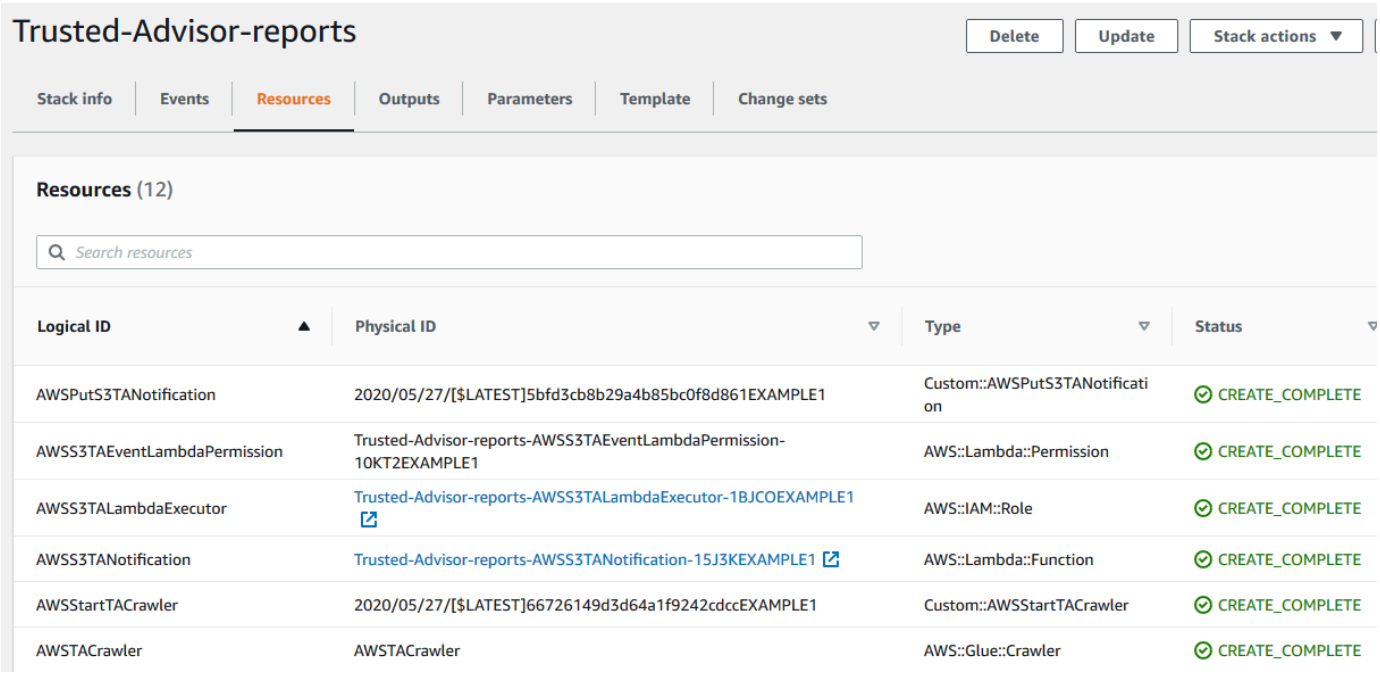
Dopo aver caricato il report su Amazon S3, carica il seguente modello YAML su AWS CloudFormation. Questo modello indica a AWS CloudFormation quali risorse creare per l'account in modo che altri servizi possano utilizzare i dati del report nel bucket S3. Il modello crea risorse per IAM, AWS Lambda, e AWS Glue.

Per creare risorse con AWS CloudFormation

1. Scarica il file trusted-advisor-reports-template.zip.
2. Decomprimere il file.
3. Apri il file modello in un editor di testo.
4. Per i parametri `BucketName` e `FolderName`, sostituisci i valori per *your-bucket-name-here* e *folder1* con il nome del bucket e il nome della cartella nel tuo account.
5. Salva il file.
6. Aprire la console AWS CloudFormation all'indirizzo https://console.aws.amazon.com/cloudformation.
7. Se non l'hai ancora fatto, nel Selettore di Regione seleziona la Regione Stati Uniti orientali (Virginia settentrionale).

8. Nel riquadro di navigazione selezionare Stacks (Stack).
9. Seleziona Crea stack, quindi seleziona Con nuove risorse (standard).
10. Nella pagina Crea stack alla voce Specifica modello, seleziona Carica file modello, quindi seleziona Scegli file.
11. Scegli il file YALM e seleziona Avanti.
12. Nella pagina Specifica dettagli stack, inserisci un nome per lo stack come ad esempio **`Organizational-view-Trusted-Advisor-reports`**, quindi seleziona Avanti.
13. Nella pagina Opzioni di configurazione stack, mantieni le opzioni predefinite e quindi scegli Avanti.
14. Nella pagina Esamina **`Organizational-view-Trusted-Advisor-reports`** , controlla le tue opzioni. In fondo alla pagina, seleziona la casella di controllo Acconsento alla creazione di risorse IAM da parte di AWS CloudFormation.
15. Seleziona Crea stack.

    La creazione dello stack richiede circa 5 minuti.
16. Dopo aver creato correttamente lo stack, la scheda Risorse viene visualizzata come nell'esempio seguente.



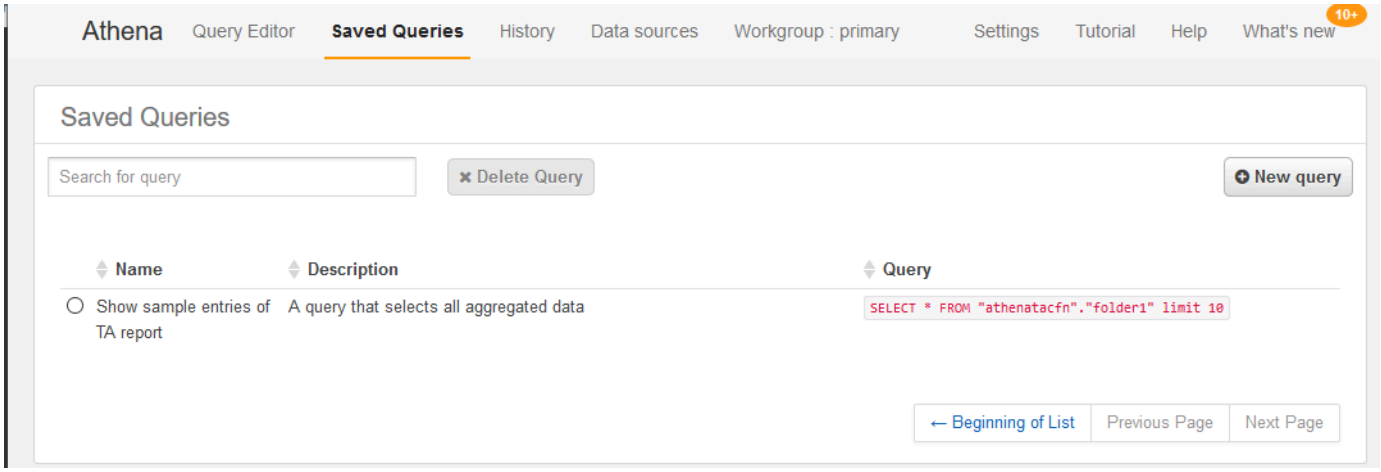
Esegue query sui dati in Amazon Athena

Dopo aver ottenuto le risorse, è possibile visualizzare i dati in Athena. Utilizza Athena per creare query e analizzare i risultati del report, ad esempio per cercare risultati di controllo specifici per gli account nell'organizzazione.

> **Note**
>
> - Seleziona la Regione Stati Uniti orientali (Virginia settentrionale).
> - Se sei un nuovo utente di Athena, devi specificare una posizione dei risultati della query prima di poter eseguire una query per il tuo report. È consigliabile specificare un bucket S3 diverso per questa posizione. Per ulteriori informazioni, consulta la sezione Specificare una posizione dei risultati delle query nella Guida per l'utente di Amazon Athena.

Per eseguire query sui dati in Athena

1. Aprire la console Athena all'indirizzo https://console.aws.amazon.com/athena/.
2. Se non l'hai ancora fatto, nel Selettore di Regione seleziona la Regione Stati Uniti orientali (Virginia settentrionale).
3. Seleziona Query salvate e nel campo di ricerca, digita **`Show sample`**.
4. Seleziona la query visualizzata, ad esempio Mostra voci di esempio del report TA.



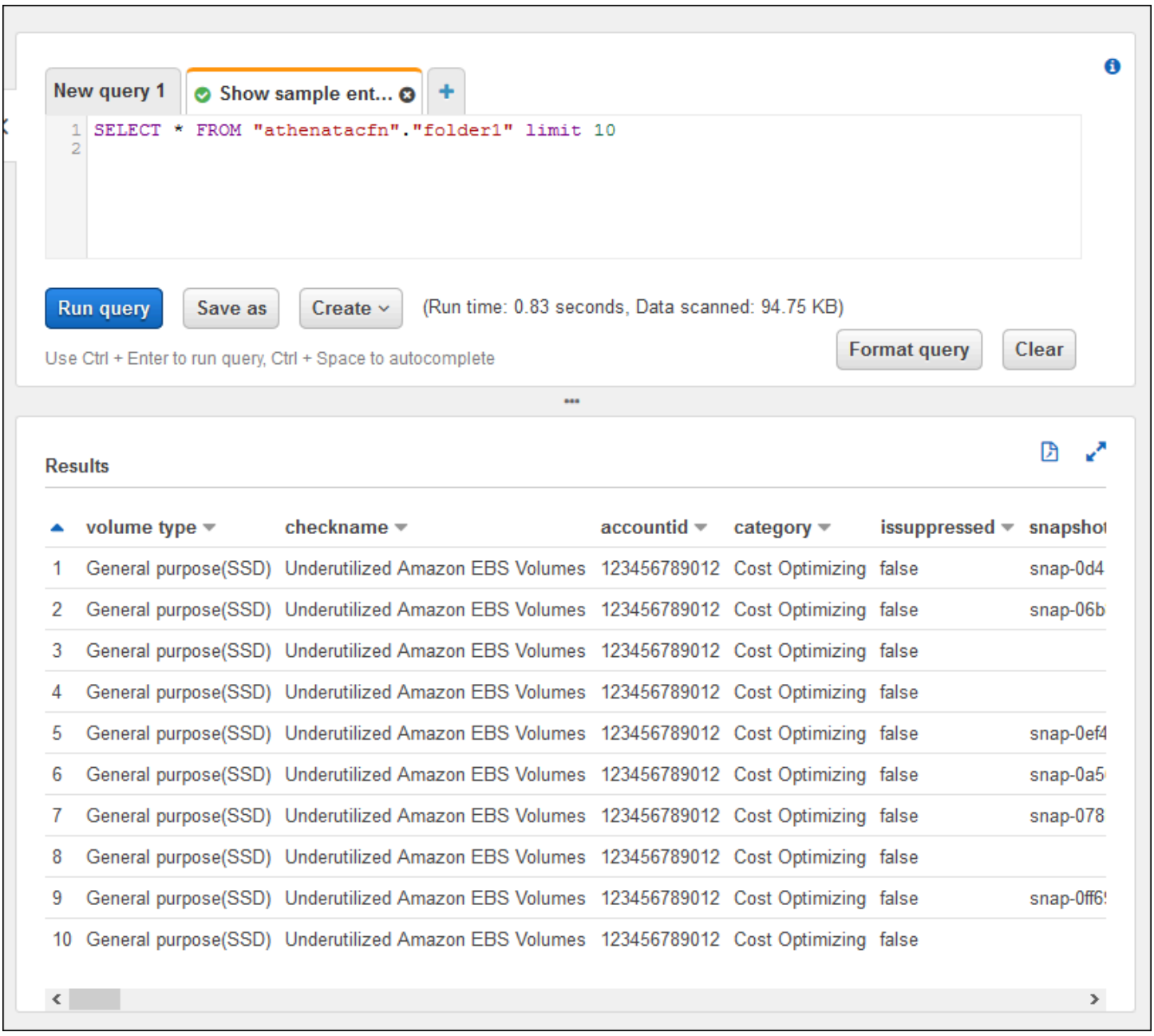
La query dovrebbe somigliare alla seguente.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. Scegli Run Query (Esegui query). Vengono visualizzati i risultati della query.

Example : Query Athena

Nell'esempio seguente vengono illustrate 10 voci di esempio del report.



	volume type	checkname	accountid	category	issuppressed	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

Per ulteriori informazioni, consulta la sezione Esecuzione di query SQL con Amazon Athena nella Guida per l'utente di Amazon Athena.

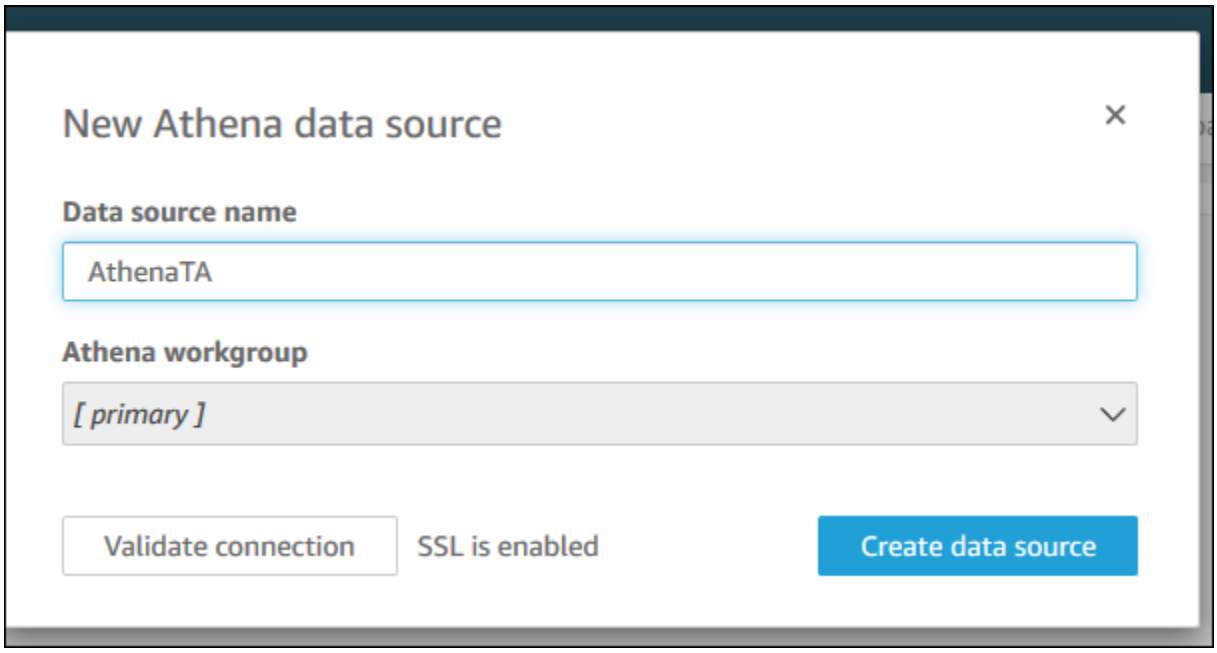
Creazione di un pannello di controllo in Amazon QuickSight

Amazon QuickSight può anche essere configurato in modo da poter visualizzare i dati in un pannello di controllo e visualizzare le informazioni del report.

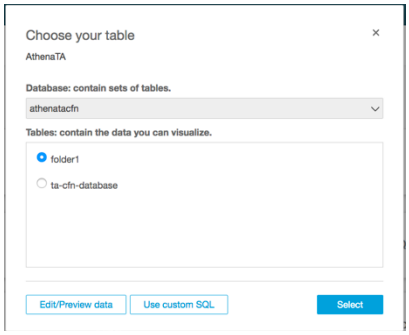
> **Note**
>
> È necessario utilizzare la Regione Stati Uniti orientali (Virginia settentrionale).

Per creare un pannello di controllo in Amazon QuickSight

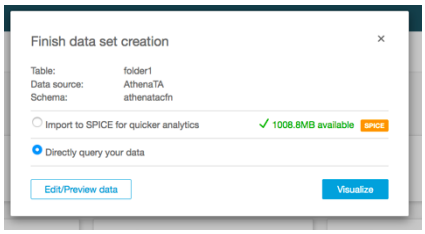
1. Esplora la console Amazon QuickSight e accedi al tuo account.
2. Seleziona Nuova analisi, Nuovo set di dati, quindi scegli Athena.
3. Nella finestra di dialogo Nuova origine dati Athena, inserisci un nome per l'origine dati, ad esempio TA Athena, quindi seleziona Crea origine dati.



4. Nella finestra di dialogo Scegli la tabella seleziona la casella athenatacfn, poi cartella1, quindi scegli Seleziona.



5. Nella finestra di dialogo Fine della creazione del set di dati, seleziona Query diretta dei dati, quindi scegli Visualizza.

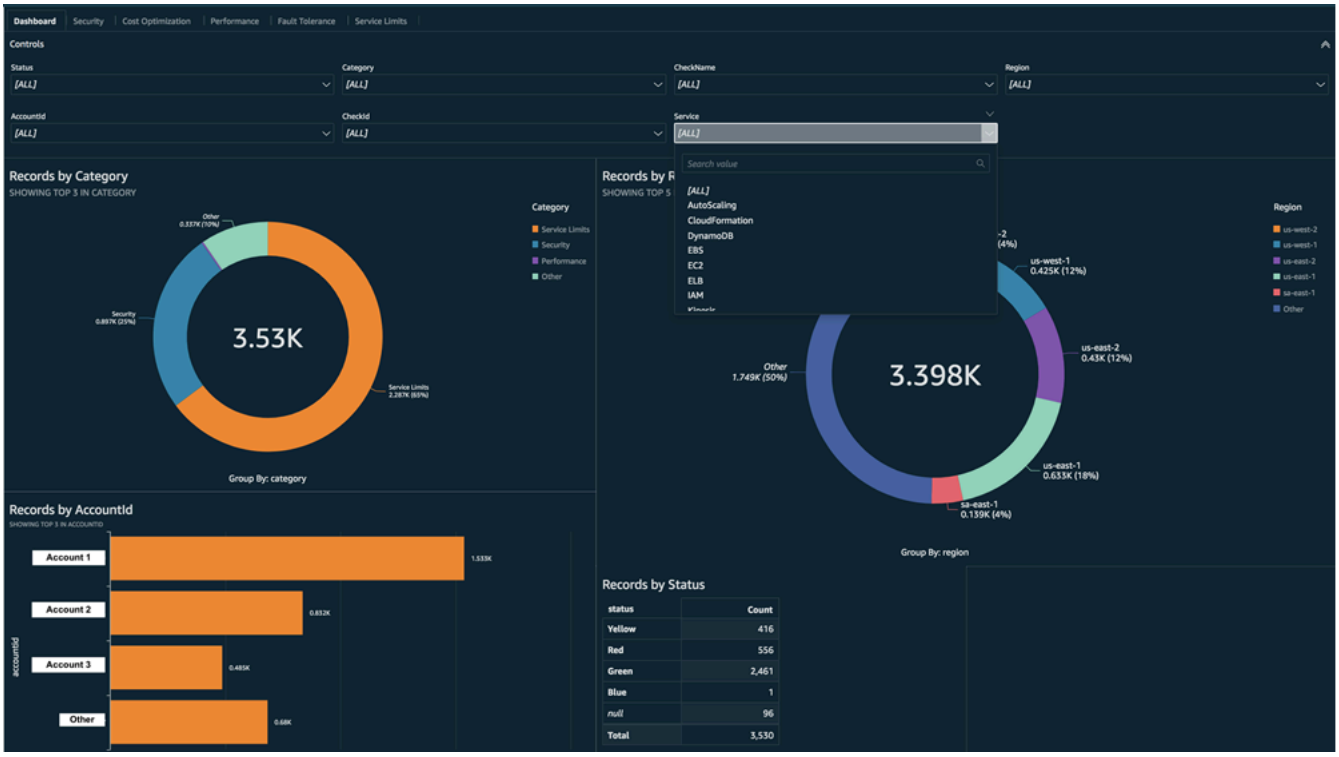


Ora puoi creare un pannello di controllo in Amazon QuickSight. Per ulteriori informazioni, consulta Come utilizzare i pannelli di controllo nella Guida per l'utente di Amazon QuickSight.

Example : Pannello di controllo Amazon QuickSight

L'esempio seguente di pannello di controllo mostra informazioni sui controlli Trusted Advisor, ad esempio:

- ID degli account interessati
- Riepilogo per Regione AWS
- Categorie di controllo
- Stati del controllo
- Numero di voci nel report per ciascun account



> **Note**
>
> Se hai errori di autorizzazione durante la creazione del pannello di controllo, assicurati che Amazon QuickSight possa utilizzare Athena. Per ulteriori informazioni, consulta la sezione Non riesco a stabilire la connessione ad Amazon Athena nella Guida per l'utente Amazon QuickSight.

Per ulteriori informazioni ed esempi per dati di report di visualizzazione, consulta la sezione Visualizza suggerimenti di AWS Trusted Advisor su scala con AWS Organizations nel Blog AWS Management & Governance.

Risoluzione dei problemi

In caso di problemi con questo tutorial, consulta i seguenti suggerimenti per la risoluzione dei problemi.

Non vedo i dati più recenti nel mio rapporto

Quando si crea un report, la funzione di visualizzazione dell'organizzazione non aggiorna automaticamente i controlli Trusted Advisor nell'organizzazione. Per ottenere i risultati dei controlli più

recenti, aggiorna i controlli per l'account di gestione e per ogni account membro nell'organizzazione. Per ulteriori informazioni, consulta Aggiorna i controlli Trusted Advisor.

Ci sono colonne duplicate nel report

La console Athena potrebbe mostrare il seguente errore nella tabella se il report contiene colonne duplicate.

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table descriptor contains duplicate columns
```

Ad esempio, se nel report è stata aggiunta una colonna già esistente, ciò può causare problemi quando si tentano di visualizzare i dati del report nella console Athena. Per correggere questo problema, attieniti alla seguente procedura

Trovare le colonne duplicate

Puoi utilizzare la console AWS Glue per visualizzare lo schema e verificare rapidamente se nel report sono presenti colonne duplicate.

Per trovare colonne duplicate

1. Apri la console AWS Glue all'indirizzo https://console.aws.amazon.com/glue/.
2. Se non l'hai ancora fatto, nel Selettore di Regione seleziona la Regione Stati Uniti orientali (Virginia settentrionale).
3. Nel pannello di navigazione, seleziona Tabelle.
4. Scegli il nome della cartella, ad esempio ***cartella1*** e quindi in Schema, visualizza i valori per Nome colonna.

   Se hai una colonna duplicata, devi caricare un nuovo report nel tuo bucket Amazon S3. Consulta la seguente sezione Caricamento di un nuovo report.

Caricamento di un nuovo report

Dopo aver identificato la colonna duplicata, è consigliabile sostituire il report esistente con uno nuovo. Questo assicura che le risorse create da questa esercitazione utilizzino i dati di report più recenti dell'organizzazione.

Per caricare un nuovo report

1. Se non l'hai ancora fatto, aggiorna i controlli Trusted Advisor per gli account nell'organizzazione. Per informazioni, consultare Aggiorna i controlli Trusted Advisor.
2. Crea e scarica un altro report JSON nella console Trusted Advisor. Per informazioni, consultare Creazione di report di visualizzazione organizzativa. Per questo tutorial è necessario utilizzare un file JSON.
3. Accedi alla AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
4. Seleziona il tuo bucket Amazon S3 e scegli la cartella *`folder1`*.
5. Seleziona il report *`resources`*`.json` precedente e scegli Elimina.
6. Nella pagina Elimina oggetti, alla voce Eliminare definitivamente gli oggetti?, fai clic su **`permanently delete`**, quindi seleziona Elimina di oggetti.
7. Nel bucket S3, seleziona Carica e specifica il nuovo report. Questa azione aggiorna automaticamente la tua tabella Athena e le risorse crawler AWS Glue con i dati di report più recenti. Potrebbero volerci alcuni minuti per aggiornare le risorse.
8. Inserisci una nuova query nella console Athena. Per informazioni, consultare Esegue query sui dati in Amazon Athena.

> **Note**
>
> Se ci sono ancora problemi con questo tutorial, puoi creare una richiesta di supporto tecnico nel Centro AWS Support.

Visualizzazione dei controlli AWS Trusted Advisor forniti da AWS Config

AWS Config è un servizio che valuta, verifica e valuta continuamente le configurazioni delle risorse per le impostazioni desiderate. AWS Config fornisce regole gestite, ovvero regole predefinite, controlli di conformità personalizzabili che utilizzano AWS Config per valutare se le risorse AWS sono conformi alle best practice.

La console di AWS Config ti guiderà durante la configurazione l'attivazione di regole gestite. Puoi anche utilizzare AWS Command Line Interface (AWS CLI) o l'API AWS Config per passare il

codice JSON che definisce la configurazione di una regola gestita. Puoi inoltre personalizzare il comportamento di una regola gestita per adattarlo alle tue esigenze. Hai la possibilità di personalizzare i parametri della regola per definire gli attributi che le risorse devono avere per soddisfare la regola. Per ulteriori informazioni sull'abilitazione di AWS Config, consulta la Guida per gli sviluppatori di AWS Config.

Le regole gestite da AWS Config forniscono una serie di controlli Trusted Advisor in tutte le categorie. Quando abiliti determinate regole gestite, i controlli Trusted Advisor corrispondenti vengono abilitati automaticamente. Per sapere quali controlli Trusted Advisor sono forniti da regole gestite da AWS Config specifiche, consulta AWS Trusted Advisor verifica riferimento.

I controlli forniti da AWS Config sono disponibili per i clienti con piani AWS Business Support, AWS Enterprise On-Ramp e AWS Enterprise Support. Se abiliti AWS Config e disponi di uno di questi piani di AWS Support, vedrai automaticamente i suggerimenti forniti dalle corrispondenti regole gestite da AWS Config e distribuite.

> **Note**
>
> I risultati di questi controlli vengono aggiornati automaticamente più volte al giorno in base agli aggiornamenti attivati dalle modifiche relativi alle regole gestite da AWS Config. Le richieste di aggiornamento non sono consentite. Al momento, non è possibile escludere le risorse da questi controlli.

Risoluzione dei problemi

Se riscontri problemi con questa integrazione, consulta le informazioni seguenti sulla risoluzione dei problemi.

Indice

Ho appena abilitato i record e le regole gestite per AWS Config, ma non vedo i controlli Trusted Advisor corrispondenti.

Dopo che la regola AWS Config ha generato i risultati della valutazione, i risultati vengono visualizzati in Trusted Advisor quasi in tempo reale. Se riscontri problemi con questa funzionalità, crea una richiesta di supporto tecnico in AWS Support Center.

Ho implementato due volte la stessa regola gestita da AWS Config; cosa verrà visualizzato in Trusted Advisor?

Nei risultati di controllo Trusted Advisor vengono visualizzate voci separate per ogni regola gestita che hai installato.

Ho disattivato i record per AWS Config in una regione AWS. Che cosa verrà visualizzato in Trusted Advisor?

Se hai disattivato i record delle risorse per AWS Config in una regione AWS, Trusted Advisor non riceve più i dati dei controlli e delle regole gestite corrispondenti in tale regione. I risultati delle regole gestite esistenti rimangono attivi in AWS Config e in Trusted Advisor fino alla scadenza di AWS Config, in base alla policy di conservazione dei registratori. Se elimini una regola gestita, i dati di controllo Trusted Advisor generalmente vengono eliminati quasi in tempo reale.

Visualizzazione controlli AWS Security Hub in AWS Trusted Advisor

Dopo aver abilitato AWS Security Hub per le Account AWS, è possibile visualizzare i controlli di sicurezza e i relativi risultati nella console Trusted Advisor. È possibile utilizzare i controlli Security Hub per identificare le vulnerabilità della sicurezza nel tuo account nello stesso modo in cui puoi utilizzare i controlli Trusted Advisor. È possibile visualizzare lo stato del controllo, l'elenco delle risorse interessate e quindi seguire i suggerimenti di Security Hub per risolvere i problemi di sicurezza. È possibile utilizzare questa caratteristica per trovare i suggerimenti sulla sicurezza di Trusted Advisor e Security Hub in un'unica pratica posizione.

> **Note**
>
> - Da Trusted Advisor, puoi visualizzare i controlli negli standard di sicurezza AWS Foundational Security Best Practices eccetto per i controlli con Categoria: Ripristino >

Resilienza. Per un elenco dei controlli supportati, consulta Controlli AWS Foundational Security Best Practices nella Guida per l'utente di AWS Security Hub.

Per ulteriori informazioni sulle categorie Security Hub, consultaCategorie di controllo.

- Attualmente, quando Security Hub aggiunge nuovi controlli al standard di sicurezza AWS Foundational Security Best Practices, ci può essere un ritardo di due a quattro settimane prima di poterle visualizzare in Trusted Advisor. Questo lasso di tempo è il risultato massimo e non è garantito.

Argomenti

Prerequisiti

Per abilitare l'integrazione di Security Hub con Trusted Advisor, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un piano di supporto Business, Enterprise On-Ramp o Enterprise per utilizzare questa caratteristica. Puoi trovare il tuo piano di supporto dal Centro AWS Support o dalla pagina Piani di supporto. Per ulteriori informazioni, consulta Confronta piani AWS Support.
- Devi abilitare il registro della risorsa in AWS Config per Regioni AWS che desideri per i controlli di Security Hub. Per ulteriori informazioni, consulta Abilitazione e configurazione di AWS Config.
- È necessario abilitare Security Hub e selezionare lo standard di sicurezza AWS Foundational Security Best Practices v1.0.0. Se non l'hai già fatto, consulta Configurazione di AWS Security Hub nella Guida per l'utente di AWS Security Hub.

> **Note**
>
> Se i prerequisiti sono già stati completati, è possibile passare alla Visualizza i risultati del Security Hub.

Informazioni sugli account AWS Organizations

Se sono già stati completati i prerequisiti per un account di gestione, questa integrazione viene abilitata automaticamente per tutti gli account membri dell'organizzazione. Gli account dei singoli membri non devono contattare AWS Support per abilitare questa caratteristica. Tuttavia, gli account membri dell'organizzazione devono abilitare Security Hub se desiderano visualizzare i risultati in Trusted Advisor.

Se vuoi disabilitare questa integrazione per un account membro specifico, consulta Disabilita questa caratteristica per gli account AWS Organizations.

Visualizza i risultati del Security Hub

Dopo aver abilitato il Security Hub per il tuo account, possono essere necessarie fino a 24 ore prima che i risultati del Security Hub vengano visualizzati nella pagina di Sicurezzadella console Trusted Advisor.

Visualizza i risultati del Security Hub in Trusted Advisor

1. Passare alla console Trusted Advisor e quindi scegliere la categoria Sicurezza.
2. Nel campo Ricerca per parola chiave, immettere il nome o la descrizione del controllo.

   > **Tip**
   >
   > Per Fonte, è possibile scegliere AWS Security Hub per filtrare i controlli Security Hub.

3. Scegliere il nome del controllo Security Hub per visualizzare le seguenti informazioni:

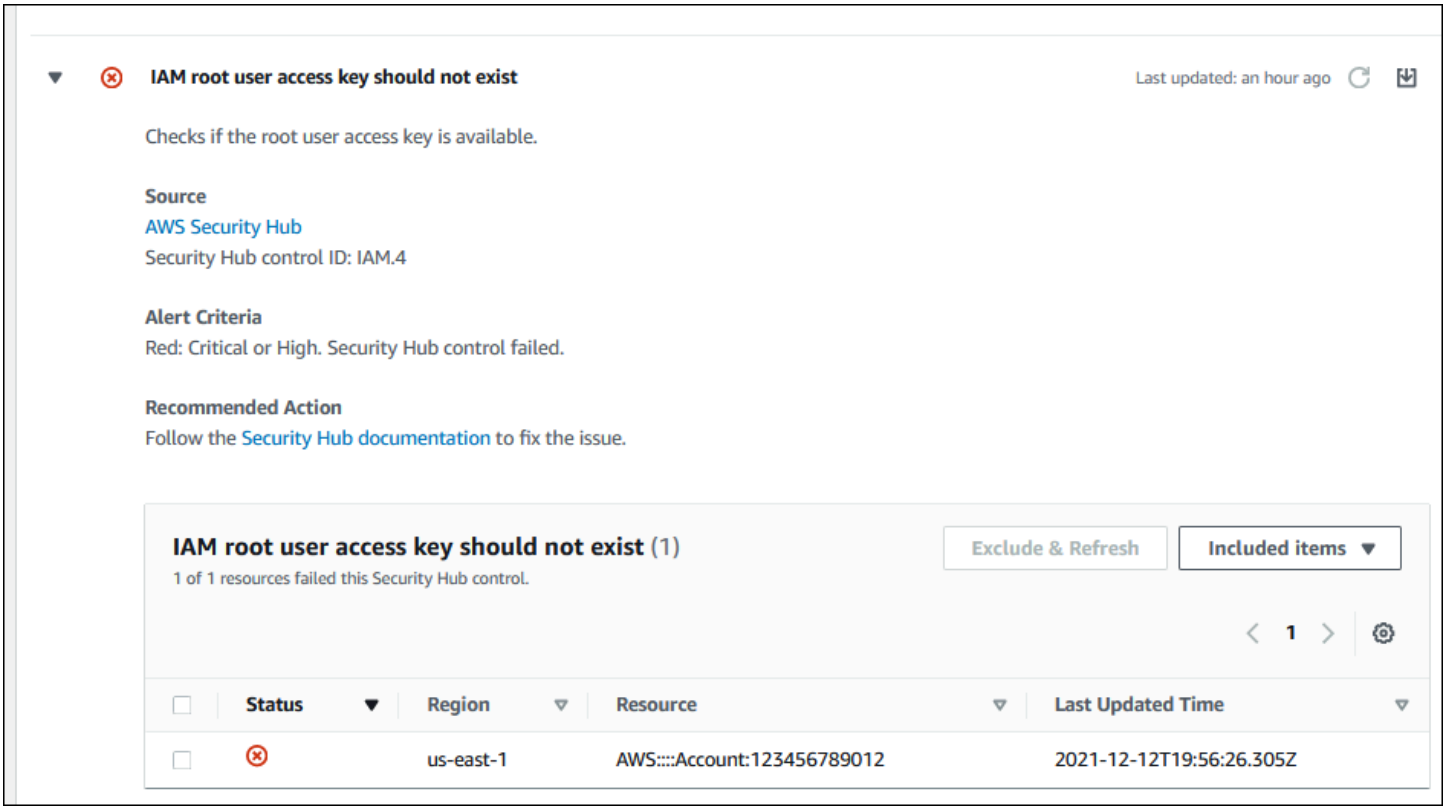
   - Description: descrive come questo controllo verifica la presenza di vulnerabilità di sicurezza nel tuo account.
   - Fonte: se il controllo proviene da AWS Trusted Advisor o da AWS Security Hub. Per i controlli Security Hub, è possibile trovare l'ID di controllo.

- Criteri di avviso: lo stato del controllo. Ad esempio, se Security Hub rileva un problema importante, lo stato potrebbe essere Red: Critical or High (Rosso: critico o alto).
- Operazione consigliata: utilizzare il collegamento della documentazione di Security Hub per trovare i passaggi consigliati per risolvere il problema.
- Risorse Security Hub: è possibile trovare le risorse nel tuo account in cui Security Hub ha rilevato un problema.

> **Note**
>
> - È necessario utilizzare Security Hub per escludere risorse dai risultati. Non è attualmente possibile utilizzare la console Trusted Advisor per escludere elementi dai controlli Security Hub. Per ulteriori informazioni, consulta Impostazione dello stato del flusso di lavoro per i risultati.
> - La caratteristica di visualizzazione organizzativa supporta questa integrazione con Security Hub. Puoi visualizzare i risultati per i controlli Security Hub in tutta l'organizzazione e quindi creare e scaricare report. Per ulteriori informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor.

Example Esempio: il controllo Security Hub per la chiave di accesso utente IAM non deve esistere

Di seguito è riportato un risultato di esempio per un controllo Security Hub nella console Trusted Advisor.



Aggiorna i risultati del Security Hub

Dopo aver abilitato uno standard di sicurezza, possono essere necessarie fino a due ore prima che Security Hub rileva i risultati per le risorse. Potrebbero essere necessarie fino a 24 ore prima che i dati siano visualizzati della console Trusted Advisor. Se di recente hai abilitato lo standard di sicurezza AWS Foundational Security Best Practices v1.0.0, controlla di nuovo la console Trusted Advisor più tardi.

> **Note**
>
> - La pianificazione per ogni controllo Security Hub è periodica o attivata dalle modifiche. Non è attualmente possibile utilizzare la console Trusted Advisor o l'API AWS Support per aggiornare i controlli Security Hub. Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza.
> - È necessario utilizzare Security Hub se si desidera escludere risorse dai risultati. Non è attualmente possibile utilizzare la console Trusted Advisor per escludere elementi dai controlli Security Hub. Per ulteriori informazioni, consulta Impostazione dello stato del flusso di lavoro per i risultati.

Disabilitare Security Hub da Trusted Advisor

Seguire questa procedura se non si desidera che le informazioni di Security Hub vengano visualizzate nella console Trusted Advisor. Questa procedura disattiva solo l'integrazione di Security Hub con Trusted Advisor. Non influirà sulle tue configurazioni con Security Hub. Puoi continuare a utilizzare la console di Security Hub per visualizzare i controlli di sicurezza, le risorse e i suggerimenti.

Per disabilitare l'integrazione di Security Hub

1. Contatta AWS Support e richiedi di disabilitare l'integrazione di Security Hub con Trusted Advisor.

   Dopo che AWS Support disabilita questa caratteristica, Security Hub interrompe l'invio di dati a Trusted Advisor. I dati di Security Hub verranno rimossi da Trusted Advisor.
2. Se desideri abilitare nuovamente questa integrazione, contatta AWS Support.

Disabilita questa caratteristica per gli account AWS Organizations

Se è già stata completata la procedura precedente per un account di gestione, l'integrazione con Security Hub viene rimossa automaticamente da tutti gli account membri dell'organizzazione. I singoli account membri dell'organizzazione non devono contattare AWS Support separatamente.

Se disponi di un account membro di un'organizzazione, puoi contattare AWS Support per rimuovere questa caratteristica solo dal tuo account.

Risoluzione dei problemi

Se riscontri problemi con questa integrazione, consulta le informazioni seguenti sulla risoluzione dei problemi.

Indice

- Visualizzo molteplici Regioni AWS per la stessa risorsa interessata per la verifica Security Hub
- Ho disattivato Security Hub o AWS Config in una regione
- Il mio controllo è archiviato in Security Hub ma visualizzo ancora i risultati in Trusted Advisor
- Non riesco ancora a visualizzare i risultati del mio Security Hub

Non vedo i risultati di Security Hub nella console Trusted Advisor

Verifica di avere completato i seguenti passaggi:

- Disponi di un piano di supporto Business, Enterprise On-Ramp o Enterprise.
- Hai abilitato il registro della risorsa in AWS Config all'interno della stessa regione di Security Hub.
- Hai abilitato il Security Hub e selezionato lo standard di sicurezza AWS Foundational Security Best Practices v1.0.0.
- I nuovi controlli di Security Hub vengono aggiunti come controlli in Trusted Advisor entro due a quattro settimane. Consulta la nota.

Per ulteriori informazioni, consulta la sezione Prerequisiti.

Ho configurato Security Hub e AWS Config correttamente, ma i miei risultati non sono ancora disponibili

Possono essere necessarie fino a due ore prima che Security Hub abbia i risultati per le risorse. Potrebbero essere necessarie fino a 24 ore prima che i dati siano visualizzati della console Trusted Advisor. Controlla di nuovo la console Trusted Advisor più tardi.

> **Note**
>
> - Solo i tuoi risultati per i controlli negli standard di sicurezza AWS Foundational Security Best Practices verranno visualizzati in Trusted Advisor eccetto per i controlli con Categoria: Ripristino > Resilienza.
> - Se si verifica un problema di servizio con Security Hub o Security Hub non è disponibile, potrebbero essere necessarie fino a 24 ore prima che i risultati vengano visualizzati in Trusted Advisor. Controlla di nuovo la console Trusted Advisor più tardi.

Voglio disattivare controlli specifici Security Hub

Security Hub invia i tuoi dati a Trusted Advisor automaticamente. Se disabiliti un controllo Security Hub o non disponi più di risorse per quel controllo, i risultati non verranno visualizzati in Trusted Advisor.

Puoi effettuare l'accesso alla console Security Hub e verificare se il controllo è abilitato o disabilitato.

Se disabiliti un controllo Security Hub o tutti i controlli per lo standard di sicurezza AWS Foundational Security Best Practices, i risultati vengono archiviati entro i prossimi cinque giorni. Questo periodo di cinque giorni per l'archiviazione è approssimativo, è il risultato massimo e non è garantito. Quando i risultati sono stati archiviati, vengono rimossi da Trusted Advisor.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Disabilitazione e abilitazione dei controlli individuali
- Disabilitazione o abilitazione di uno standard di sicurezza

Desidero trovare le risorse di Security Hub escluse

Dalla console Trusted Advisor è possibile scegliere il nome del controllo di Security Hub e quindi scegliere l'opzione Elementi esclusi. Questa opzione visualizza tutte le risorse che vengono eliminate in Security Hub.

Se lo stato del flusso di lavoro per una risorsa è impostato su `SUPPRESSED`, quella risorsa è un elemento escluso in Trusted Advisor. Non è possibile sopprimere le risorse di Security Hub dalla console Trusted Advisor. A tale scopo, utilizzare la console Security Hub. Per ulteriori informazioni, consulta Impostazione dello stato del flusso di lavoro per i risultati.

Desidero abilitare o disabilitare questa caratteristica per un account membro appartenente a un'organizzazione AWS

Per impostazione predefinita, gli account membri ereditano la caratteristica dall'account di gestione per AWS Organizations. Se l'account di gestione ha abilitato la caratteristica, anche tutti gli account dell'organizzazione avranno la caratteristica. Se si dispone di un account membro e si desidera apportare modifiche specifiche al proprio account, contattare AWS Support.

Visualizzo molteplici Regioni AWS per la stessa risorsa interessata per la verifica Security Hub

Alcuni Servizi AWS sono globali e non sono specifici per una regione, come IAM e Amazon CloudFront. Per impostazione predefinita, le risorse globali come bucket Amazon S3 appariranno nella regione Stati Uniti orientali (Virginia settentrionale).

Per i controlli Security Hub che valutano le risorse per i servizi globali, è possibile che venga visualizzato più di un elemento per le risorse interessate. Ad esempio, se il controllo `Hardware MFA should be enabled for the root user` identifica che il tuo account non ha attivato questa funzione, vedrai più regioni nella tabella per la stessa risorsa.

Puoi configurare Security Hub e AWS Config in modo che non vengano visualizzate più regioni per la stessa risorsa. Per ulteriori informazioni, consulta AWS i controlli di Foundational Best Practices che potrebbe essere necessario disabilitare.

Ho disattivato Security Hub o AWS Config in una regione

Se interrompi la registrazione della risorsa con AWS Config o disabiliti Security Hub in una Regione AWS, Trusted Advisor non riceve più alcun dato per i controlli in tale regione. Trusted Advisor rimuove i risultati di Security Hub entro 7-9 giorni. Questo lasso di tempo è il risultato massimo e non è garantito. Per ulteriori informazioni, consulta Disabilitazione di Security Hub.

Per disabilitare questa caratteristica per il tuo account, consulta Disabilitare Security Hub da Trusted Advisor.

Il mio controllo è archiviato in Security Hub ma visualizzo ancora i risultati in Trusted Advisor

Quando lo stato di `RecordState` diventa `ARCHIVED` per un risultato, Trusted Advisor elimina il risultato per tale controllo Security Hub dal tuo account. Puoi ancora visualizzare il risultato in Trusted Advisor per 7-9 giorni prima che venga eliminato. Questo lasso di tempo è il risultato massimo e non è garantito.

Non riesco ancora a visualizzare i risultati del mio Security Hub

Se ci sono ancora problemi con questa caratteristica, puoi creare una richiesta di supporto tecnico nel Centro AWS Support.

Attiva AWS Compute Optimizer i Trusted Advisor controlli

Compute Optimizer è un servizio che analizza i parametri di configurazione e di utilizzo delle risorse AWS . Questo servizio segnala se le risorse sono configurate correttamente per garantire efficienza e affidabilità. Suggerisce inoltre miglioramenti che è possibile implementare per migliorare le prestazioni del carico di lavoro. Con Compute Optimizer, visualizzi gli stessi consigli nei tuoi controlli. Trusted Advisor

Puoi attivare Account AWS solo il tuo account membro o tutti gli account membri che fanno parte di un'organizzazione. AWS Organizations Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS Compute Optimizer .

Una volta che si è eseguito la iscrizione per Compute Optimizer, i seguenti controlli ricevono i dati dalle funzioni Lambda e dai volumi Amazon EBS. Potranno essere necessarie fino a 12 ore affinché i risultati e i consigli di ottimizzazione generino risultati. Possono quindi essere necessarie fino a 48 ore Trusted Advisor per visualizzare i risultati dei seguenti controlli:

Ottimizzazione dei costi

- Volumi Amazon EBS con provisioning eccessivo
- AWS Lambda funzioni sovradimensionate per le dimensioni della memoria

Prestazioni

- Volumi Amazon EBS con provisioning insufficiente
- AWS Lambda funzioni con dotazione insufficiente per le dimensioni della memoria

> **Note**
>
> - I risultati di questi controlli vengono aggiornati automaticamente più volte al giorno. Le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questi controlli.
> - Trusted Advisor dispone già dei controlli Amazon EBS Volumes sottoutilizzati e Amazon EBS Magnetic Volumes sovrautilizzati.

Una volta effettuato la iscrizione al Compute Optimizer, si consiglia di utilizzare invece i nuovi controlli dei volumi Amazon EBS con provisioning eccessivo e dei volumi Amazon EBS con provisioning insufficiente.

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

- Visualizzazione dei consigli sui volumi Amazon EBS nella Guida per l'utente di AWS Compute Optimizer
- Visualizzazione dei consigli sulle funzioni Lambda nella Guida per l'utente di AWS Compute Optimizer
- Configurazione della memoria delle funzioni Lambda nella Guida per gli sviluppatori di AWS Lambda
- Richiedi modifiche ai tuoi volumi Amazon EBS nella Amazon EC2 User Guide

Nozioni di base su AWS Trusted Advisor Priority

Trusted Advisor Priority ti aiuta a proteggere e ottimizzare il tuo Account AWS per seguire meglio le best practice di AWS. Con Trusted Advisor Priority, il team del tuo Account AWS può monitorare in modo proattivo il tuo account e generare suggerimenti prioritari quando identificano opportunità per te.

Il team del tuo account, ad esempio, può stabilire se il tuo account utente root AWS non dispone dell'autenticazione a più fattori (MFA). Il team del tuo account può creare un suggerimento in modo da consentirti di agire immediatamente su un controllo, ad esempio `MFA on Root Account`. Il suggerimento viene visualizzato come un suggerimento prioritario attivo sulla pagina di Trusted Advisor Priority della console Trusted Advisor. Dopodiché, puoi seguire i suggerimenti per risolverlo.

I suggerimenti di Trusted Advisor Priority possono provenire dalle seguenti due origini:

- Servizi AWS: servizi come Trusted Advisor, AWS Security Hub e AWS Well-Architected creano automaticamente suggerimenti. Il team del tuo account condivide questi suggerimenti con te in modo che vengano visualizzati in Trusted Advisor Priority.
- Il team del tuo account: il team del tuo account può creare suggerimenti manuali.

Trusted Advisor Priority ti aiuta a concentrarti sui suggerimenti più importanti. Tu e il team del tuo account potete tenere traccia del ciclo di vita dei suggerimenti, dal momento in cui il team ha condiviso il suggerimento fino al momento in cui lo riconoscete, risolvete o ignorate. Puoi utilizzare Trusted Advisor Priority per trovare suggerimenti per tutti gli account membri nella tua organizzazione.

Argomenti

Prerequisiti

Per utilizzare Trusted Advisor Priority, devi soddisfare i seguenti requisiti:

- devi disporre di un piano di supporto Enterprise.
- l'account deve far parte di un'organizzazione che abbia tutte le funzionalità abilitate in AWS Organizations. Per ulteriori informazioni, consulta la sezione Abilitazione di tutte le caratteristiche nell'organizzazione nella Guida per l'utente di AWS Organizations.
- L'organizzazione deve avere abilitato un accesso attendibile a Trusted Advisor. Per abilitare l'accesso attendibile, accedi con l'account di gestione. Apri la pagina La tua organizzazione nella console Trusted Advisor.
- Per visualizzare i suggerimenti di Trusted Advisor Priority per il tuo account, è necessario effettuare l'accesso all'account AWS.

- Per visualizzare i suggerimenti aggregati in tutta l'organizzazione, devi effettuare l'accesso all'account di gestione o all'account di amministratore delegato dell'organizzazione. Per istruzioni su come registrare gli account di amministratore delegato, consulta Registrazione degli amministratori delegati.
- È necessario disporre delle autorizzazione AWS Identity and Access Management (IAM) per accedere a Trusted Advisor Priority. Per ulteriori informazioni sul controllo dell'accesso a Trusted Advisor Priority, consulta Gestisci l'accesso a AWS Trusted Advisor e AWS politiche gestite per AWS Trusted Advisor.

Abilitazione di Trusted Advisor Priority.

Chiedi al team del tuo account di abilitare automaticamente questa funzionalità. È necessario disporre di un piano di supporto Enterprise ed essere il proprietario dell'account di gestione dell'organizzazione. Se la pagina di Trusted Advisor Priority nella console ti informa che è necessario un accesso attendibile con AWS Organizations, seleziona Abilita accesso attendibile con AWS Organizations. Per ulteriori informazioni, consulta la sezione Prerequisiti.

Visualizzare i suggerimenti prioritari

Dopo che il team del tuo account ha abilitato automaticamente Trusted Advisor Priority per tuo conto, puoi visualizzare i consigli più recenti per il tuo account AWS.

Come visualizzare i suggerimenti prioritari

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Sulla pagina Trusted Advisor Priority puoi visualizzare i seguenti elementi:

   Se utilizzi un account di gestione o di amministratore delegato AWS Organizations, passa alla scheda Il mio account.

   - Azioni necessarie: il numero di suggerimenti in attesa di risposta o in corso.
   - Overview (Panoramica): le informazioni riportate di seguito.
     - Suggerimenti ignorati negli ultimi 90 giorni
     - Suggerimenti rifiutati negli ultimi 90 giorni
     - Suggerimenti senza aggiornamento da oltre 30 giorni
     - Tempo medio di risoluzione dei suggerimenti

3. Nella scheda Attivo, Suggerimenti attivi prioritari mostra i suggerimenti ai quali il team del tuo account ha assegnato automaticamente la priorità. La scheda Chiuso mostra i suggerimenti risolti o ignorati.

   - Per filtrare i risultati, utilizza le seguenti opzioni:

     - Recommendation (Suggerimento): inserisci parole chiave per cercare in base al nome. Può trattarsi di un nome di controllo o di un nome personalizzato creato dal team del tuo account.
     - Stato: se il suggerimento è in attesa di una risposta, in corso, ignorato o risolto.
     - Fonte: l'origine di una raccomandazione prioritaria. I suggerimenti possono provenire da Servizi AWS, il team del tuo Account AWS o un evento di assistenza pianificato.
     - Categoria: la categoria di suggerimenti, come la sicurezza o l'ottimizzazione dei costi.
     - Age (Periodo/data): quando il team del tuo account ha condiviso il suggerimento con te.

4. Scegli un suggerimento per saperne di più sui dettagli, sulle risorse interessate e sulle azioni consigliate. È quindi possibile riconoscere o ignorare il suggerimento.

Visualizzazione dei consigli con priorità per tutti gli account della tua organizzazione AWS

Sia l'account di gestione che gli amministratori delegati di Trusted Advisor Priority possono visualizzare i consigli aggregati nella tua l'organizzazione.

> **Note**
>
> Gli account dei membri non hanno accesso ai suggerimenti aggregati.

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Priority, accedi alla scheda La mia organizzazione.
3. Per visualizzare i consigli per un account, seleziona un account dall'elenco a discesa Seleziona un account dalla tua organizzazione. In alternativa, puoi visualizzare i consigli per tutti i tuoi account.

   Sulla scheda La mia organizzazione puoi visualizzare i seguenti elementi:

- Azioni necessarie: il numero di suggerimenti nella tua organizzazione in attesa di risposta o in corso.
- Panoramica: mostra i seguenti elementi:

  - suggerimenti ignorati negli ultimi 90 giorni.

  - suggerimenti risolti negli ultimi 90 giorni.

  - suggerimenti senza aggiornamento da oltre 30 giorni.

  - tempo medio di risoluzione dei suggerimenti.

4. Nella scheda Attivo, la sezione Suggerimenti attivi prioritari mostra i suggerimenti ai quali il team del tuo account ha assegnato automaticamente la priorità. La scheda Chiuso mostra i suggerimenti risolti o ignorati.

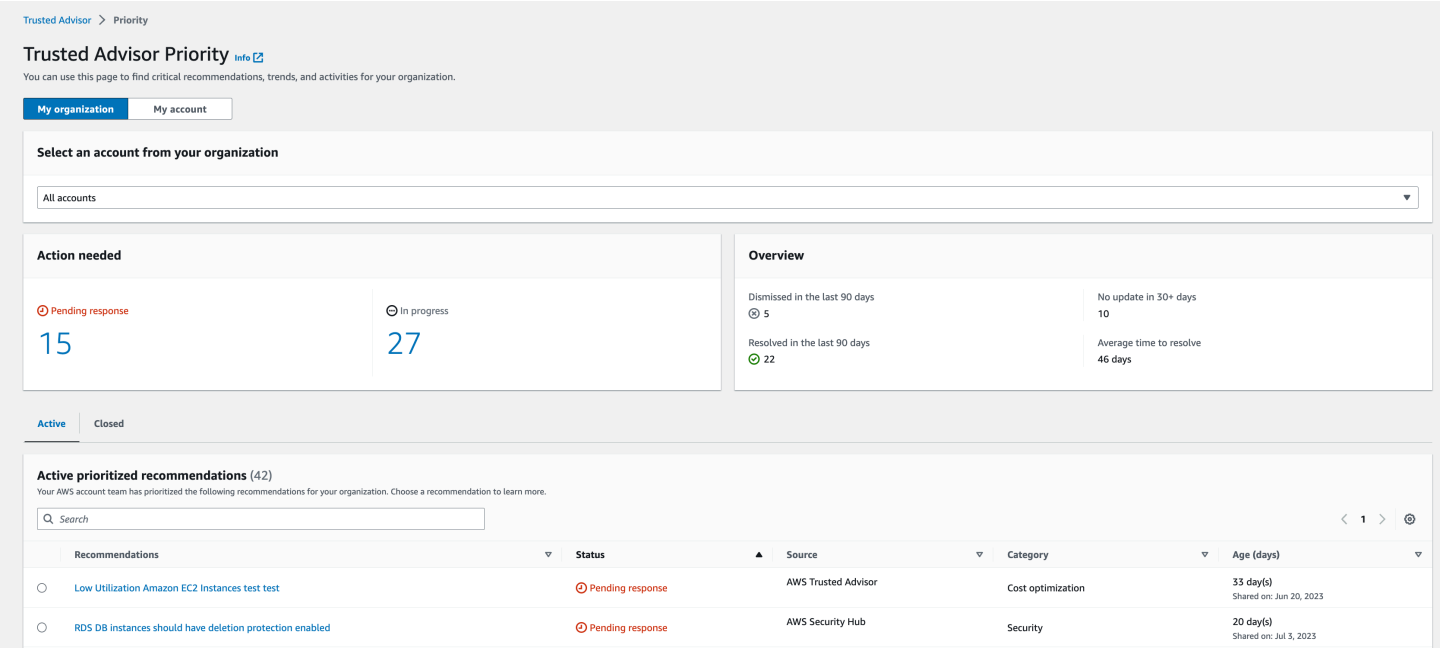
   Per filtrare i risultati, utilizza le seguenti opzioni:

   - Recommendation (Suggerimento): inserisci parole chiave per cercare in base al nome. Può trattarsi o di un nome di controllo o di un nome personalizzato creato dal team del tuo account.
   - Stato: se il suggerimento è in attesa di una risposta, in corso, ignorato o risolto.
   - Fonte: l'origine di una raccomandazione prioritaria. I suggerimenti possono provenire da Servizi AWS, il team del tuo Account AWS o un evento di assistenza pianificato.
   - Categoria: la categoria di suggerimenti, come la sicurezza o l'ottimizzazione dei costi.
   - Age (Periodo/data): quando il team del tuo account ha condiviso il suggerimento con te.

5. Scegli un suggerimento per vedere dettagli aggiuntivi, gli account e le risorse interessate, oltre alle azioni consigliate. È quindi possibile riconoscere o ignorare il suggerimento.

Example : suggerimenti di Trusted Advisor Priority

L'esempio seguente mostra 15 suggerimenti in attesa di risposta e 27 suggerimenti in corso nella sezione Azione necessaria. L'immagine seguente mostra due dei suggerimenti in attesa di risposta nella scheda Suggerimenti prioritari attivi.



Riconoscimento di un suggerimento

Nella scheda Attivo, puoi trovare maggiori informazioni sul suggerimento e poi decidere se riconoscerlo.

Riconoscere un suggerimento

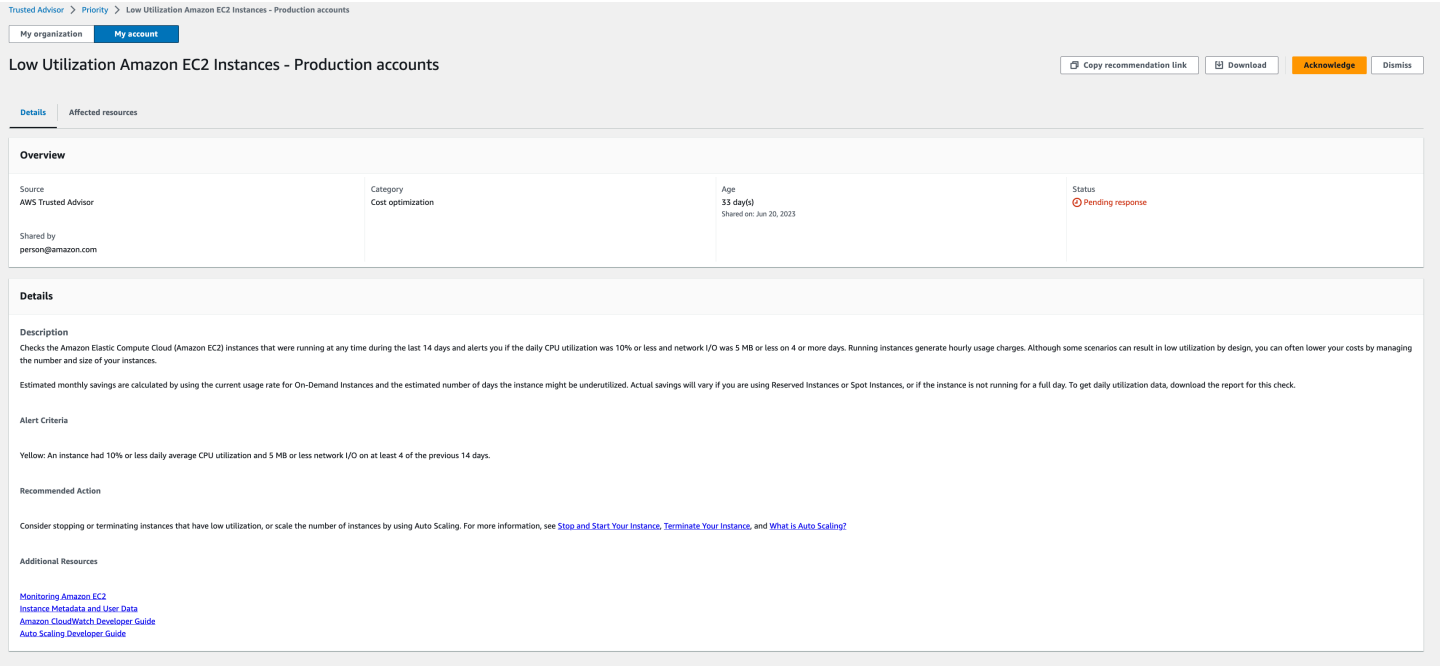
1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Se utilizzi un account di gestione o di amministratore delegato di AWS Organizations, passa alla scheda Il mio account.
3. Nella pagina di Trusted Advisor Priority, nella scheda Active (Attivo), scegli il nome di un suggerimento.
4. Nella sezione Dettagli, puoi esaminare le azioni consigliate per risolvere il suggerimento.
5. Nella sezione Risorse interessate, puoi esaminare le risorse interessate e filtrarle in base allo Stato.
6. Scegli Riconosci.
7. Nella finestra di dialogo Riconosci suggerimento, scegli Riconosci.

   Lo stato del suggerimento cambia in In progress (in corso). I suggerimenti in corso o in attesa di risposta vengono visualizzati nella scheda Active (Attivo) sulla pagina di Trusted Advisor Priority.

8. Segui le azioni consigliate per risolvere il suggerimento. Per ulteriori informazioni, consulta Risolvere un suggerimento.

Example : suggerimento manuale da Trusted Advisor Priority

L'immagine seguente mostra un suggerimento sulle Istanze EC2 con utilizzo ridotto che è in attesa di risposta.



Conferma di un suggerimento per tutti gli account della tua organizzazione AWS

L'account di gestione o gli amministratori delegati di Trusted Advisor possono confermare un suggerimento per tutti gli account interessati.

> **Note**
>
> Gli account dei membri non hanno accesso ai suggerimenti aggregati.

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Priority, accedi alla scheda La mia organizzazione.
3. Nella scheda Attivo seleziona il nome di un suggerimento.
4. Scegli Riconosci.

5. Nella finestra di dialogo Riconosci suggerimento, scegli Riconosci.

   Lo stato del suggerimento cambia in In progress (in corso).

6. Segui le azioni consigliate per risolvere il suggerimento. Per ulteriori informazioni, consulta Risolvere un suggerimento.

7. Per visualizzare i dettagli del suggerimento, scegli il nome del suggerimento.

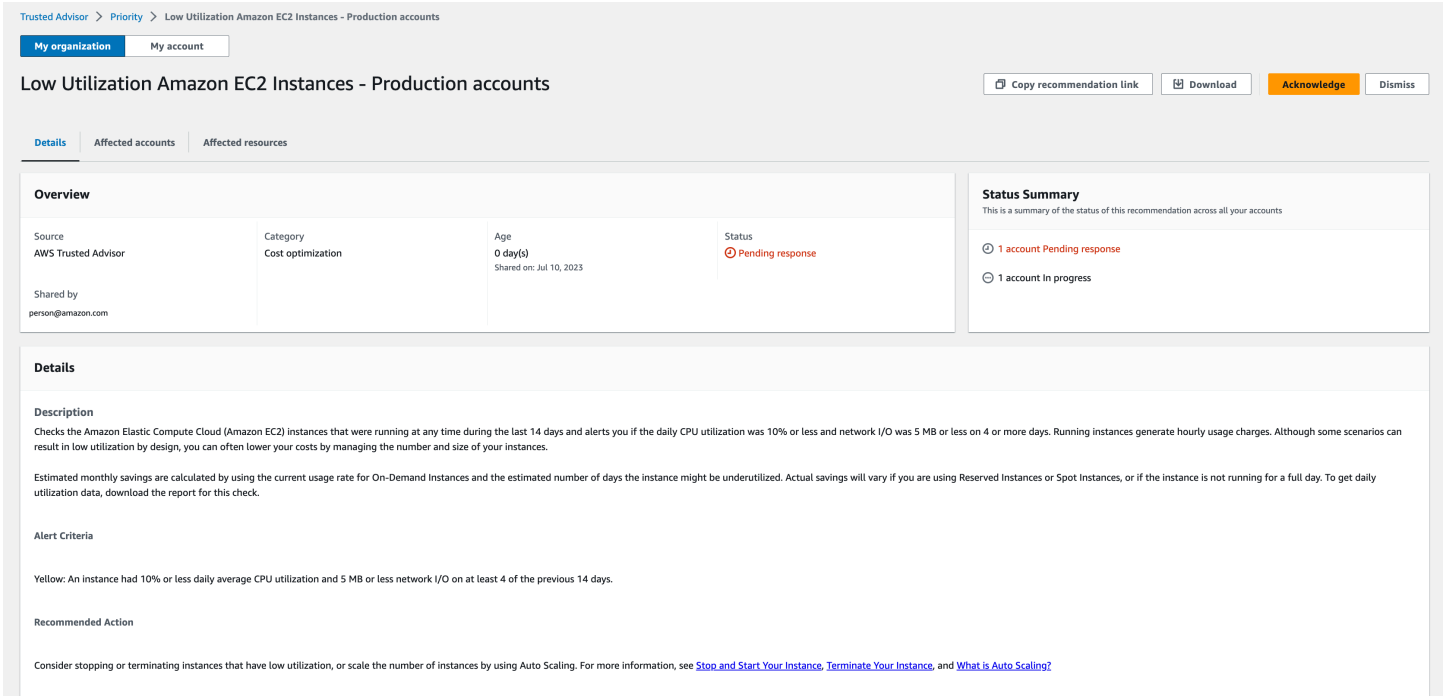
   Nella sezione Dettagli, puoi esaminare le seguenti informazioni sul suggerimento:

   - Una Panoramica del suggerimento e una sezione Dettagli che descrive le azioni consigliate.

     Un Riepilogo dello stato che mostra i suggerimenti per tutti gli account interessati.
   - Nella sezione Account interessati puoi esaminare le risorse interessate di tutti i tuoi account. Puoi filtrare in base al Numero di account e allo Stato.
   - Nella sezione Risorse interessate, puoi esaminare le risorse interessate di tutti i tuoi account. Puoi filtrare in base al Numero di account e allo Stato.

Example : suggerimento manuale da Trusted Advisor Priority

L'immagine seguente mostra il suggerimento sulle Istanze di Amazon EC2 con utilizzo ridotto che è in attesa di risposta. Un account interessato ha accettato il suggerimento. Un altro account è in attesa di risposta, quindi viene impostato lo stato del suggerimento In attesa di risposta.



Ignorare un suggerimento

Puoi anche ignorare un suggerimento. Ciò significa che riconosci il suggerimento, ma non lo segui. Puoi ignorare un suggerimento se non è rilevante per il tuo account. Ad esempio, se hai un test Account AWS che intendi eliminare, non devi seguire le azioni consigliate.

Ignorare un suggerimento

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Se utilizzi un account di gestione o di amministratore delegato di AWS Organizations, passa alla scheda Il mio account.
3. Nella pagina di Trusted Advisor Priority, nella scheda Active (Attivo), scegli il nome di un suggerimento.
4. Nella pagina dei dettagli del suggerimento, esamina le informazioni sulle risorse interessate.
5. Se questo suggerimento non si applica al tuo account, scegli Ignora.
6. Nella finestra di dialogo Ignora suggerimento, seleziona un motivo per cui non seguirai al suggerimento.
7. (Facoltativo) Inserisci una nota che descriva il motivo per cui stai ignorando il suggerimento. Se scegli Altro, devi inserire una descrizione nella sezione Nota.
8. Scegli Ignora. Lo stato del suggerimento diventa Ignorato e appare nella scheda Chiuso nella pagina di Trusted Advisor Priority.

Ignorare un suggerimento per tutti gli account della tua organizzazione AWS

L'account di gestione o l'amministratore delegato di Trusted Advisor Priority possono ignorare un suggerimento per tutti i loro account.

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina di Trusted Advisor Priority, accedi alla scheda La mia organizzazione.
3. Nella scheda Attivo, seleziona il nome di un suggerimento.
4. Se questo suggerimento non si applica al tuo account, seleziona Ignora.
5. Nella finestra di dialogo Ignora suggerimento, seleziona un motivo per cui non seguirai al suggerimento.

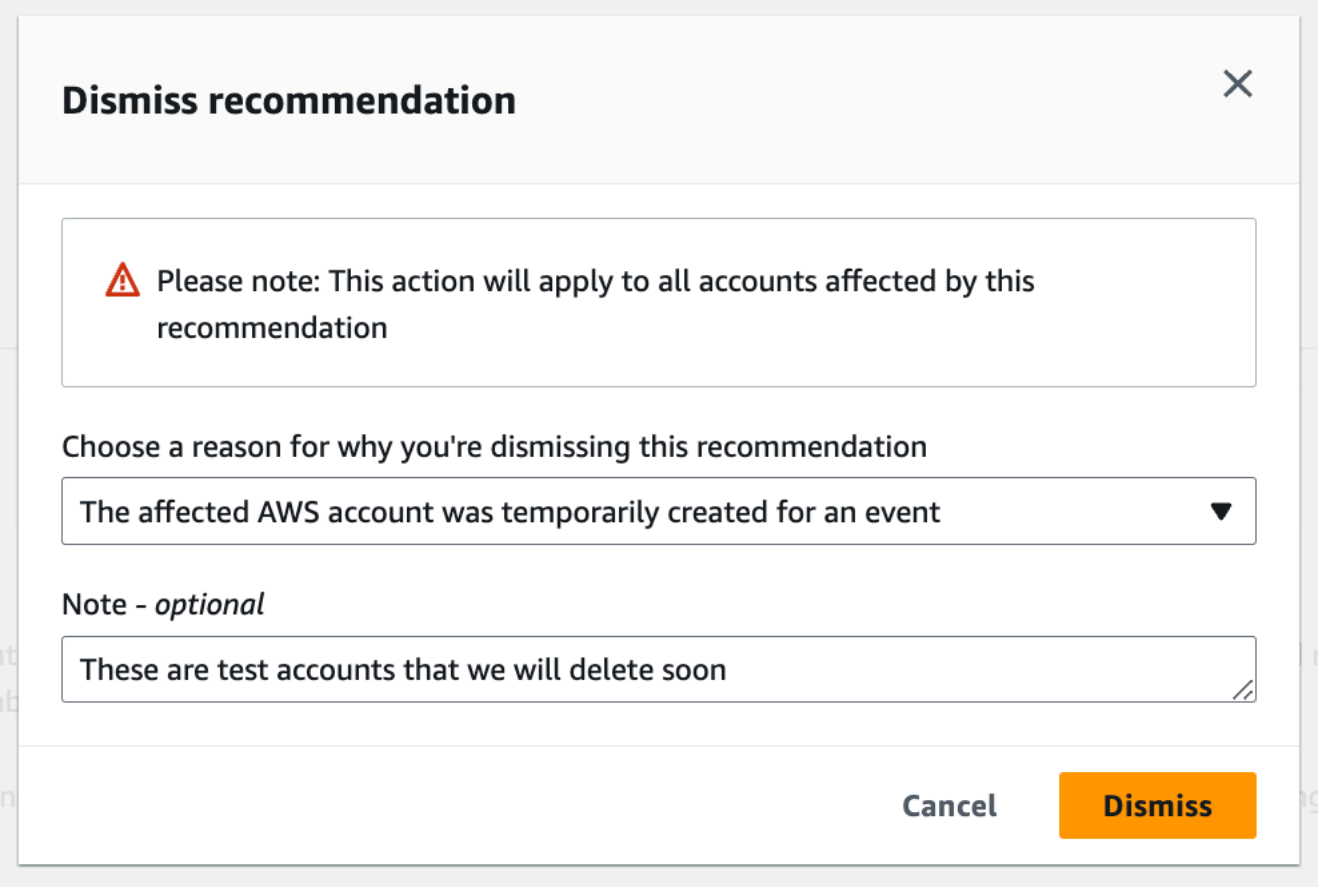
6. (Facoltativo) Inserisci una nota che descriva il motivo per cui stai ignorando il suggerimento. Se selezioni Altro, devi inserire una descrizione nella sezione Nota.
7. Scegli Ignora. Lo stato del suggerimento cambia diventando Ignorato. Lo stato del suggerimento viene visualizzato nella scheda Chiuso nella pagina di Trusted Advisor Priority.

> **Note**
>
> Puoi scegliere il nome del suggerimento e Visualizza nota per trovare il motivo per cui hai deciso di ignorarlo. Se il team del tuo account ha ignorato il suggerimento per te, il loro indirizzo email viene visualizzato accanto alla nota.

Inoltre, Trusted Advisor Priority comunica al team del tuo account che hai ignorato il suggerimento.

Example : ignorare una raccomandazione di Trusted Advisor Priority

L'esempio seguente mostra in che modo è possibile ignorare un suggerimento.



Risolvere un suggerimento

Dopo aver riconosciuto il suggerimento e completato le azioni consigliate, puoi risolvere il suggerimento.

> **Tip**
>
> Dopo avere risolto un suggerimento, non è possibile riaprirlo. Se desideri rivedere il suggerimento in un secondo momento, consulta Ignorare un suggerimento.

Come risolvere un suggerimento

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina di Trusted Advisor Priority, accedi alla scheda La mia organizzazione.
3. Sulla pagina Trusted Advisor Priority, seleziona il suggerimento, quindi scegli Resolve (risolvi).
4. Nella finestra di dialogo Risolvi suggerimento, scegli Risolvi. I suggerimenti risolti vengono visualizzati nella scheda Closed (Chiuso) della pagina di Trusted Advisor Priority. Trusted Advisor Priority comunica al team del tuo account che hai risolto il suggerimento.

Risoluzione di un suggerimento per tutti gli account della tua organizzazione AWS

L'account di gestione o gli amministratori delegati di Trusted Advisor Priority possono risolvere un suggerimento per tutti i loro account.

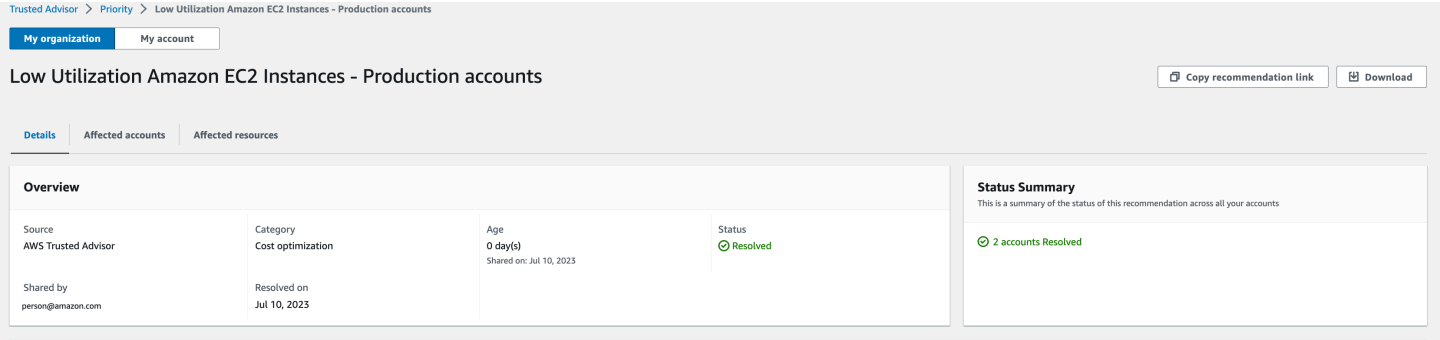
> **Note**
>
> Gli account dei membri non hanno accesso ai suggerimenti aggregati.

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Se utilizzi un account di gestione o di amministratore delegato di AWS Organizations, passa alla scheda Il mio account.
3. Nella scheda Attivo, seleziona il nome di un suggerimento.

4. Se questo suggerimento non si applica al tuo account, seleziona Risolvi.
5. Nella finestra di dialogo Risolvi suggerimento, scegli Risolvi. I suggerimenti risolti vengono visualizzati nella scheda Closed (Chiuso) della pagina di Trusted Advisor Priority. Trusted Advisor Priority comunica al team del tuo account che hai risolto il suggerimento.

Example : suggerimento manuale da Trusted Advisor Priority

L'esempio seguente mostra il suggerimento risolto sulle Istanze di Amazon EC2 con utilizzo ridotto.



Riapertura di un suggerimento

Dopo avere ignorato un suggerimento, tu o il team del tuo account potete riaprire il suggerimento.

Come riaprire un suggerimento

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Se utilizzi un account di gestione o di amministratore delegato di AWS Organizations, passa alla scheda Il mio account.
3. Nella pagina di Trusted Advisor Priority, seleziona la scheda Closed (Chiuso).
4. In Suggerimenti chiusi, seleziona un suggerimento Ignorato, quindi scegli Riapri.
5. Nella finestra di dialogo Riapri suggerimento, descrivi il motivo per cui stai riaprendo il suggerimento.
6. Scegli Reopen (Riapri). Lo stato del suggerimento diventa In progress (In corso) e appare nella scheda Active (Attivo).

> **Tip**
>
> Puoi scegliere il nome del suggerimento e selezionare Visualizza nota per trovare il motivo per cui hai deciso di riaprirlo. Se il team del tuo account ha riaperto il suggerimento per te, il loro indirizzo email viene visualizzato accanto alla nota.

7. Segui i passaggi riportati nei dettagli del suggerimento.

Riapertura di un suggerimento per tutti gli account della tua organizzazione AWS

L'account di gestione o gli amministratori delegati di Trusted Advisor Priority possono riaprire un suggerimento per tutti i loro account.

> **Note**
>
> Gli account dei membri non hanno accesso ai suggerimenti aggregati.

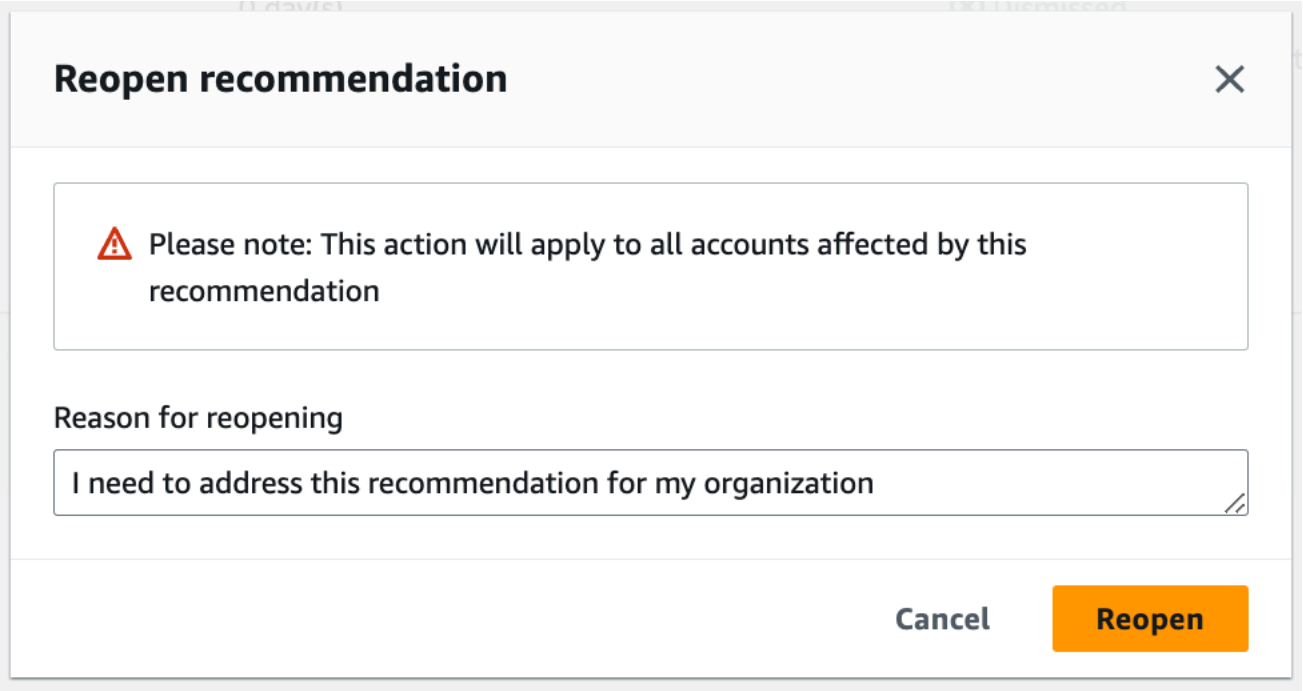
1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina di Trusted Advisor Priority, accedi alla scheda La mia organizzazione.
3. In Suggerimenti chiusi, seleziona un suggerimento Ignorato, quindi scegli Riapri.
4. Nella finestra di dialogo Riapri suggerimento, descrivi il motivo per cui stai riaprendo il suggerimento.
5. Scegli Reopen (Riapri). Lo stato del suggerimento diventa In progress (In corso) e appare nella scheda Active (Attivo).

> **Tip**
>
> Puoi scegliere il nome del suggerimento e Visualizza nota per trovare il motivo per cui hai deciso di riaprirlo. Se il team del tuo account ha riaperto il suggerimento per te, il loro indirizzo email viene visualizzato accanto alla nota.

6. Segui i passaggi riportati nei dettagli del suggerimento.

Example : riapertura di un suggerimento da Trusted Advisor Priority

L'esempio seguente mostra un suggerimento che desideri riaprire.



Scarica i dettagli sul suggerimento

È inoltre possibile scaricare i risultati di un suggerimento con Trusted Advisor Priority.

> **Note**
>
> Attualmente, puoi scaricare solo un suggerimento alla volta.

Come scaricare un suggerimento

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Sulla pagina Trusted Advisor Priority, seleziona il suggerimento, quindi scegli Download (scarica).
3. Apri il file per visualizzare i dettagli del suggerimento.

Registrazione degli amministratori delegati

Puoi aggiungere account membri che fanno parte dell'organizzazione come amministratori delegati. Gli account amministratori delegati possono esaminare, riconoscere, risolvere, ignorare e riaprire i suggerimenti in Trusted Advisor Priority.

Dopo la registrazione di un account, devi concedere all'amministratore delegato le autorizzazioni AWS Identity and Access Management necessarie per accedere a Trusted Advisor Priority. Per ulteriori informazioni, consultare Gestisci l'accesso a AWS Trusted Advisor e AWS politiche gestite per AWS Trusted Advisor.

Puoi registrare fino a cinque account membri. Solo l'account di gestione può aggiungere amministratori delegati per l'organizzazione. Per registrare o annullare la registrazione di un amministratore delegato, devi accedere all'account di gestione dell'organizzazione.

Come registrare un amministratore delegato

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home con l'account di gestione.
2. Nel riquadro di navigazione, in Preferences (Preferenze), scegli Your organization (La tua organizzazione).
3. In Delegated administrator (Amministratore delegato), scegli Register new account (Registra un nuovo account).
4. Nella finestra di dialogo immetti l'ID dell'account membro, quindi scegli Register (Registra).
5. (Facoltativo) Per annullare la registrazione di un account, selezionane uno e scegli Deregister (Annulla registrazione). Nella finestra di dialogo, scegli di nuovo Deregister (Annulla registrazione).

Annullamento della registrazione di amministratori delegati

Quando annulli la registrazione di un account membro, tale account non dispone più dell'accesso a Trusted Advisor Priority di cui dispone l'account di gestione. Gli account che non sono più amministratori delegati non riceveranno notifiche e-mail da Trusted Advisor Priority.

Come annullare la registrazione di un amministratore delegato

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home con l'account di gestione.

2. Nel riquadro di navigazione, in Preferences (Preferenze), scegli Your organization (La tua organizzazione).
3. Per la voce Amministratore delegato seleziona un account e scegli Annulla registrazione.
4. Nella finestra di dialogo, scegli Deregister (Annulla registrazione).

Gestione delle notifiche di Trusted Advisor Priority

Trusted Advisor Priority invia notifiche via e-mail. Questa notifica via e-mail include un riepilogo dei suggerimenti a cui il team del tuo account ha dato la priorità per te. È possibile specificare la frequenza con la quale ricevere aggiornamenti da Trusted Advisor Priority.

Se hai registrato degli account membri come amministratori delegati, anch'essi possono configurare i propri account per ricevere notifiche e-mail da Trusted Advisor Priority.

Le notifiche e-mail di Priorità Trusted Advisor non includono i risultati dei controlli per i singoli account e sono diverse dalla notifica settimanale per Consigli per Trusted Advisor. Per ulteriori informazioni, consulta Configura le preferenze di notifica.

> **Note**
>
> Solo l'account di gestione o l'amministratore delegato possono configurare le notifiche e-mail di Trusted Advisor Priority.

Come gestire le notifiche di Trusted Advisor Priority

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home con un account di gestione o di amministratore delegato.
2. Nel riquadro di navigazione, sotto Preferences (Preferenze), scegli Notifications (Notifiche).
3. In Priority è possibile selezionare le seguenti opzioni.

    a. Daily (Giornaliera): ricevi una notifica via e-mail ogni giorno.
    b. Weekly (Settimanale): ricevi una notifica via e-mail una volta alla settimana.
    c. Scegli le notifiche da ricevere:

        - Riepilogo dei suggerimenti prioritari
        - Date di risoluzione

4. Per la voce Destinatari, seleziona altri contatti a cui intendi inviare le notifiche e-mail. È possibile aggiungere ed eliminare contatti dalla pagina Impostazioni Account nella console AWS Billing and Cost Management.
5. In Language (Lingua), seleziona la lingua delle notifiche e-mail.
6. Scegli Save your preferences (Salva preferenze).

> **Note**
>
> Trusted Advisor Priority invia notifiche e-mail dall'indirizzo noreply@notifications.trustedadvisor.us-west-2.amazonaws.com. Potrebbe essere necessario verificare che il tuo client di posta elettronica non contrassegni queste e-mail come spam.

Disabilitare Trusted Advisor Priority.

Contatta il team responsabile del tuo account e chiedi di disabilitare questa opzione. Dopo la disattivazione di questa funzionalità, i suggerimenti prioritari non vengono più visualizzati nella console di Trusted Advisor.

Se disabiliti Trusted Advisor Priority e lo riabiliti in un secondo momento, potrai comunque possibile visualizzare i suggerimenti che il team del tuo account ha inviato prima della disabilitazione di Trusted Advisor Priority.

Nozioni di base di AWS Trusted Advisor Engage (anteprima)

> **Note**
>
> AWS Trusted Advisor Engage è disponibile nella versione di anteprima e soggetto a modifiche. Puoi consultare in anteprima i termini del servizio qui https://aws.amazon.com/service-terms/.

Puoi utilizzare AWS Trusted Advisor Engage per sfruttare al massimo i tuoi piani AWS Support semplificando la visualizzazione, le richieste e il monitoraggio di tutti i tuoi impegni attivi, nonché le comunicazioni con il tuo team Account AWS sugli impegni in corso.

Ad esempio, puoi chiedere una "Analisi delle attività di gestione" al tuo team Account AWS accedendo alla pagina Engage nella console AWS Trusted Advisor. In tal modo, un esperto AWS verrà assegnato alla tua richiesta e seguirà l'intero impegno.

Argomenti

Prerequisiti

Per poter utilizzare Trusted Advisor Engage, devi adottare le misure necessarie per soddisfare i seguenti requisiti:

- Devi disporre di un piano di supporto Enterprise On-Ramp.
- L'account deve far parte di un'organizzazione che abbia tutte le funzionalità abilitate in AWS Organizations. Per ulteriori informazioni, consulta la sezione Abilitazione di tutte le caratteristiche nell'organizzazione nella Guida per l'utente di AWS Organizations.
- L'organizzazione deve avere abilitato un accesso attendibile a Trusted Advisor. Puoi abilitare un accesso attendibile accedendo con l'account di gestione e aprendo la pagina La tua organizzazione nella console Trusted Advisor.
- Devi disporre delle autorizzazioni AWS Identity and Access Management (IAM) per accedere a Trusted Advisor Engage. Per ulteriori informazioni sul controllo dell'accesso a Trusted Advisor Engage, consulta Gestisci l'accesso a AWS Trusted Advisor.

> **Note**
>
> Qualsiasi account all'interno di un'organizzazione AWS può creare una richiesta di impegno. Se un account proprietario di un impegno viene trasferito in un'altra organizzazione AWS, l'impegno sarà accessibile solo dall'account. Per limitare i controlli, consulta Policy di controllo dei servizi di esempio per AWS Trusted Advisor.

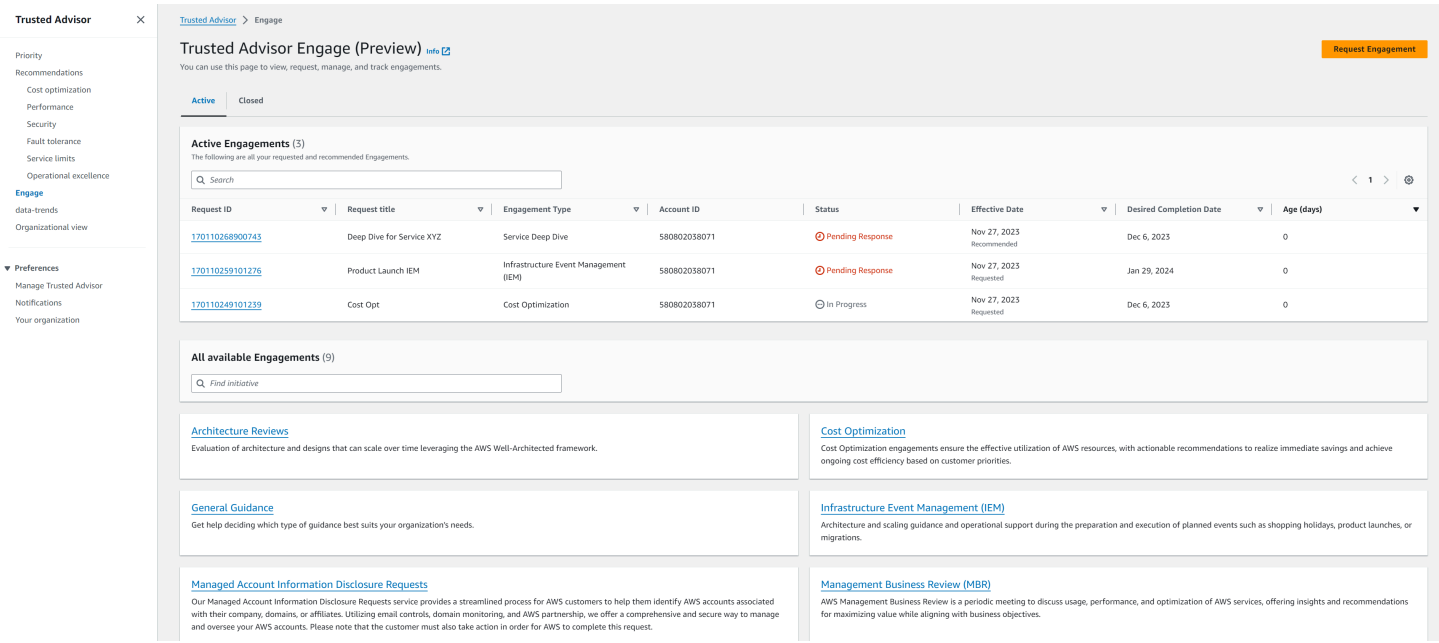
Visualizzazione del pannello di controllo degli impegni

Dopo aver ottenuto i diritti di accesso, puoi accedere alla pagina Trusted Advisor Engage nella console Trusted Advisor per visualizzare un pannello di controllo in cui gestire gli impegni con il tuo team Account AWS.

Per gestire i tuoi impegni:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage puoi visualizzare:
   - Pulsante Chiedi impegno
   - Tabella Impegni attivi
   - Tabella Impegni chiusi
   - Catalogo di Tutti gli impegni disponibili

Example : Pannello di controllo degli impegni



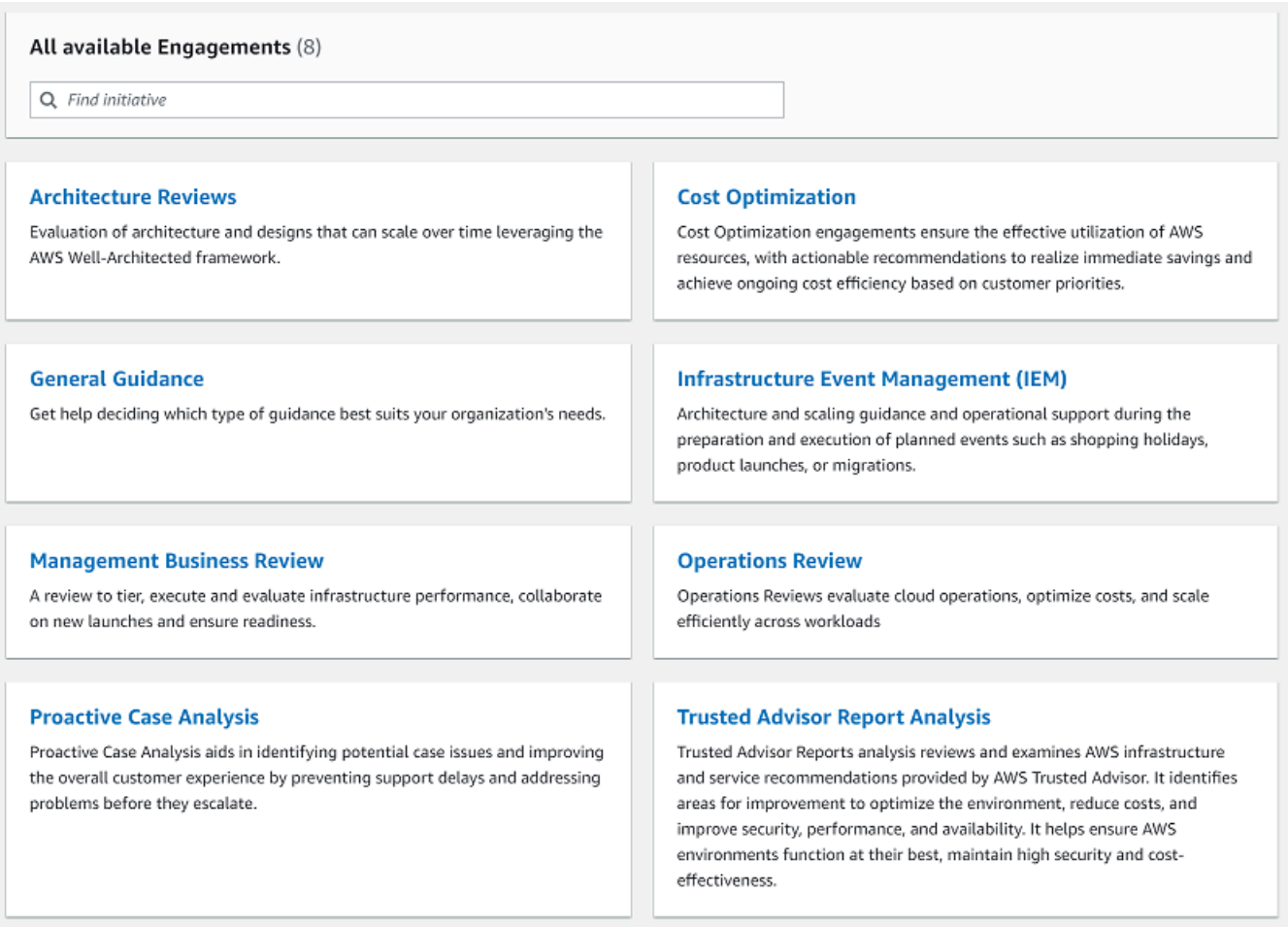
Visualizza il catalogo dei tipi di impegno

Puoi visualizzare il catalogo dei tipi di impegno per trovare i tipi di impegno più recenti che puoi chiedere al tuo team Account AWS.

Per visualizzare il catalogo dei tipi di impegno:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage, puoi trovare il catalogo dei tipi di impegno.

Example : Catalogo dei tipi di impegno



Richiesta di un impegno

Puoi chiedere impegni al tuo team Account AWS in base ai tipi di impegno presenti nel tuo piano di supporto AWS.

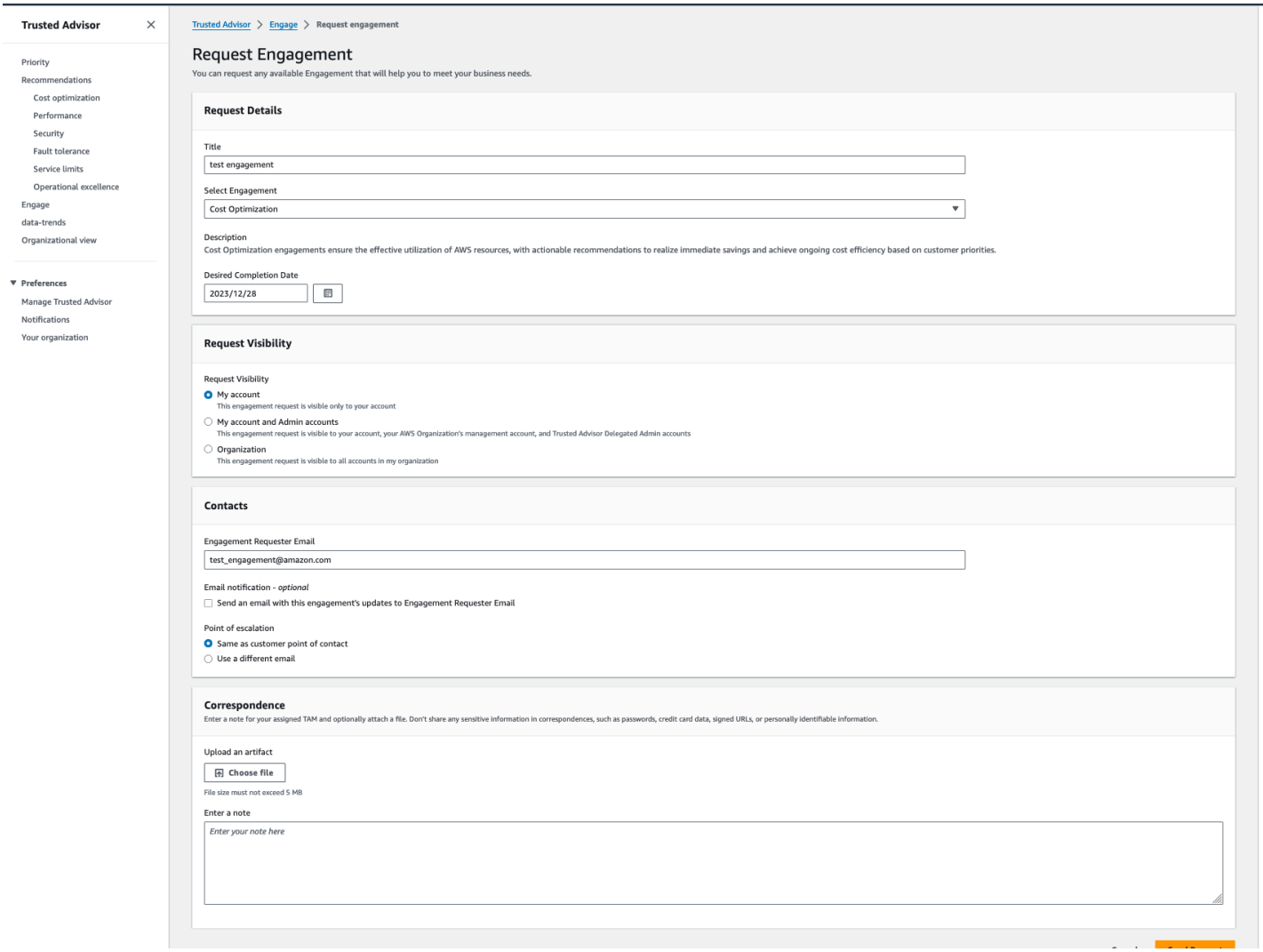
Per chiedere un impegno:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage, seleziona Chiedi impegno.
3. Compila i seguenti campi:
   - Titolo
   - Seleziona impegno: il tipo di impegno da chiedere.

- Data di completamento desiderata: la data di completamento desiderata dell'impegno. Ogni tipo di impegno ha una durata diversa, calcolata in base alla data di completamento minima desiderata.
- Chiedi visibilità:
  - Il mio account: questa richiesta di impegno è visibile solo al tuo account.
  - Il mio account e gli account di amministratori: questa richiesta di impegno è visibile al tuo account, all'account di gestione e a tutti gli account di amministratori delegati della tua organizzazione AWS.
  - Organizzazione: questa richiesta di impegno è visibile a tutti gli account della tua organizzazione AWS.
- E-mail del richiedente di coinvolgimento: l'indirizzo e-mail che AWS verrà utilizzato come punto di contatto principale per questo coinvolgimento.
- Impostazioni di notifica e-mail: scegli se l'Engagement Requester Email riceverà notifiche e-mail relative al coinvolgimento.
- Punto di escalation: l'indirizzo e-mail che AWS utilizzerà quando sarà necessaria un'escalation per questo impegno.
- Corrispondenza: una nota e un file allegato facoltativo per fornire dettagli relativi a questo impegno.

4. Seleziona Invia richiesta.

Example : Chiedi impegno



Modifica di un impegno

Puoi modificare i dettagli nella richiesta di impegno.

Come modificare un impegno:

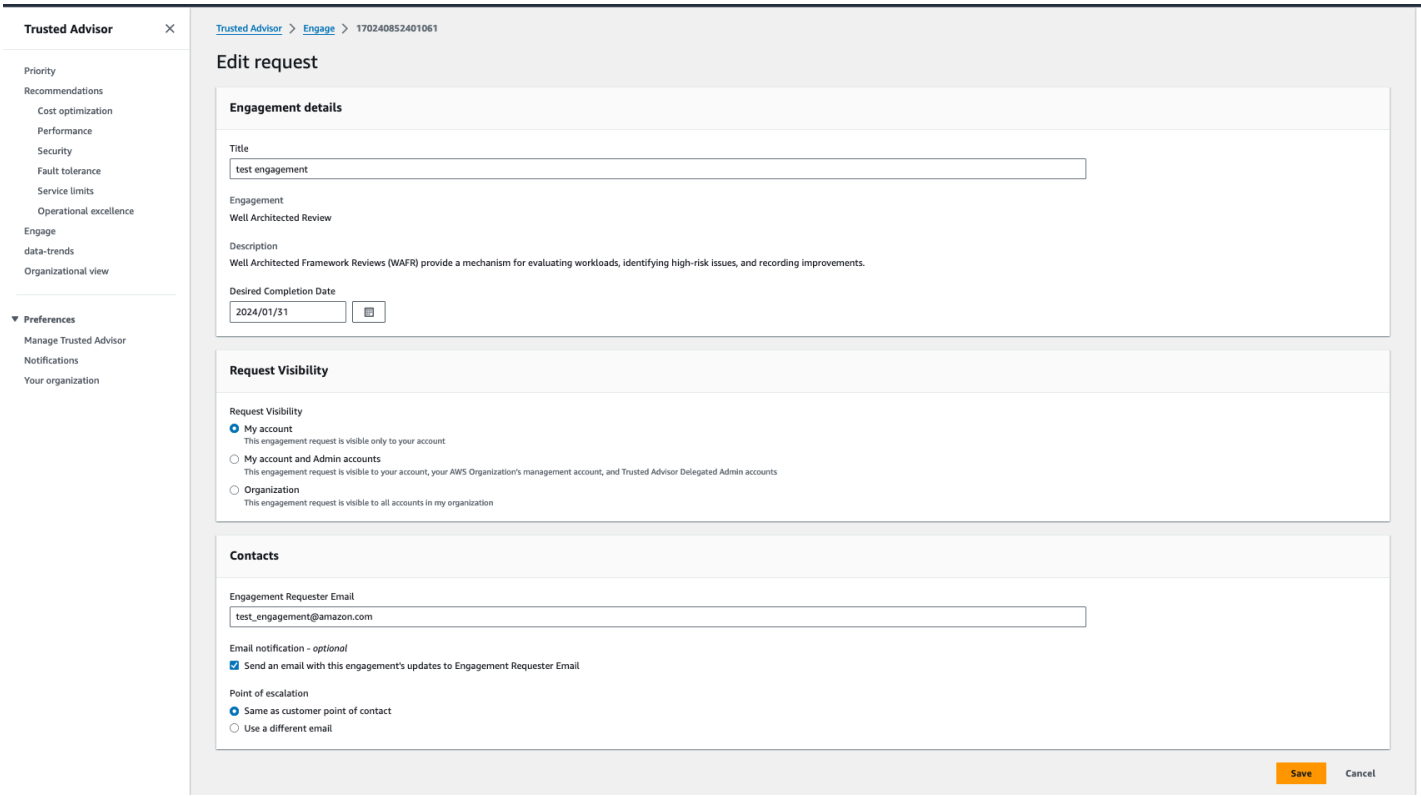
1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage, seleziona un impegno esistente.
3. Seleziona Edit (Modifica).
4. Puoi modificare i seguenti dati:

    - Titolo

- Data di completamento desiderata: la data di completamento desiderata dell'impegno. Ogni tipo di impegno ha una durata diversa, calcolata in base alla data di completamento minima desiderata.
- Chiedi visibilità:
  - Il mio account: questa richiesta di impegno è visibile solo al tuo account.
  - Il mio account e gli account di amministratori: questa richiesta di impegno è visibile al tuo account, all'account di gestione e a tutti gli account di amministratori delegati della tua organizzazione AWS.
  - Organizzazione: questa richiesta di impegno è visibile a tutti gli account della tua organizzazione AWS.
- Email del richiedente di coinvolgimento: l'indirizzo e-mail che AWS verrà utilizzato come punto di contatto principale per questo coinvolgimento.
- Impostazioni di notifica e-mail: scegli se l'Engagement Requester Email riceverà notifiche e-mail relative al coinvolgimento.
- Punto di escalation: l'indirizzo e-mail che AWS utilizzerà quando sarà necessaria un'escalation per questo impegno.

5. Selezionare Salva.

Example : Modifica impegno



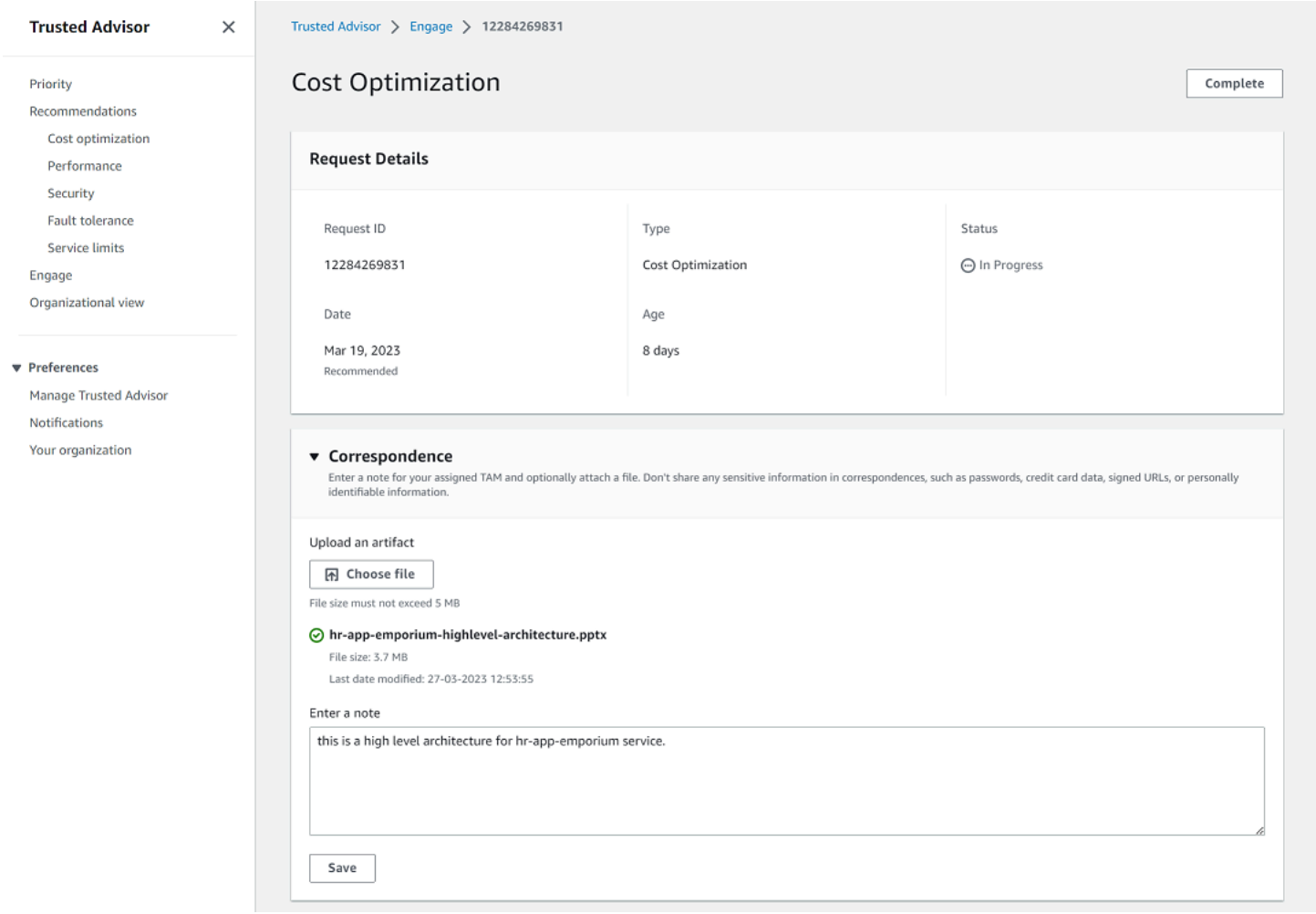
Invio di allegati e note

Puoi stabilire una comunicazione con il tuo team Account AWS in merito ai singoli impegni inviando note e file allegati a sostegno della tua richiesta di impegno. Puoi includere un solo allegato e una nota per comunicazione, puoi allegare file solo a un impegno con lo stesso Account AWS che ha chiesto l'impegno e non puoi eliminare allegati o note dopo l'invio di una comunicazione.

Per allegare file o aggiungere note a una richiesta di Impegno attivo:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage, seleziona l'ID dell'impegno attivo a cui allegare file o aggiungere note.
3. Seleziona Corrispondenza per espandere il modulo.
4. Inserisci una nota per il TAM assegnato e, facoltativamente, allega un file. Non condividere informazioni sensibili nelle corrispondenze, ad esempio password, dati di carte di credito, URL firmati o informazioni di identificazione personale.
5. Selezionare Salva.

Example : Aggiungi nota e allega file a un impegno



Modifica dello stato degli impegni

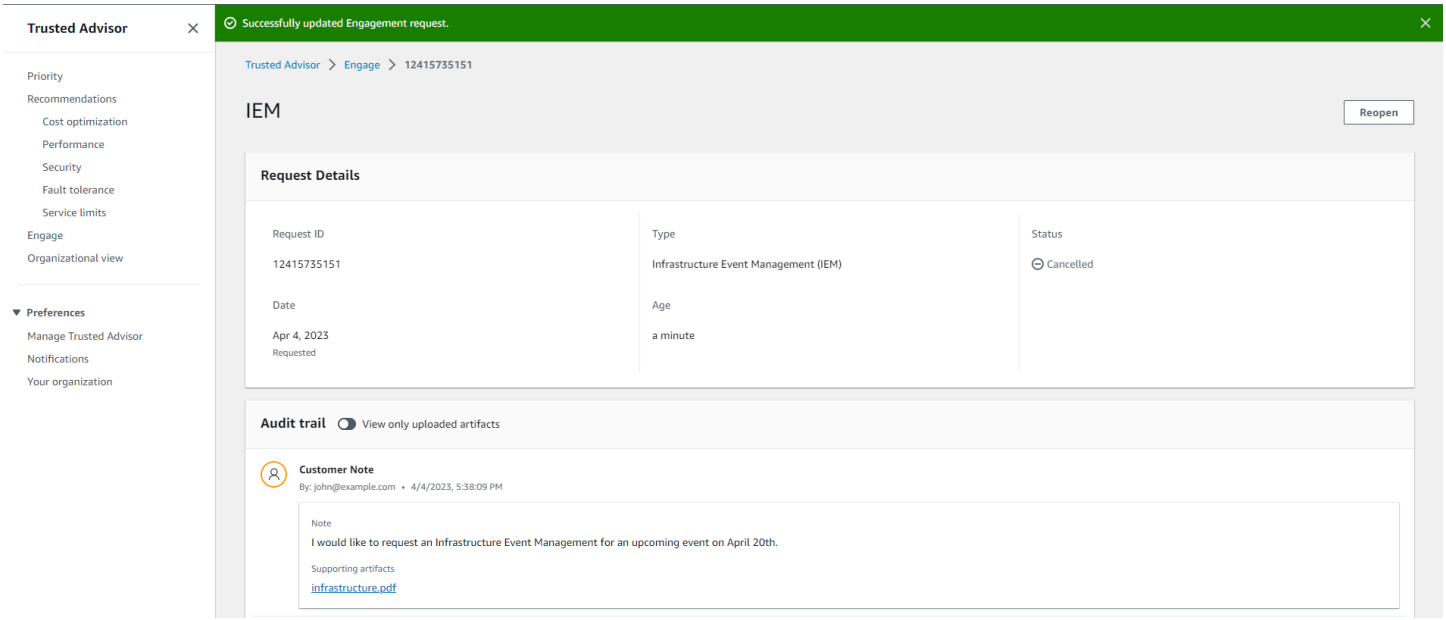
Puoi modificare lo stato degli impegni in modo da annullare gli impegni in attesa di risposta, completare gli impegni in corso e riaprire gli impegni contrassegnati come annullati o chiusi.

Per modificare lo stato di un impegno:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage, seleziona l'ID dell'impegno attivo di cui modificare lo stato.
3. Nella pagina dei dettagli dell'impegno, puoi modificare lo stato in Annullato o Completato.
   - Puoi selezionare Annulla quando lo stato dell'impegno è In attesa di risposta.
   - Puoi selezionare Completato quando lo stato dell'impegno è In corso.

- Puoi selezionare Riapri per gli impegni chiusi. Gli impegni annullati diventano In attesa di risposta, mentre gli impegni completati diventano In corso.

Example : Modifica lo stato di un impegno



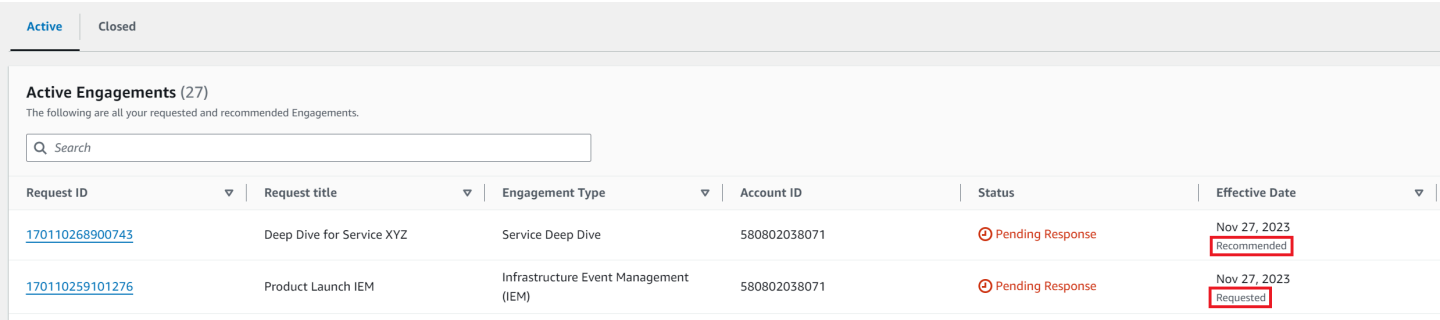
Distinzione tra impegni consigliati e impegni chiesti

Puoi identificare l'origine dell'impegno per appurare se un impegno è stato chiesto da te o consigliato dal team del tuo Account AWS.

Per visualizzare le diverse origini degli impegni attivi:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted AdvisorInteragisci, visualizza la colonna Data di validità per distinguere tra impegni consigliati e richiesti:
   - Consigliati: richiesta di impegno creata dai team del tuo Account AWS.
   - Chiesti: richiesta di impegno creata dall'utente.

Example : Distingui tra impegni consigliati e impegni chiesti



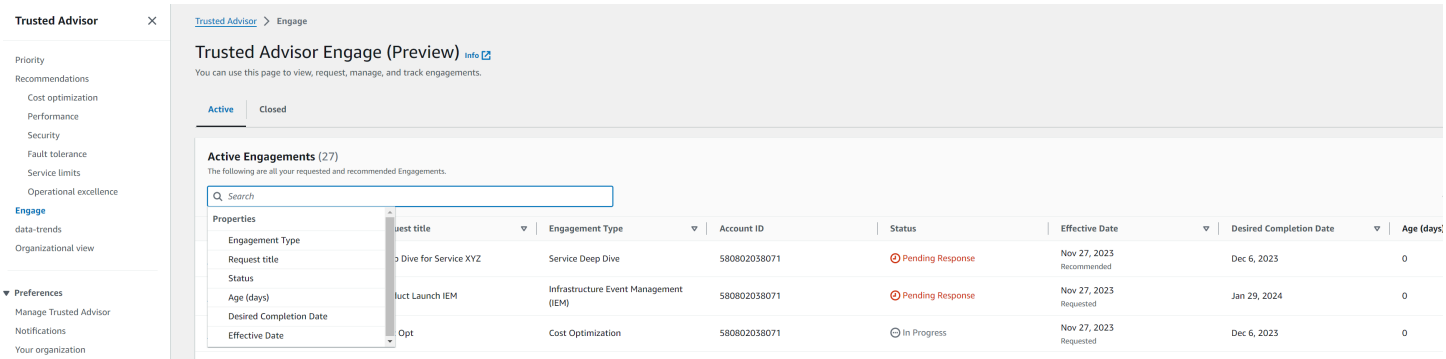
Ricerca di impegni

Puoi cercare gli attuali impegni attivi e chiusi utilizzando i filtri.

Per cercare impegni:

1. Accedi alla console Trusted Advisor all'indirizzo https://console.aws.amazon.com/trustedadvisor/home.
2. Nella pagina Trusted Advisor Engage, puoi selezionare uno dei seguenti filtri:
   - Età (giorni)
   - Tipo di impegno
   - Titolo della richiesta
   - Stato
   - Data di completamento desiderata
   - Data di validità

Example : Ccerca impegni



AWS Trusted Advisor verifica riferimento

È possibile Trusted Advisor visualizzare tutti i nomi, le descrizioni e gli ID degli assegni nel riferimento seguente. Puoi anche accedere alla console Trusted Advisor per visualizzare ulteriori informazioni sui controlli, le azioni consigliate e i relativi stati.

Se hai un piano di supporto Business, Enterprise On-Ramp o Enterprise, è possibile utilizzare anche l'API AWS Trusted Advisor e la AWS Command Line Interface (AWS CLI) per accedere ai controlli. Per ulteriori informazioni, consulta i seguenti argomenti:

- Inizia a usare l' Trusted Advisor API
- AWS Trusted Advisor Documentazione di riferimento delle API

> **Note**
>
> Se hai un piano di supporto Basic e Developer, puoi utilizzare la console Trusted Advisor per accedere a tutti i controlli nella categoria Limiti del servizio e i seguenti controlli nella categoria sicurezza:
>
> - Snapshot pubblici Amazon EBS
> - Snapshot pubblici di Amazon RDS
> - Autorizzazioni Bucket Amazon S3
> - MFA su Account Root
> - Gruppi di sicurezza — Porte specifiche senza restrizioni

Categorie di controllo

- Ottimizzazione dei costi
- Prestazioni
- Sicurezza
- Tolleranza ai guasti
- Limiti del servizio
- Eccellenza operativa

Ottimizzazione dei costi

Per la categoria di ottimizzazione dei costi, puoi utilizzare i seguenti controlli.

Controlla i nomi

- Account AWS che non fa parte di AWS Organizations
- Endpoint Amazon Comprehend sottoutilizzato
- Volumi Amazon EBS con provisioning eccessivo
- Consolidamento di istanze Amazon EC2 per Microsoft SQL Server
- Istanze Amazon EC2 con provisioning eccessivo per Microsoft SQL Server
- Istanze di Amazon EC2 interrotte
- Scadenza locazione istanze riservate Amazon EC2
- Ottimizzazione delle istanze riservate Amazon EC2
- Repository di Amazon ECR senza policy del ciclo di vita configurata
- Ottimizzazione dei nodi ElastiCache riservati Amazon
- Ottimizzazione delle istanze riservate di Amazon OpenSearch Service
- Istanze database Amazon RDS inattive
- Ottimizzazione dei nodi riservati Amazon Redshift
- Ottimizzazione dell'istanza riservata Amazon Relational Database Service (RDS)
- Set di registri delle risorse di latenza Amazon Route 53
- Policy del ciclo di vita dei bucket di Amazon S3 configurata
- Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3
- Bucket abilitati alla versione di Amazon S3 senza policy del ciclo di vita configurate
- AWS Lambda Funzioni con timeout eccessivi
- AWS Lambda Funzioni con elevati tassi di errore
- Funzioni AWS Lambda con provisioning eccessivo per la dimensione della memoria
- Problemi ad alto rischio di AWS Well-Architected per l'ottimizzazione dei costi
- Bilanciatori del carico inattivi
- Istanze Amazon EC2 con utilizzo ridotto
- Savings Plan

- Indirizzi IP elastici non associati
- Volumi Amazon EBS sottoutilizzati
- Cluster Amazon Redshift sottoutilizzati

Account AWS che non fa parte di AWS Organizations

Descrizione

Controlla se un account AWS fa parte di AWS Organizations nell'account di gestione appropriato.

AWS Organizations è un servizio di gestione degli account per aggregare più account AWS in un'organizzazione gestita a livello centralizzato. Ciò consente di strutturare a livello centralizzato gli account per aggregare le fatture e di implementare policy di proprietà e sicurezza con il progressivo dimensionamento dei carichi di lavoro su AWS.

È possibile specificare l'ID dell'account di gestione utilizzando il MasterAccountIdparametro delle AWS Config regole.

Per ulteriori informazioni, consulta Che cos'è AWS Organizations?

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz127`

Origine

`AWS Config Managed Rule: account-part-of-organizations`

Criteri di avviso

Giallo: questo account AWS non fa parte di AWS Organizations.

Operazione consigliata

Aggiungi questo account AWS come parte di AWS Organizations.

Per ulteriori informazioni, consulta il Tutorial: creazione e configurazione di un'organizzazione.

Colonne del report

- Stato
- Regione
- Risorsa
- Regola AWS Config
- Parametri di input
- Ora ultimo aggiornamento

Endpoint Amazon Comprehend sottoutilizzato

Descrizione

Controlla la configurazione della velocità effettiva degli endpoint. Questo controllo ti avvisa quando gli endpoint non vengono utilizzati attivamente per richieste di inference in tempo reale. Un endpoint che non viene utilizzato per più di 15 giorni consecutivi è considerato sottoutilizzato. Tutti gli endpoint accumulano addebiti in base alla velocità effettiva impostata, e il periodo di tempo in cui l'endpoint è attivo.

> **Note**
>
> Questo controllo viene aggiornato automaticamente una volta al giorno. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Cm24dfsM12`

Criteri di avviso

Giallo: l'endpoint è attivo, ma non è stato utilizzato per le richieste di inference in tempo reale negli ultimi 15 giorni.

Operazione consigliata

Se l'endpoint non è stato utilizzato negli ultimi 15 giorni, consigliamo di definire una policy di ridimensionamento per la risorsa utilizzando l'Applicazione Auto Scaling.

Se l'endpoint ha una policy di ridimensionamento definita e non è stato utilizzato negli ultimi 30 giorni, è consigliabile eliminarlo e utilizzare l'inference asincrona. Per ulteriori informazioni, consulta Eliminazione di un endpoint con Amazon Comprehend.

Colonne del report

- Stato
- Regione
- ARN endpoint
- Unità di inference fornita in provisioning
- AutoScaling Stato
- Motivo
- Ora ultimo aggiornamento

Volumi Amazon EBS con provisioning eccessivo

Descrizione

Controlla i volumi Amazon Elastic Block Store (Amazon EBS) in esecuzione in qualsiasi momento durante il periodo di ricerca posticipata. Questo controllo avvisa se alcuni volumi EBS sono stati sottoposti a provisioning eccessivo per i carichi di lavoro. Quando si hanno volumi con provisioning eccessivo, si pagano le risorse inutilizzate. Sebbene alcuni scenari possano comportare un'ottimizzazione ridotta in base alla progettazione, spesso è possibile ridurre i costi modificando la configurazione dei volumi EBS. I risparmi mensili stimati vengono calcolati utilizzando il tasso di utilizzo corrente per i volumi EBS. I risparmi effettivi variano se il volume non è presente per un mese intero.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`C0r6dfpM03`

Criteri di avviso

Giallo: un volume EBS sottoposto a provisioning eccessivo durante il periodo di ricerca posticipata. Per determinare se un volume è sovradimensionato, prendiamo in considerazione tutte le CloudWatch metriche predefinite (inclusi IOPS e throughput). L'algoritmo utilizzato per identificare i volumi EBS sottoposti a provisioning eccessivo segue le best practice AWS. L'algoritmo viene aggiornato quando viene identificato un nuovo modello.

Operazione consigliata

Valuta la possibilità di ridimensionare i volumi con un utilizzo ridotto.

Per ulteriori informazioni, consulta Attiva AWS Compute Optimizer i Trusted Advisor controlli.

Colonne del report

- Stato
- Regione
- ID volume
- Tipo di volume
- Dimensioni volume
- Volume IOPS di base
- Volume IOPS moderato
- Volume velocità di trasmissione effettiva moderata
- Tipo di volume consigliato
- Dimensione volume consigliata (GB)
- Volume IOPS di base consigliato
- Volume IOPS moderata consigliato
- Volume velocità di trasmissione effettiva di base consigliato
- Volume velocità di trasmissione effettiva moderata consigliato
- Periodo di ricerca posticipata (giorni)
- Opportunità di risparmio (%)

- Risparmi mensili stimati
- Valuta dei risparmi mensili stimati
- Ora ultimo aggiornamento

Consolidamento di istanze Amazon EC2 per Microsoft SQL Server

Descrizione

Verifica le istanze Amazon Elastic Compute Cloud (Amazon EC2) che hanno eseguito SQL Server nelle ultime 24 ore. Questo controllo avvisa se l'istanza ha un numero inferiore al minimo di licenze SQL Server. In base alla Guida alle licenze per Microsoft SQL Server, stai pagando 4 licenze vCPU anche se un'istanza ha solo 1 o 2 vCPU. Puoi consolidare istanze SQL Server più piccole per ridurre i costi.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Qsdfp3A4L2`

Criteri di avviso

Giallo: un'istanza con SQL Server ha meno di 4 vCPU.

Operazione consigliata

Valuta la possibilità di consolidare carichi di lavoro SQL Server più piccoli in istanze con almeno 4 vCPU.

Risorse aggiuntive

- Microsoft SQL Server in AWS
- Licenze per Microsoft in AWS
- Guida alle licenze per Microsoft SQL Server

Colonne del report

- Stato
- Regione
- ID istanza
- Tipo di istanza
- VPCU
- vCPU minima
- SQL Server Edition
- Ora ultimo aggiornamento

Istanze Amazon EC2 con provisioning eccessivo per Microsoft SQL Server

Descrizione

Verifica le istanze Amazon Elastic Compute Cloud (Amazon EC2) che hanno eseguito SQL Server nelle ultime 24 ore. Un database SQL Server ha un limite di capacità di calcolo per ogni istanza. Un'istanza con SQL Server Standard Edition può utilizzare fino a 48 vCPU. Un'istanza con SQL Server Web può utilizzare fino a 32 vCPU. Questo controllo ti avvisa se un'istanza supera questo limite di vCPU.

Se la tua istanza ha un provisioning eccessivo, paghi il prezzo intero senza realizzare un miglioramento delle prestazioni. Puoi gestire il numero e le dimensioni delle istanze per ridurre i costi.

I risparmi mensili stimati vengono calcolati utilizzando la stessa famiglia di istanze con il numero massimo di vCPU che un'istanza di SQL Server può utilizzare e il prezzo on-demand. I risparmi effettivi variano se si utilizzano Istanze riservate (IR) o se l'istanza non è in esecuzione per un giorno intero.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

Qsdfp3A4L1

Criteri di avviso

- Rosso: un'istanza con SQL Server Standard Edition ha più di 48 vCPU.
- Rosso: un'istanza con SQL Server Web Edition ha più di 32 vCPU.

Operazione consigliata

Per SQL Server Standard Edition, valuta la possibilità di passare a un'istanza della stessa famiglia di istanze con 48 vCPU. Per SQL Server Web Edition, valuta la possibilità di passare a un'istanza della stessa famiglia di istanze con 32 vCPU. Se è necessaria molta memoria, valuta la possibilità di passare a istanze R5 ottimizzate per la memoria. Per ulteriori informazioni, consulta Best practice per l'implementazione di Microsoft SQL Server su Amazon EC2.

Risorse aggiuntive

- Microsoft SQL Server in AWS
- È possibile utilizzare Launch Wizard per semplificare l'implementazione di SQL Server su EC2.

Colonne del report

- Stato
- Regione
- ID istanza
- Tipo di istanza
- VPCU
- SQL Server Edition
- vCPU massima
- Tipo di istanza consigliato
- Risparmi mensili stimati
- Ora ultimo aggiornamento

Istanze di Amazon EC2 interrotte

Descrizione

Controlla se sono presenti istanze di Amazon EC2 che sono state interrotte per più di 30 giorni.

È possibile specificare il valore del numero di giorni consentito nei parametri of. AllowedDaysAWS Config

Per ulteriori informazioni, consulta Perché mi viene addebitato un costo per Amazon EC2 quando tutte le mie istanze sono interrotte?

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz150`

Origine

`AWS Config Managed Rule: ec2-stopped-instance`

Criteri di avviso

- Giallo: esistono istanze di Amazon EC2 interrotte per un numero di giorni maggiore rispetto a quello consentito.

Operazione consigliata

Esamina le istanze Amazon EC2 che sono state interrotte per almeno 30 giorni. Per evitare di incorrere in costi inutili, termina tutte le istanze che non sono più necessarie.

Per ulteriori informazioni, consulta Termina le istanze.

Risorse aggiuntive

- Prezzi di Amazon EC2 on demand

Colonne del report

- Stato
- Regione
- Risorsa
- Regola AWS Config

- Parametri di input
- Ora ultimo aggiornamento

Scadenza locazione istanze riservate Amazon EC2

Descrizione

Controlla le istanze riservate di Amazon EC2 che scadono entro i 30 giorni successivi, o sono scaduti nei 30 giorni precedenti.

Le istanze riservate non si rinnovano automaticamente. Puoi continuare a utilizzare un'istanza Amazon EC2 riservata senza interruzioni, ma ti verranno addebitate le tariffe On Demand. Le nuove istanze riservate possono avere gli stessi parametri di quelle scadute, oppure è possibile acquistare istanze riservate con parametri diversi.

Il risparmio mensile stimato è la differenza tra le tariffe On Demand e l'istanza riservata per lo stesso tipo di istanza.

Controlla ID

`1e93e4c0b5`

Criteri di avviso

- Giallo: la locazione dell'istanza riservata scade in meno di 30 giorni.
- Giallo: la locazione dell'istanza riservata è scaduta nei 30 giorni precedenti.

Operazione consigliata

Valuta l'acquisto di una nuova istanza riservata per sostituire quella che sta per scadere. Per ulteriori informazioni, consulta Come acquistare istanze riservate e Acquisto di istanze riservate.

Risorse aggiuntive

- Istanze riservate
- Tipi di istanza

Colonne del report

- Stato
- Zona
- Tipo di istanza
- Piattaforma

- Conteggio istanze
- Costo mensile corrente
- Risparmi mensili stimati
- Data di scadenza
- ID Istanza riservata
- Motivo

Ottimizzazione delle istanze riservate Amazon EC2

Descrizione

Una parte consistente dell'utilizzo di AWS implica trovare un equilibrio tra le istanze riservate (RI) acquistate e le istanze on demand utilizzate. Questo controllo fornisce suggerimenti in base ai quali le istanze riservate contribuiranno a ridurre i costi sostenuti dall'utilizzo delle istanze On Demand.

Questi suggerimenti vengono creati analizzando l'utilizzo On Demand degli ultimi 30 giorni. Quindi viene categorizzato l'utilizzo in categorie idonee per le prenotazioni. Ciascuna combinazione di prenotazioni viene simulata nella categoria di utilizzo generata per identificare il numero consigliato per ciascun tipo di istanza riservata da acquistare. Questo processo di simulazione e ottimizzazione ci permette di massimizzare i risparmi sui costi. Questo controllo riguarda i suggerimenti basati su Istanze Riservate Standard con l'opzione di pagamento anticipato parziale.

Questo controllo non è disponibile per gli account collegati nella fatturazione consolidata. I suggerimenti per questo controllo sono disponibili solo per l’account di pagamento.

ID di controllo

`cX3c2R1chu`

Criteri di avviso

Giallo: l'ottimizzazione dell'uso di istanze riservate con pagamento anticipato parziale può contribuire a ridurre i costi.

Operazione consigliata

Consulta la pagina Cost Explorer per suggerimenti più dettagliati e personalizzati. Inoltre, fai riferimento alla guida all'acquisto per capire come acquistare le istanze riservate e le opzioni disponibili.

Risorse aggiuntive

- Puoi trovare informazioni sulle istanze riservate e su come possono farti risparmiare denaro qui.
- Per ulteriori informazioni a riguardo, consulta Domande relative al controllo di ottimizzazione delle istanze riservate nelle Domande frequenti di Trusted Advisor.

Colonne del report

- Regione
- Tipo di istanza
- Piattaforma
- Numero consigliato di istanze riservate da acquistare
- Utilizzo medio previsto delle istanze riservate
- Risparmi stimati con i suggerimenti (mensile)
- Costo del pagamento anticipato delle istanze riservate
- Costi stimati delle istanze riservate (mensili)
- Costo stimato di On-Demand dopo l'acquisto delle istanze riservate consigliate (mensile)
- Break Even stimato (mesi)
- Periodo di ricerca posticipata (giorni)
- Durata (anni)

Repository di Amazon ECR senza policy del ciclo di vita configurata

Descrizione

Controlla se per un repository di Amazon ECR privato è configurata almeno una policy del ciclo di vita. Le policy del ciclo di vita consentono di definire una serie di regole per ripulire automaticamente immagini vecchie o inutilizzate dei container. Ciò consente di controllare la gestione del ciclo di vita delle immagini, consente di organizzare meglio i repository di Amazon ECR e contribuisce a ridurre i costi di archiviazione complessivi.

Per ulteriori informazioni, consulta Policy del ciclo di vita.

ID di controllo

```
c18d2gz128
```

Origine

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

Criteri di avviso

Giallo: per un repository privato di Amazon ECR non è configurata alcuna policy del ciclo di vita.

Operazione consigliata

Considera la possibilità di creare almeno una policy del ciclo di vita per il tuo repository privato di Amazon ECR.

Per ulteriori informazioni, consulta Creazione di una policy del ciclo di vita.

Risorse aggiuntive

- Policy del ciclo di vita.
- Creazione di una policy del ciclo di vita.
- Esempi di policy del ciclo di vita.

Colonne del report

- Stato
- Regione
- Risorsa
- Regola AWS Config
- Parametri di input
- Ora ultimo aggiornamento

Ottimizzazione dei nodi ElastiCache riservati Amazon

Descrizione

Verifica l'utilizzo dei nodi riservati ElastiCache e fornisce consigli sull'acquisto dei nodi riservati. Questi consigli sono offerti per ridurre i costi derivanti dall'utilizzo di ElastiCache On-Demand. Questi suggerimenti vengono creati analizzando l'utilizzo On Demand degli ultimi 30 giorni.

Questa analisi viene utilizzata per simulare ogni combinazione di prenotazioni nella categoria di utilizzo generata. Questo ci permette di consigliare il numero di ogni tipo di nodo riservato da acquistare per massimizzare i risparmi. Questo controllo riguarda i suggerimenti basati sull'opzione di pagamento anticipato parziale con un impegno di 1 anno o 3 anni.

Questo controllo non è disponibile per gli account collegati nella fatturazione consolidata. I suggerimenti per questo controllo sono disponibili solo per l’account di pagamento.

ID di controllo

`h3L1otH3re`

Criteri di avviso

Giallo: l'ottimizzazione dell'acquisto di nodi ElastiCache riservati può aiutare a ridurre i costi.

Operazione consigliata

Consulta la pagina Cost Explorer per consigli più dettagliati, opzioni di personalizzazione (ad esempio, periodo di riferimento, opzione di pagamento e così via) e per acquistare nodi riservati. ElastiCache

Risorse aggiuntive

- Le informazioni sui nodi ElastiCache riservati e su come possono farti risparmiare denaro sono disponibili qui.
- Per ulteriori informazioni a riguardo, consulta Domande relative al controllo di ottimizzazione delle istanze riservate nelle Domande frequenti di Trusted Advisor.
- Per una descrizione più dettagliata dei campi, consulta la documentazione relativa a Cost Explorer

Colonne del report

- Regione
- Family
- Tipo di nodo
- Descrizione del prodotto
- Numero consigliato di nodi riservati da acquistare
- Utilizzo medio previsto dei nodi riservati
- Risparmi stimati con i suggerimenti (mensile)
- Costo del pagamento anticipato dei nodi riservati
- Costo stimato dei nodi riservati (mensile)
- Costo stimato di On-Demand dopo l'acquisto dei nodi riservati consigliati (mensile)
- Break Even stimato (mesi)
- Periodo di ricerca posticipata (giorni)
- Durata (anni)

Ottimizzazione delle istanze riservate di Amazon OpenSearch Service

Descrizione

Verifica l'utilizzo del OpenSearch servizio Amazon e fornisce consigli sull'acquisto di istanze riservate. Questi consigli sono offerti per ridurre i costi derivanti dall'utilizzo OpenSearch di On-Demand. Questi suggerimenti vengono creati analizzando l'utilizzo On Demand degli ultimi 30 giorni.

Questa analisi viene utilizzata per simulare ogni combinazione di prenotazioni nella categoria di utilizzo generata. Questo ci permette di consigliare il numero di ogni tipo di istanza riservata da acquistare per massimizzare i risparmi. Questo controllo riguarda i suggerimenti basati sull'opzione di pagamento anticipato parziale con un impegno di 1 anno o 3 anni.

Questo controllo non è disponibile per gli account collegati nella fatturazione consolidata. I suggerimenti per questo controllo sono disponibili solo per l'account di pagamento.

ID di controllo

`7ujm6yhn5t`

Criteri di avviso

Giallo: l'ottimizzazione dell'acquisto di istanze riservate di Amazon OpenSearch Service può aiutare a ridurre i costi.

Operazione consigliata

Consulta la pagina Cost Explorer per consigli più dettagliati, opzioni di personalizzazione (ad esempio periodo di riferimento, opzione di pagamento, ecc.) e per acquistare istanze riservate di Amazon OpenSearch Service.

Risorse aggiuntive

- Le informazioni sulle istanze riservate del OpenSearch servizio Amazon e su come possono farti risparmiare denaro sono disponibili qui.
- Per ulteriori informazioni a riguardo, consulta Domande relative al controllo di ottimizzazione delle istanze riservate nelle Domande frequenti di Trusted Advisor.
- Per una descrizione più dettagliata dei campi, consulta la documentazione relativa a Cost Explorer

Colonne del report

- Regione

- Classe istanza
- Dimensioni istanza
- Numero consigliato di istanze riservate da acquistare
- Utilizzo medio previsto delle istanze riservate
- Risparmi stimati con i suggerimenti (mensile)
- Costo del pagamento anticipato delle istanze riservate
- Costo stimato delle istanze riservate (mensile)
- Costo stimato di On-Demand dopo l'acquisto delle istanze riservate consigliate (mensile)
- Break Even stimato (mesi)
- Periodo di ricerca posticipata (giorni)
- Durata (anni)

Istanze database Amazon RDS inattive

Descrizione

Controlla la configurazione di Amazon Relational Database Service (Amazon RDS) per qualsiasi istanza database (DB) che sembra inattiva.

È possibile eliminare un'istanza database per ridurre i costi se questa non dispone di una connessione per un periodo di tempo prolungato. Un'istanza database è considerata inattiva se questa non si è connessa negli ultimi 7 giorni. Se è necessaria l'archiviazione persistente per i dati sull'istanza, è possibile utilizzare opzioni a basso costo, come l'acquisizione e la conservazione di uno snapshot DB. Gli snapshot DB creati manualmente vengono conservati finché non vengono eliminati.

ID di controllo

`Ti39halfu8`

Criteri di avviso

Giallo: un'istanza DB attiva non si è connessa negli ultimi 7 giorni.

Operazione consigliata

Valuta la possibilità di acquisire uno snapshot dell'istanza DB inattiva e quindi di interromperla o eliminarla. L'interruzione dell'istanza DB comporta la rimozione di alcuni costi, ma non dei costi

di archiviazione. Un'istanza interrotta conserva tutti i backup automatici in base al periodo di conservazione configurato. L'interruzione di un'istanza DB comporta in genere costi aggiuntivi rispetto all'eliminazione dell'istanza e quindi al mantenimento solo dello snapshot finale. Consulta Interruzione temporanea di un'istanza Amazon RDS ed Eliminazione di un'istanza DB con uno snapshot finale.

Risorse aggiuntive

Backup e ripristino

Colonne del report

- Regione
- Nome dell'istanza DB
- Multi-AZ
- Tipo di istanza
- Archiviazione fornita (GB)
- Giorni dall'ultima connessione
- Risparmi mensili stimati (On Demand)

Ottimizzazione dei nodi riservati Amazon Redshift

Descrizione

Controlla l'utilizzo di Amazon Redshift e fornisce suggerimenti sull'acquisto di nodi riservati per ridurre i costi sostenuti dall'utilizzo On Demand di Amazon Redshift.

Questi suggerimenti vengono generati analizzando l'utilizzo On Demand degli ultimi 30 giorni. Questa analisi viene utilizzata per simulare ogni combinazione di prenotazioni nella categoria di utilizzo generata. Questo ci permette di identificare il numero ottimale di ogni tipo di nodi riservati da acquistare per massimizzare i risparmi. Questo controllo riguarda i suggerimenti basati sull'opzione di pagamento anticipato parziale con un impegno di 1 anno o 3 anni.

Questo controllo non è disponibile per gli account collegati nella fatturazione consolidata. I suggerimenti per questo controllo sono disponibili solo per l'account di pagamento.

ID di controllo

`1qw23er45t`

Criteri di avviso

Giallo: l'ottimizzazione dell'acquisto di nodi riservati Amazon Redshift può contribuire a ridurre i costi.

Operazione consigliata

Consulta la pagina Cost Explorer per suggerimenti più dettagliati, opzioni di personalizzazione (ad es. periodo di ricerca posticipata, opzione di pagamento, ecc.) e per acquistare nodi riservati Amazon Redshift.

Risorse aggiuntive

- Puoi trovare informazioni sui nodi riservati di Amazon Redshift e su come possono farti risparmiare denaro qui.
- Per ulteriori informazioni a riguardo, consulta Domande relative al controllo di ottimizzazione delle istanze riservate nelle Domande frequenti di Trusted Advisor.
- Per una descrizione più dettagliata dei campi, consulta la documentazione relativa a Cost Explorer

Colonne del report

- Regione
- Family
- Tipo di nodo
- Numero consigliato di nodi riservati da acquistare
- Utilizzo medio previsto dei nodi riservati
- Risparmi stimati con i suggerimenti (mensile)
- UpFront Costo dei nodi riservati
- Costo stimato dei nodi riservati (mensile)
- Costo stimato di On-Demand dopo l'acquisto dei nodi riservati consigliati (mensile)
- Break Even stimato (mesi)
- Periodo di ricerca posticipata (giorni)
- Durata (anni)

Ottimizzazione dell’istanza riservata Amazon Relational Database Service (RDS)

Descrizione

Controlla l'utilizzo di servizi RDS e fornisce consigli sull'acquisto di istanze riservate per ridurre i costi sostenuti dall'utilizzo di servizi RDS On Demand.

Questi suggerimenti vengono generati analizzando l'utilizzo On Demand degli ultimi 30 giorni. Questa analisi viene utilizzata per simulare ogni combinazione di prenotazioni nella categoria di utilizzo generata. Questo ci permette di identificare il numero ottimale di ogni tipo di istanza riservata da acquistare per massimizzare i risparmi. Questo controllo riguarda i suggerimenti basati sull'opzione di pagamento anticipato parziale con impegno di 1 anno o 3 anni.

Questo controllo non è disponibile per gli account collegati nella fatturazione consolidata. I suggerimenti per questo controllo sono disponibili solo per l’account di pagamento.

ID di controllo

`1qazXsw23e`

Criteri di avviso

Giallo: l'ottimizzazione dell'acquisto di istanze riservate di Amazon RDS può contribuire a ridurre i costi.

Operazione consigliata

Consulta la pagina Cost Explorer per suggerimenti più dettagliati, opzioni di personalizzazione (ad es. periodo di ricerca posticipata, opzione di pagamento, ecc.) e per acquistare istanze riservate di Amazon RDS.

Risorse aggiuntive

- Puoi trovare informazioni sulle istanze riservate di Amazon RDS e su come possono farti risparmiare denaro qui.
- Per ulteriori informazioni a riguardo, consulta Domande relative al controllo di ottimizzazione delle istanze riservate nelle Domande frequenti di Trusted Advisor.
- Per una descrizione più dettagliata dei campi, consulta la documentazione relativa a Cost Explorer

Colonne del report

- Regione

- Family
- Tipo di istanza
- Modello di licenza
- Edizione Database
- Motore di database
- Opzione di distribuzione
- Numero consigliato di istanze riservate da acquistare
- Utilizzo medio previsto delle istanze riservate
- Risparmi stimati con i suggerimenti (mensile)
- Costo del pagamento anticipato delle istanze riservate
- Costo stimato delle istanze riservate (mensile)
- Costo stimato di On-Demand dopo l'acquisto consigliato delle istanze riservate (mensile)
- Break Even stimato (mesi)
- Periodo di ricerca posticipata (giorni)
- Durata (anni)

Set di registri delle risorse di latenza Amazon Route 53

Descrizione

Controlla i set di registro di latenza Amazon Route 53 configurati in modo inefficiente.

Per consentire ad Amazon Route 53 di instradare le query alla Regione AWS con la latenza di rete più bassa, è necessario creare set di registri delle risorse di latenza per un particolare nome di dominio (ad esempio example.com) in Regioni diverse. Se si crea un solo set di registri delle risorse di latenza per un nome di dominio, tutte le query vengono instradate verso una Regione e viene addebitato un supplemento per l'instradamento basato sulla latenza senza ottenerne i vantaggi.

Le zone ospitate create da AWS non verranno visualizzate nei risultati del controllo.

ID di controllo

`51fC20e7I2`

Criteri di avviso

Giallo: solo un set di registri delle risorse di latenza è configurato per un particolare nome di dominio.

Operazione consigliata

Se disponi di risorse in più regioni, assicurati di definire un set di registri delle risorse di latenza per ciascuna regione. Consulta Routing basato sulla latenza.

Se disponi di risorse in una sola Regione AWS, valuta la possibilità di creare risorse in più di una Regione AWS e definire set di registri delle risorse di latenza per ciascuna regione. Consulta Routing basato sulla latenza.

Se non desideri utilizzare più Regioni AWS, devi utilizzare un set di registri delle risorse semplice. Consulta Utilizzo di set di registri delle risorse.

Risorse aggiuntive

- Guida per gli sviluppatori di Amazon Route 53
- Prezzi di Amazon Route 53

Colonne del report

- Nome della zona ospitata
- ID della zona ospitata
- Nome del set di registri delle risorse
- Tipo di set di registri delle risorse

Policy del ciclo di vita dei bucket di Amazon S3 configurata

Descrizione

Controlla se per un bucket di Amazon S3 è configurata una policy del ciclo di vita. Una policy del ciclo di vita di Amazon S3 garantisce che gli oggetti Amazon S3 all'interno del bucket siano archiviati in maniera conveniente durante l'intero ciclo di vita. Ciò è importante per soddisfare i requisiti normativi per l'archiviazione e la conservazione dei dati. Una configurazione della policy è un insieme di regole che definisce le operazioni applicate dal servizio Amazon S3 a un gruppo di oggetti. Una policy del ciclo di vita consente di automatizzare la transizione degli oggetti verso classi di archiviazione dai costi inferiori o eliminare gli oggetti mano a mano che invecchiano. Ad

esempio, puoi trasferire un oggetto nell'archiviazione Amazon S3 Standard-IA 30 giorni dopo la sua creazione o su Amazon S3 Glacier dopo 1 anno.

Puoi anche definire la scadenza dell'oggetto in modo che Amazon S3 elimini automaticamente l'oggetto dopo un certo periodo di tempo.

Puoi regolare la configurazione di controllo tramite i parametri nelle tue regole AWS Config

Per ulteriori informazioni, consulta Gestione del ciclo di vita dell'archiviazione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz100`

Origine

`AWS Config Managed Rule: s3-lifecycle-policy-check`

Criteri di avviso

Giallo: per il bucket di Amazon S3 non è configurata alcuna policy del ciclo di vita.

Operazione consigliata

Assicurati che una policy del ciclo di vita sia configurata nel tuo bucket Amazon S3.

Se la tua organizzazione non dispone di una policy di conservazione, considera la possibilità di utilizzare il Piano intelligente Amazon S3 per ottimizzare i costi.

Per informazioni su come definire la policy del ciclo di vita di Amazon S3, consulta Impostazione della configurazione del ciclo di vita in un bucket.

Per informazioni sul Piano intelligente Amazon S3, consulta Classe di archiviazione del Piano intelligente Amazon S3

Risorse aggiuntive

Impostazione della configurazione del ciclo di vita in un bucket

Esempi di configurazione del ciclo di vita S3

Colonne del report

- Stato
- Regione
- Risorsa
- Regola AWS Config
- Parametri di input

Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3

Descrizione

Verifica che ogni bucket Amazon S3 sia configurato con una regola del ciclo di vita per interrompere i caricamenti in più parti che rimangono incompleti dopo 7 giorni. Si consiglia di utilizzare una regola del ciclo di vita per interrompere questi caricamenti incompleti ed eliminare lo storage associato.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente una o più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1cj39rr6v`

Criteri di avviso

Giallo: il bucket di configurazione del ciclo di vita non contiene una regola del ciclo di vita per interrompere tutti i caricamenti in più parti che rimangono incompleti dopo 7 giorni.

Operazione consigliata

Rivedi la configurazione del ciclo di vita per i bucket senza una regola del ciclo di vita che eliminerebbe tutti i caricamenti multiparte incompleti. È improbabile che i caricamenti che non vengono completati dopo 24 ore vengano completati. Fai clic qui per seguire le istruzioni per creare una regola del ciclo di vita. Si consiglia di applicarla a tutti gli oggetti del bucket. Se hai bisogno di applicare altre azioni del ciclo di vita agli oggetti selezionati nel tuo bucket, puoi avere più regole con filtri diversi. Controlla la dashboard di Storage Lens o chiama l' ListMultipartUpload API per ulteriori informazioni.

Risorse aggiuntive

Creazione di una configurazione del ciclo di vita

Individuazione ed eliminazione di caricamenti multiparte incompleti per ridurre i costi di Amazon S3

Caricamento e copia di oggetti utilizzando il caricamento in più parti

Elementi di configurazione del ciclo di vita

Elementi per descrivere le azioni del ciclo di vita

Configurazione del ciclo di vita per interrompere i caricamenti in più parti

Colonne del report

- Stato
- Regione
- Bucket Name (Nome bucket)
- Bucket ARN
- Regola del ciclo di vita per l'eliminazione di MPU incomplete
- Giorni dopo l'iniziazione
- Ora ultimo aggiornamento

Bucket abilitati alla versione di Amazon S3 senza policy del ciclo di vita configurate

Descrizione

Verifica se per i bucket abilitati alla versione di Amazon S3 è configurata una policy del ciclo di vita.

Per ulteriori informazioni, consulta Gestione del ciclo di vita dell'archiviazione.

Puoi specificare i nomi dei bucket da controllare utilizzando i parametri bucketNames nelle tue regole AWS Config.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz171`

Origine

`AWS Config Managed Rule: s3-version-lifecycle-policy-check`

Criteri di avviso

Giallo: per un bucket abilitato alla versione di Amazon S3 non è configurata una policy del ciclo di vita.

Operazione consigliata

Configura le policy del ciclo di vita per i bucket di Amazon S3 per gestire gli oggetti in modo da archiviarli in maniera conveniente durante l'intero ciclo di vita.

Per ulteriori informazioni, consulta Impostazione della configurazione del ciclo di vita in un bucket.

Risorse aggiuntive

Gestione del ciclo di vita dello storage

Impostazione della configurazione del ciclo di vita in un bucket

Colonne del report

- Stato
- Regione

- Risorsa
- Regola AWS Config
- Parametri di input
- Ora ultimo aggiornamento

AWS Lambda Funzioni con timeout eccessivi

Descrizione

Controlla le funzioni Lambda con tassi di timeout elevati che potrebbero comportare costi elevati.

Addebiti Lambda basati su runtime e numero di richieste per la funzione. I timeout delle funzioni generano errori che possono causare nuovi tentativi. Ritentare le funzioni comporterà ulteriori costi di richiesta e runtime.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`L4dfs2Q3C3`

Criteri di avviso

Giallo: funzioni in cui più del 10% dei richiami termina con un errore a causa di un timeout in un dato giorno negli ultimi 7 giorni.

Operazione consigliata

Ispeziona la registrazione delle funzioni e le tracce dei raggi X per determinare cosa contribuisce alla durata elevata della funzione. Implementa la registrazione del codice nelle parti pertinenti, ad esempio prima o dopo le chiamate API o le connessioni al database. Per impostazione predefinita, i timeout dei client AWS SDK possono essere più lunghi della durata della funzione configurata. Regola i client di connessione API e SDK per riprovare o non andare a buon fine

entro il timeout della funzione. Se la durata prevista è superiore al timeout configurato, puoi aumentarne l'impostazione per la funzione. Per ulteriori informazioni, consulta Monitoraggio e risoluzione dei problemi delle applicazioni Lambda.

Risorse aggiuntive

- Monitoraggio e risoluzione dei problemi delle applicazioni Lambda
- SDK del timeout relativo ai tentativi della funzione Lambda
- Utilizzo di AWS Lambda con AWS X-Ray
- Accesso ai CloudWatch log di Amazon per AWS Lambda
- Applicazione di esempio del processore di errori per AWS Lambda

Colonne del report

- Stato
- Regione
- ARN della funzione
- Tasso massimo di timeout giornaliero
- Data del tasso massimo di timeout giornaliero
- Tasso medio di timeout giornaliero
- Impostazioni timeout funzione (millisecondi)
- Costo di calcolo giornaliero perso
- Media richiami giornalieri
- Richiami per il giorno corrente
- Tasso di timeout del giorno corrente
- Ora ultimo aggiornamento

AWS Lambda Funzioni con elevati tassi di errore

Descrizione

Controlla le funzioni Lambda con alti tassi di errore che potrebbero comportare costi più elevati.

Gli addebiti Lambda si basano sul numero di richieste e sul runtime aggregato per la funzione. Gli errori di funzione possono causare nuovi tentativi che comportano costi aggiuntivi.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`L4dfs2Q3C2`

Criteri di avviso

Giallo: funzioni in cui più del 10% dei richiami termina con un errore in un dato giorno negli ultimi 7 giorni.

Operazione consigliata

Segui le seguenti linee guida per ridurre gli errori. Gli errori di funzione includono gli errori restituiti dal codice della funzione e gli errori restituiti dal runtime della funzione.

Per aiutarti a risolvere gli errori Lambda, Lambda si integra con servizi come Amazon e. CloudWatch AWS X-Ray Puoi utilizzare una combinazione di registri, parametri, allarmi e traccia X-Ray per rilevare e identificare rapidamente problemi di codice della funzione, API e altre risorse che supportano l'applicazione. Per ulteriori informazioni, consulta Monitoraggio e risoluzione dei problemi delle applicazioni Lambda.

Per ulteriori informazioni sulla gestione degli errori con runtime specifici, consulta Gestione degli errori e tentativi automatici in AWS Lambda.

Per ulteriori procedure di risoluzione dei problemi, consulta Risoluzione dei problemi in Lambda.

Puoi anche scegliere tra un ecosistema di strumenti di monitoraggio e osservabilità forniti dai partner AWS Lambda. Per ulteriori informazioni, consulta Partner AWS Lambda.

Risorse aggiuntive

- Gestione degli errori e tentativi automatici in AWS Lambda
- Monitoraggio e risoluzione dei problemi delle applicazioni Lambda
- SDK del timeout relativo ai tentativi della funzione Lambda
- Risoluzione dei problemi in Lambda

- Errori di richiamo dell'API
- Applicazione di esempio del processore di errori per AWS Lambda

Colonne del report

- Stato
- Regione
- ARN della funzione
- Tasso di errore massimo giornaliero
- Data del tasso di errore massimo
- Tasso di errore medio giornaliero
- Costo di calcolo giornaliero perso
- Media richiami giornalieri
- Richiami per il giorno corrente
- Tasso di errore del giorno corrente
- Ora ultimo aggiornamento

Funzioni AWS Lambda con provisioning eccessivo per la dimensione della memoria

Descrizione

Controlla le funzioni AWS Lambda che sono state richiamate almeno una volta durante il periodo di ricerca posticipata. Questo controllo avvisa se una qualsiasi delle funzioni Lambda è stata sottoposta a provisioning eccessivo per le dimensioni della memoria. Quando si dispone di funzioni Lambda che sono state sottoposti a provisioning eccessivo per le dimensioni della memoria, si paga per le risorse inutilizzate. Sebbene alcuni scenari possano comportare un utilizzo ridotto in base alla progettazione, spesso è possibile ridurre i costi modificando la configurazione della memoria delle funzioni Lambda. I risparmi mensili stimati vengono calcolati utilizzando il tasso di utilizzo corrente per le funzioni Lambda.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`C0r6dfpM05`

Criteri di avviso

Giallo: una funzione Lambda sottoposta a provisioning eccessivo per le dimensioni della memoria durante il periodo di ricerca posticipata. Per determinare se il provisioning di una funzione Lambda è eccessivo, consideriamo tutte le metriche predefinite CloudWatch per quella funzione. L'algoritmo utilizzato per identificare le funzioni Lambda sottoposte a provisioning eccessivo per le dimensioni della memoria segue le best practice AWS. L'algoritmo viene aggiornato quando viene identificato un nuovo modello.

Operazione consigliata

Valuta la possibilità di ridurre le dimensioni della memoria delle tue funzioni Lambda.

Per ulteriori informazioni, consulta Attiva AWS Compute Optimizer i Trusted Advisor controlli.

Colonne del report

- Stato
- Regione
- Nome funzione
- Versione della funzione
- Dimensioni della memoria (MB)
- Dimensioni della memoria consigliate (MB)
- Periodo di ricerca posticipata (giorni)
- Opportunità di risparmio (%)
- Risparmi mensili stimati
- Valuta dei risparmi mensili stimati
- Ora ultimo aggiornamento

Problemi ad alto rischio di AWS Well-Architected per l'ottimizzazione dei costi

Descrizione

Verifica problemi ad alto rischio (HRI) per i carichi di lavoro nel pilastro di ottimizzazione dei costi. Questo controllo è basato sulle tue revisioni di AWS-Well Architected. I risultati dei controlli dipendono dal completamento della valutazione del carico di lavoro con AWS Well-Architected.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Wxdfp4B1L1`

Criteri di avviso

- Rosso: almeno un problema attivo ad alto rischio è stato identificato nel pilastro dell'ottimizzazione dei costi per AWS Well-Architected.
- Verde: non sono stati rilevati problemi attivi ad alto rischio nel pilastro dell'ottimizzazione dei costi per AWS Well-Architected.

Operazione consigliata

AWS Well-Architected ha rilevato problemi ad alto rischio durante la valutazione del carico di lavoro. Questi problemi offrono opportunità per ridurre i rischi e risparmiare denaro. Accedi allo strumento AWS Well-Architected per rivedere le tue risposte e risolvere i problemi attivi.

Colonne del report

- Stato
- Regione
- ARN del carico di lavoro
- Nome del carico di lavoro
- Nome del revisore
- Tipo di carico di lavoro
- Data di inizio del carico di lavoro
- Data dell'ultima modifica del carico di lavoro
- Numero di HRI identificati per Ottimizzazione dei costi
- Numero di HRI risolti per Ottimizzazione dei costi
- Numero di domande risposte per Ottimizzazione dei costi
- Numero totale di domande nel pilastro Ottimizzazione dei costi

- Ora ultimo aggiornamento

Bilanciatori del carico inattivi

Descrizione

Controlla la configurazione Elastic Load Balancing per i bilanciatori del carico inattivi.

Qualsiasi load balancer configurato farà maturare gli addebiti. Se un load balancer non ha istanze back-end associate o se il traffico di rete è seriamente limitato, il load balancer non verrà utilizzato in modo efficace. Attualmente questo controllo verifica solo il tipo Classic Load Balancer all'interno del servizio ELB. Non include altri tipi di ELB (Application Load Balancer, Network Load Balancer).

ID di controllo

`hjLMh88uM8`

Criteri di avviso

- Giallo: un load balancer non ha istanze back-end attive.
- Giallo: un load balancer non ha istanze back-end integre.
- Giallo: un load balancer ha ricevuto meno di 100 richieste al giorno negli ultimi 7 giorni.

Operazione consigliata

Se il load balancer non ha istanze back-end attive, valuta la possibilità di registrare istanze o eliminare il load balancer. Consulta Registrazione delle istanze Amazon EC2 con il load balancer o Rimozione del load balancer.

Se il load balancer non dispone di istanze back-end integre, consulta Risoluzione dei problemi di Elastic Load Balancing: configurazione del controllo dell'integrità.

Se il load balancer ha un numero di richieste basso, valutane l'eliminazione. Consulta Rimozione del load balancer.

Risorse aggiuntive

- Gestione dei load balancer
- Risoluzione di Elastic Load Balancing

Colonne del report

- Regione
- Nome del load balancer

- Motivo
- Risparmi mensili stimati

Istanze Amazon EC2 con utilizzo ridotto

Descrizione

Controlla le istanze Amazon Elastic Compute Cloud (Amazon EC2) in esecuzione in qualsiasi momento durante gli ultimi 14 giorni. Questo controllo avvisa se l'utilizzo giornaliero della CPU è pari o inferiore al 10% e l'I/O di rete è stato pari o inferiore a 5 MB per almeno 4 giorni.

Le istanze in esecuzione generano costi di utilizzo orari. Sebbene alcuni scenari possano comportare un utilizzo ridotto in base alla progettazione, spesso è possibile ridurre i costi gestendo il numero e le dimensioni delle istanze.

I risparmi mensili stimati vengono calcolati utilizzando il tasso di utilizzo corrente per le Istanze On Demand e il numero stimato di giorni in cui l'istanza potrebbe essere sottoutilizzata. I risparmi effettivi variano se si utilizzano Istanze Riservate o Istanze Spot o se l'istanza non è in esecuzione per un giorno intero. Per ottenere i dati di utilizzo giornaliero scarica il report per questo controllo.

ID di controllo

`Qch7DwouX1`

Criteri di avviso

Giallo: un'istanza ha avuto un utilizzo medio giornaliero della CPU pari o inferiore al 10% e un I/O di rete pari o inferiore a 5 MB per almeno 4 dei 14 giorni precedenti.

Operazione consigliata

Valuta la possibilità di interrompere o chiudere le istanze che hanno un utilizzo ridotto o ridimensionare il numero di istanze utilizzando Auto Scaling. Per ulteriori informazioni, consulta Arresto e avvio dell'istanza, Interruzione di un'istanza e Cos'è Auto Scaling?

Risorse aggiuntive

- Monitoraggio di Amazon EC2
- Metadati dell'istanza e dati utente
- Guida per CloudWatch l'utente di Amazon
- Guida per gli sviluppatori di Auto Scaling

Colonne del report

- Regione/AZ
- ID istanza
- Nome dell'istanza
- Tipo di istanza
- Risparmi mensili stimati
- Utilizzo medio della CPU per 14 giorni
- Media I/O di rete per 14 giorni
- Numero di giorni con utilizzo ridotto

Savings Plan

Descrizione

Controlla l'utilizzo di Amazon EC2, Fargate e Lambda negli ultimi 30 giorni e fornisce suggerimenti per l'acquisto di Savings Plan. Questi suggerimenti consentono di impegnarsi per un importo di utilizzo adeguato misurato in dollari all'ora per un periodo di uno o tre anni in cambio di tariffe scontate.

Questi provengono da AWS Cost Explorer, che può ottenere suggerimenti più dettagliati. Puoi anche acquistare un savings plan (piano di risparmio) tramite Cost Explorer. Questi suggerimenti vanno considerati come un'alternativa ai suggerimenti dell'istanza riservata. Ti suggeriamo di agire solo su un set di suggerimenti. Agire su entrambi i set può portare ad un impegno eccessivo.

Questo controllo non è disponibile per gli account collegati nella fatturazione consolidata. I suggerimenti per questo controllo sono disponibili solo per l'account di pagamento.

ID di controllo

`vZ2c2W1srf`

Criteri di avviso

Giallo: l'ottimizzazione dell'acquisto di Savings Plans può aiutare a ridurre i costi.

Operazione consigliata

Consulta la pagina Cost Explorer per suggerimenti più dettagliati e personalizzati e per acquistare Savings Plans.

Risorse aggiuntive

- Guida per l'utente di Savings Plan
- Domande frequenti di Savings Plans

Colonne del report

- Tipo di Savings Plan
- Opzione di pagamento
- Costo anticipato
- Impegno orario all'acquisto
- Utilizzo medio stimato
- Risparmi mensili stimati
- Percentuale stimata di risparmio
- Durata (anni)
- Periodo di ricerca posticipata (giorni)

Indirizzi IP elastici non associati

Descrizione

Verifica la presenza di indirizzi IP elastici (EIP) che non sono associati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) in esecuzione.

Gli EIP sono indirizzi IP statici progettati per il cloud computing dinamico. A differenza degli indirizzi IP statici tradizionali, gli EIP mascherano il fallimento di un'istanza o di una zona di disponibilità rimappando un indirizzo IP pubblico in un'altra istanza presente nell'account. Un addebito nominale viene imposto per un EIP non associato a un'istanza in esecuzione.

ID di controllo

`Z4AUBRNSmz`

Criteri di avviso

Giallo: un indirizzo IP elastico (EIP) assegnato non è associato a un'istanza Amazon EC2 in esecuzione.

Operazione consigliata

Associa l'EIP a un'istanza attiva in esecuzione o rilascia l'EIP non associato. Per ulteriori informazioni, consulta Associazione di un indirizzo IP elastico a un'istanza in esecuzione diversa e Rilascio di un indirizzo IP elastico.

Risorse aggiuntive

Indirizzi IP elastici

Colonne del report

- Regione
- Indirizzo IP

Volumi Amazon EBS sottoutilizzati

Descrizione

Controlla le configurazioni dei volumi Amazon Elastic Block Store (Amazon EBS) e avvisa quando i volumi sembrano sottoutilizzati.

Le spese vengono addebitate quando viene creato un volume. Se un volume rimane non associato o ha un'attività di scrittura molto bassa (esclusi i volumi di avvio) per un periodo di tempo, il volume viene sottoutilizzato. Per ridurre i costi, si consiglia di rimuovere i volumi sottoutilizzati.

ID di controllo

`DAvU99Dc4C`

Criteri di avviso

Giallo: un volume non è collegato o ha registrato meno di 1 IOPS al giorno negli ultimi 7 giorni.

Operazione consigliata

Valuta la possibilità di creare uno snapshot ed eliminare il volume per ridurre i costi. Per ulteriori informazioni, consulta Creazione di uno snapshot Amazon EBS ed Eliminazione di un volume Amazon EBS.

Risorse aggiuntive

- Amazon Elastic Block Store (Amazon EBS)

- Monitoraggio dello stato dei volumi

Colonne del report

- Regione
- ID volume
- Nome volume
- Tipo di volume
- Dimensioni volume
- Costo di archiviazione mensile
- ID snapshot
- Nome snapshot
- Età snapshot

> **Note**
>
> Se si è optato nel proprio account per AWS Compute Optimizer, si consiglia di utilizzare invece il controllo dei volumi Amazon EBS con provisioning eccessivo. Per ulteriori informazioni, consulta Attiva AWS Compute Optimizer i Trusted Advisor controlli.

Cluster Amazon Redshift sottoutilizzati

Descrizione

Controlla la configurazione Amazon Redshift per i cluster che sembrano essere sottoutilizzati.

Se un cluster Amazon Redshift non dispone di una connessione per un periodo di tempo prolungato o utilizza una quantità ridotta di CPU, è possibile utilizzare opzioni a basso costo come il ridimensionamento del cluster o l'arresto del cluster e lo snapshot finale. Gli snapshot finali vengono conservati anche dopo l'eliminazione del cluster.

ID di controllo

`G31sQ1E9U`

Criteri di avviso

- Giallo: un cluster in esecuzione non si è connesso negli ultimi 7 giorni.

- Giallo: un cluster in esecuzione ha registrato un utilizzo medio della CPU a livello di cluster inferiore al 5% per il 99% degli ultimi 7 giorni.

Operazione consigliata

Valuta la possibilità di chiudere il cluster e scattare uno snapshot finale o di ridimensionare il cluster. Consulta Chiusura ed eliminazione di cluster e Ridimensionamento di un cluster.

Risorse aggiuntive

Guida per CloudWatch l'utente di Amazon

Colonne del report

- Stato
- Regione
- Cluster
- Tipo di istanza
- Motivo
- Risparmi mensili stimati

Prestazioni

Migliorare le prestazioni del servizio controllando le quote di servizio (in precedenza denominate limiti), in modo da poter sfruttare la velocità effettiva assegnata, monitorare le istanze sovrautilizzate e rilevare eventuali risorse inutilizzate.

Per la categoria delle prestazioni, puoi utilizzare i seguenti controlli.

Controlla i nomi

- Cluster Amazon Aurora DB con un provisioning insufficiente per il carico di lavoro di lettura
- Dimensionamento automatico di Amazon DynamoDB non abilitato
- Ottimizzazione Amazon EBS non abilitata
- Configurazione degli allegati di Volume (SSD) IOPS con provisioning Amazon EBS
- Volumi Amazon EBS con provisioning insufficiente
- Il gruppo con dimensionamento automatico Amazon EC2 non è associato a un modello di avvio
- Ottimizzazione della velocità effettiva da Amazon EC2 a EBS

- Il tipo di virtualizzazione EC2 è paravirtuale
- Limite massimo di memoria di Amazon ECS
- Ottimizzazione della modalità di velocità di trasmissione effettiva di Amazon EFS
- Il parametro Amazon RDS autovacuum è disattivato
- I cluster Amazon RDS DB supportano solo volumi fino a 64 TiB
- Istanze database Amazon RDS nei cluster con classi di istanze eterogenee
- Istanze database di Amazon RDS nei cluster con dimensioni di istanze eterogenee
- I parametri di memoria DB di Amazon RDS sono diversi da quelli predefiniti
- Il parametro Amazon RDS enable_indexonlyscan è disattivato
- Il parametro Amazon RDS enable_indexscan è disattivato
- Il parametro general_logging di Amazon RDS è attivato
- Parametro Amazon RDS Innodb_change_buffering che utilizza un valore inferiore a quello ottimale
- Il parametro innodb_open_files di Amazon RDS è basso
- Il parametro innodb_stats_persistent di Amazon RDS è disattivato
- Istanza Amazon RDS con capacità di sistema insufficiente
- Il volume magnetico Amazon RDS è in uso
- I gruppi di parametri Amazon RDS non utilizzano pagine enormi
- Il parametro della cache delle query di Amazon RDS è attivato
- È richiesto l'aggiornamento della classe di istanza delle risorse Amazon RDS
- Risorse Amazon RDS: è richiesto l'aggiornamento delle versioni principali
- Risorse Amazon RDS che utilizzano End of Support Engine Edition con licenza inclusa
- Set di registri delle risorse Alias Amazon Route 53
- Funzioni AWS Lambda con provisioning insufficiente per la dimensione della memoria
- AWS Lambda Funzioni senza limite di concorrenza configurate
- Problemi ad alto rischio di AWS Well-Architected per le prestazioni
- CloudFront Nomi di dominio alternativi
- CloudFront Ottimizzazione della distribuzione dei contenuti
- CloudFront Inoltro delle intestazioni e rapporto di accesso alla cache
- Istanze Amazon EC2 con utilizzo elevato

Cluster Amazon Aurora DB con un provisioning insufficiente per il carico di lavoro di lettura

Descrizione

Verifica se il cluster Amazon Aurora DB dispone delle risorse per supportare un carico di lavoro di lettura.

ID di controllo

`c1qf5bt038`

Criteri di avviso

Giallo:

Aumento delle letture del database: il carico del database era elevato e il database leggeva più righe rispetto alla scrittura o all'aggiornamento delle righe.

Operazione consigliata

Si consiglia di ottimizzare le query per ridurre il carico del database o di aggiungere un'istanza DB reader al cluster DB con la stessa classe e dimensione dell'istanza DB writer nel cluster. La configurazione corrente prevede almeno un'istanza DB con un carico di database costantemente elevato causato principalmente da operazioni di lettura. Distribuisci queste operazioni aggiungendo un'altra istanza DB al cluster e indirizzando il carico di lavoro di lettura all'endpoint di sola lettura del cluster DB.

Risorse aggiuntive

Un cluster Aurora DB dispone di un endpoint di lettura per connessioni di sola lettura. Questo endpoint utilizza il bilanciamento del carico per gestire le query che contribuiscono maggiormente al carico del database nel cluster DB. L'endpoint reader indirizza queste istruzioni alle Aurora Read Repliche e riduce il carico sull'istanza principale. L'endpoint reader ridimensiona inoltre la capacità di gestire le query SELECT simultanee in base al numero di Aurora Read Repliche nel cluster.

Per ulteriori informazioni, vedere Aggiungere repliche Aurora a un cluster DB e Gestione delle prestazioni e della scalabilità per i cluster Aurora DB.

Colonne del report

- Stato

- Regione
- Risorsa
- Aumento della lettura (numero) del database
- Ultimo periodo di rilevamento
- Ora ultimo aggiornamento

Dimensionamento automatico di Amazon DynamoDB non abilitato

Descrizione

Controlla se per le tabelle e gli indici secondari globali di Amazon DynamoDB è abilitato il dimensionamento automatico o su richiesta.

Il dimensionamento automatico di Amazon DynamoDB utilizza il servizio Application Auto Scaling per regolare in modo dinamico la capacità effettiva di trasmissione assegnata automaticamente in risposta ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione. Quando il carico di lavoro diminuisce, Application Auto Scaling riduce la velocità effettiva in modo da non dover pagare per la capacità assegnata inutilizzata.

È possibile modificare la configurazione del controllo utilizzando i parametri AWS Config delle regole.

Per ulteriori informazioni, consulta Gestione della capacità effettiva di trasmissione con il dimensionamento automatico di DynamoDB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz136`

Origine

AWS Config Regola gestita: dynamodb-autoscaling-enabled

Criteri di avviso

Giallo: il dimensionamento automatico non è abilitato per le tabelle di DynamoDB e/o gli indici secondari globali.

Operazione consigliata

A meno che non tu disponga già di un meccanismo per il dimensionamento automatico della velocità di trasmissione effettiva assegnata delle tabelle di DynamoDB e/o degli indici secondari globali in base ai requisiti del carico di lavoro, valuta l'opportunità di attivare il dimensionamento automatico per le tabelle di Amazon DynamoDB.

Per ulteriori informazioni, consulta Utilizzo della Console di gestione AWS con il dimensionamento automatico di DynamoDB.

Risorse aggiuntive

Gestione automatica della capacità effettiva di trasmissione con il dimensionamento automatico di DynamoDB

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Ottimizzazione Amazon EBS non abilitata

Descrizione

Controlla se l'ottimizzazione Amazon EBS è abilitata per le istanze di Amazon EC2.

Un'istanza ottimizzata per Amazon EBS utilizza uno stack di configurazione ottimizzato e offre capacità aggiuntiva dedicata per l'I/O di Amazon EBS. Questa ottimizzazione offre prestazioni

ottimali per i volumi di Amazon EBS, riducendo al minimo i conflitti tra l'I/O di Amazon EBS e l'altro traffico proveniente dall'istanza.

Per ulteriori informazioni, consulta Istanze ottimizzate per Amazon EBS.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz142`

Origine

AWS Config Regola gestita: ebs-optimized-instance

Criteri di avviso

Giallo: l'ottimizzazione di Amazon EBS non è abilitata su istanze di Amazon EC2 supportate.

Operazione consigliata

Attiva l'ottimizzazione di Amazon EBS sulle istanze supportate.

Per ulteriori informazioni, consulta Abilitazione dell'ottimizzazione EBS all'avvio.

Risorse aggiuntive

Istanze ottimizzate per Amazon EBS

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Configurazione degli allegati di Volume (SSD) IOPS con provisioning Amazon EBS

Descrizione

Controlli per volumi (SSD) IOPS con provisioning associati a un'istanza Amazon EBS ottimizzabile di Amazon Elastic Compute Cloud (Amazon EC2) e che non è ottimizzata per EBS.

I volumi (SSD) IOPS con provisioning nell'Amazon Elastic Block Store (Amazon EBS) sono progettati per fornire le prestazioni previste solo quando sono associati a un'istanza ottimizzata per EBS.

ID di controllo

`PPkZrjsH2q`

Criteri di avviso

Giallo: un'istanza Amazon EC2 che può essere ottimizzata per EBS ha un volume di capacità di IOPS allocata (SSD) associato ma l'istanza non è ottimizzata per EBS.

Operazione consigliata

Crea una nuova istanza ottimizzata per EBS, scollega il volume e ricollegalo alla nuova istanza. Per ulteriori informazioni, consulta Istanze ottimizzate per Amazon EBS e Collegamento di un volume Amazon EBS a un'istanza.

Risorse aggiuntive

- Tipi di volume Amazon EBS
- Prestazioni di volume Amazon EBS

Colonne del report

- Stato
- Regione/AZ
- ID volume
- Nome volume
- Allegato volume
- ID istanza
- Tipo di istanza
- Ottimizzazione per EBS

Volumi Amazon EBS con provisioning insufficiente

Descrizione

Controlla i volumi Amazon Elastic Block Store (Amazon EBS) in esecuzione in qualsiasi momento durante il periodo di ricerca posticipata. Questo controllo avvisa se alcuni volumi EBS sono stati sottoposti a provisioning insufficiente per i carichi di lavoro. Un utilizzo elevato e costante può indicare prestazioni ottimizzate e costanti, ma può anche indicare che un'applicazione non dispone di risorse sufficienti.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`C0r6dfpM04`

Criteri di avviso

Giallo: un volume EBS sottoposto a provisioning insufficiente durante il periodo di ricerca posticipata. Per determinare se il provisioning di un volume è insufficiente, prendiamo in considerazione tutte le CloudWatch metriche predefinite (inclusi IOPS e throughput). L'algoritmo utilizzato per identificare i volumi EBS con fornitura insufficiente segue le best practice. AWS L'algoritmo viene aggiornato quando viene identificato un nuovo modello.

Operazione consigliata

Valuta la possibilità di ridimensionare i volumi con un utilizzo elevato.

Per ulteriori informazioni, consulta Attiva AWS Compute Optimizer i Trusted Advisor controlli.

Colonne del report

- Stato
- Regione
- ID volume
- Tipo di volume

- Dimensioni volume
- Volume IOPS di base
- Volume IOPS moderato
- Volume velocità di trasmissione effettiva moderata
- Tipo di volume consigliato
- Dimensione volume consigliata (GB)
- Volume IOPS di base consigliato
- Volume IOPS moderata consigliato
- Volume velocità di trasmissione effettiva di base consigliato
- Volume velocità di trasmissione effettiva moderata consigliato
- Periodo di ricerca posticipata (giorni)
- Rischio prestazioni
- Ora ultimo aggiornamento

Il gruppo con dimensionamento automatico Amazon EC2 non è associato a un modello di avvio

Descrizione

Controlla se un gruppo con dimensionamento automatico Amazon EC2 viene creato da un modello di avvio di Amazon EC2.

Usa un modello di avvio per creare gruppi con dimensionamento automatico Amazon EC2 per garantire l'accesso alle funzionalità e ai miglioramenti più recenti del gruppo con dimensionamento automatico. Ad esempio, il controllo delle versioni e più tipi di istanze.

Per ulteriori informazioni, consulta Modelli di avvio.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz102`

Origine

AWS Config Regola gestita: autoscaling-launch-template

Criteri di avviso

Giallo: il gruppo con dimensionamento automatico Amazon EC2 non è associato a un modello di avvio valido.

Operazione consigliata

Utilizza un modello di avvio di Amazon EC2 per creare gruppi con dimensionamento automatico Amazon EC2.

Per ulteriori informazioni, consulta Creazione di un modello di avvio per un gruppo con dimensionamento automatico.

Risorse aggiuntive

- Modelli di avvio
- Creazione di un modello di avvio

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Ottimizzazione della velocità effettiva da Amazon EC2 a EBS

Descrizione

Controlla i volumi Amazon EBS le cui prestazioni potrebbero essere influenzate dalla capacità di velocità effettiva massima dell'istanza Amazon EC2 a cui sono associati.

Per ottimizzare le prestazioni, si consiglia di assicurarsi che la velocità effettiva massima di un'istanza Amazon EC2 sia superiore alla velocità effettiva massima aggregata dei volumi EBS

associati. Questo controllo calcola la velocità effettiva totale del volume EBS per ogni periodo di cinque minuti del giorno precedente (in base all'ora UTC) per ogni istanza ottimizzata per EBS, e notifica se l'utilizzo in più della metà di tali periodi era superiore al 95% della velocità effettiva massima dell'istanza EC2.

ID di controllo

`Bh2xRR2FGH`

Criteri di avviso

Giallo: nel giorno precedente (UTC), la velocità di trasmissione effettiva aggregata (megabyte/secondo) dei volumi EBS collegati all'istanza EC2 ha superato il 95% della velocità pubblicata tra l'istanza e i volumi EBS per oltre il 50% del tempo.

Operazione consigliata

Confronta la velocità di trasmissione effettiva massima dei volumi Amazon EBS (consulta Tipi di volume Amazon EBS) con quella massima dell'istanza Amazon EC2 a cui sono associati. Consulta Tipi di istanze che supportano l'ottimizzazione per EBS.

Valuta la possibilità di collegare i volumi a un'istanza che supporti una velocità di trasmissione effettiva più elevata in Amazon EBS per ottenere prestazioni ottimali.

Risorse aggiuntive

- Tipi di volume Amazon EBS
- Istanze ottimizzate per Amazon EBS
- Monitoraggio dello stato dei volumi
- Collegamento di un volume Amazon EBS a un'istanza
- Distaccamento di un volume Amazon EBS da un'istanza
- Eliminazione di un volume Amazon EBS

Colonne del report

- Stato
- Regione
- ID istanza
- Tipo di istanza
- Tempo vicino al limite massimo

Il tipo di virtualizzazione EC2 è paravirtuale

Descrizione

Controlla se il tipo di virtualizzazione di un'istanza di Amazon EC2 è paravirtuale.

È preferibile utilizzare istanze Hardware Virtual Machine (HVM) anziché istanze paravirtuali, quando possibile. Il motivo risiede nei miglioramenti apportati alla virtualizzazione HVM e alla disponibilità di driver PV per AMI HVM, che hanno colmato il divario di prestazioni che storicamente esisteva tra guest PV e HVM. È importante tenere conto che i tipi di istanze di generazioni precedenti non supportano le AMI PV. Pertanto, la scelta di un tipo di istanza di HVM offre le migliori prestazioni e compatibilità con l'hardware moderno.

Per ulteriori informazioni, consulta Tipi di virtualizzazione delle AMI Linux.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz148`

Origine

AWS Config Regola gestita: ec2-paravirtual-instance-check

Criteri di avviso

Giallo: il tipo di virtualizzazione di istanze di Amazon EC2 è paravirtuale.

Operazione consigliata

Utilizza la virtualizzazione HVM per le istanze di Amazon EC2 e utilizza un tipo di istanza compatibile.

Per informazioni sulla scelta del tipo di virtualizzazione appropriato, consulta Compatibilità per la modifica del tipo di istanza.

Risorse aggiuntive

Compatibilità per la modifica del tipo di istanza

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Limite massimo di memoria di Amazon ECS

Descrizione

Controlla se per le definizioni delle attività di Amazon ECS è impostato un limite di memoria per le relative definizioni dei container. La quantità totale di memoria riservata per tutti i container in un'attività deve essere inferiore al valore della memoria dell'attività.

Per ulteriori informazioni, consulta Definizioni dei container.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz176`

Origine

AWS Config Regola gestita: ecs-task-definition-memory -hard-limit

Criteri di avviso

Giallo: il limite massimo di memoria di Amazon ECS non è impostato.

Operazione consigliata

Alloca memoria per le attività di Amazon ECS per evitare l'esaurimento della memoria. Se il container tenta di superare la memoria specificata, il container sarà terminato.

Per ulteriori informazioni, consulta Come allocare memoria alle attività in Amazon ECS?.

Risorse aggiuntive

Prenotazione di cluster

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Ottimizzazione della modalità di velocità di trasmissione effettiva di Amazon EFS

Descrizione

Controlla se il file system di Amazon EFS del cliente è attualmente configurato per l'uso della modalità Bursting Throughput (velocità di trasmissione effettiva).

I file system in modalità Bursting Throughput [1] di EFS offrono un livello di velocità di trasmissione effettiva di base costante (50 KiB/s per GiB di dati nell'archiviazione EFS Standard) e utilizzano un modello di crediti per offrire livelli più elevati di prestazioni di "velocità di trasmissione effettiva burst" quando sono disponibili "crediti burst". Quando si esauriscono i crediti burst, le prestazioni del file system vengono limitate a un livello di base inferiore, il che può comportare rallentamenti, timeout o altre conseguenze sulle prestazioni per gli utenti finali o le applicazioni.

ID di controllo

`c1dfprch02`

Criteri di avviso

- Giallo: il file system utilizza la modalità Bursting throughput (velocità di trasmissione effettiva).

Operazione consigliata

Per consentire agli utenti e alle applicazioni di raggiungere la velocità di trasmissione effettiva desiderata, è preferibile aggiornare la configurazione del file system alla modalità Elastic Throughput [2]. In modalità Elastic Throughput, il file system può raggiungere fino a 10 GiB/s di velocità di trasmissione effettiva in lettura o 3 GiB/s di velocità di trasmissione effettiva in scrittura, a seconda della regione AWS [3], per cui si paga solo per la velocità di trasmissione effettiva utilizzata. Tieni presente che puoi aggiornare la configurazione del file system per passare su richiesta dalla modalità di velocità di trasmissione effettiva di tipo Elastic a quella Bursting e che i file system in modalità Elastic addebitano costi aggiuntivi per il trasferimento dei dati [4].

Risorse aggiuntive

- [1] Modalità di velocità di trasmissione effettiva per le prestazioni di Amazon EFS
- [2] Modalità di velocità di trasmissione effettiva Elastic per le prestazioni di Amazon EFS
- [3] Quote e limiti di Amazon EFS
- [4] Prezzi di Amazon EFS

Colonne del report

- Stato
- Regione
- ID dei file system EFS
- Modalità di velocità di trasmissione effettiva
- Ora ultimo aggiornamento

Il parametro Amazon RDS autovacuum è disattivato

Descrizione

Il parametro autovacuum è disattivato per le tue istanze DB. La disattivazione dell'autovacuum aumenta il volume della tabella e dell'indice e influisce sulle prestazioni.

Ti consigliamo di attivare l'autovacuum nei gruppi di parametri del database.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt025`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno l'autovacuum disattivato.

Operazione consigliata

Attiva il parametro autovacuum nei gruppi di parametri DB.

Risorse aggiuntive

Il database PostgreSQL richiede una manutenzione periodica, nota come vacuuming. Autovacuum in PostgreSQL automatizza l'esecuzione dei comandi VACCUUM e ANALYZE. Questo processo raccoglie le statistiche della tabella ed elimina le righe morte. Quando l'autovacuum è disattivato, l'aumento della tabella, l'aumento della tabella, l'aumento dell'indice e le statistiche obsolete influiranno sulle prestazioni del database.

Per ulteriori informazioni, consulta Understanding autovacuum in ambienti Amazon RDS for PostgreSQL.

Colonne del report

- Stato
- Regione

- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

I cluster Amazon RDS DB supportano solo volumi fino a 64 TiB

Descrizione

I tuoi cluster DB supportano volumi fino a 64 TiB. Le ultime versioni del motore supportano volumi fino a 128 TiB. Ti consigliamo di aggiornare la versione del motore del tuo cluster DB alle versioni più recenti per supportare volumi fino a 128 TiB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt017`

Criteri di avviso

Giallo: i cluster DB supportano solo volumi fino a 64 TiB.

Operazione consigliata

Aggiorna la versione del motore dei tuoi cluster DB per supportare volumi fino a 128 TiB.

Risorse aggiuntive

Quando scalate la vostra applicazione su un singolo cluster Amazon Aurora DB, potreste non raggiungere il limite se il limite di storage è di 128 TiB. L'aumento del limite di storage aiuta a evitare l'eliminazione dei dati o la divisione del database su più istanze.

Per ulteriori informazioni, consulta i limiti di dimensione di Amazon Aurora.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome del motore
- Versione del motore attuale
- Valore consigliato
- Ora ultimo aggiornamento

Istanze database Amazon RDS nei cluster con classi di istanze eterogenee

Descrizione

Ti consigliamo di utilizzare la stessa classe e dimensione dell'istanza DB per tutte le istanze DB del tuo cluster di database.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt009`

Criteri di avviso

Rosso: i cluster DB dispongono di istanze DB con classi di istanze eterogenee.

Operazione consigliata

Usa la stessa classe e dimensione di istanze per tutte le istanze DB del tuo cluster di database.

Risorse aggiuntive

Quando le istanze DB del cluster di database utilizzano classi o dimensioni di istanze DB diverse, può verificarsi uno squilibrio nel carico di lavoro per le istanze DB. Durante un failover, una delle istanze DB di lettura diventa un'istanza DB writer. Se le istanze DB utilizzano la stessa classe e dimensione dell'istanza DB, il carico di lavoro può essere bilanciato per le istanze DB del cluster DB.

Per ulteriori informazioni, consulta Aurora Replicas.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Istanze database di Amazon RDS nei cluster con dimensioni di istanze eterogenee

Descrizione

Ti consigliamo di utilizzare la stessa classe e dimensione dell'istanza DB per tutte le istanze DB del tuo cluster di database.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt008`

Criteri di avviso

Rosso: i cluster DB hanno istanze DB con dimensioni di istanze eterogenee.

Operazione consigliata

Usa la stessa classe e dimensione di istanze per tutte le istanze DB del tuo cluster di database.

Risorse aggiuntive

Quando le istanze DB del cluster di database utilizzano classi o dimensioni di istanze DB diverse, può verificarsi uno squilibrio nel carico di lavoro per le istanze DB. Durante un failover, una delle

istanze DB di lettura diventa un'istanza DB writer. Se le istanze DB utilizzano la stessa classe e dimensione dell'istanza DB, il carico di lavoro può essere bilanciato per le istanze DB del cluster DB.

Per ulteriori informazioni, consulta Aurora Replicas.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

I parametri di memoria DB di Amazon RDS sono diversi da quelli predefiniti

Descrizione

I parametri di memoria delle istanze DB sono significativamente diversi dai valori predefiniti. Queste impostazioni possono influire sulle prestazioni e causare errori.

Si consiglia di ripristinare i parametri di memoria personalizzati per l'istanza DB ai valori predefiniti nel gruppo di parametri DB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.

Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt020`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno parametri di memoria che differiscono notevolmente dai valori predefiniti.

Operazione consigliata

Reimposta i parametri di memoria ai valori predefiniti.

Risorse aggiuntive

Per ulteriori informazioni, consulta Best practice per la configurazione dei parametri per Amazon RDS for MySQL, parte 1: Parametri relativi alle prestazioni.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro Amazon RDS enable_indexonlyscan è disattivato

Descrizione

Il pianificatore o l'ottimizzatore di query non possono utilizzare il tipo di piano di scansione indicizzato solo quando è disattivato.

Si consiglia di impostare il valore del parametro enable_indexonlyscan su 1.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt028`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno il parametro enable_indexonlyscan disattivato.

Operazione consigliata

Imposta il parametro enable_indexonlyscan su 1.

Risorse aggiuntive

Quando si disattiva il parametro enable_indexonlyscan, si impedisce al pianificatore di query di selezionare un piano di esecuzione ottimale. Il pianificatore di query utilizza un tipo di piano diverso, come la scansione dell'indice, che può aumentare il costo delle query e i tempi di esecuzione. Il tipo di piano di scansione basato esclusivamente sull'indice recupera i dati senza accedere ai dati della tabella.

Per ulteriori informazioni, vedere enable_indexonlyscan (boolean) sul sito Web della documentazione di PostgreSQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro Amazon RDS enable_indexscan è disattivato

Descrizione

Il pianificatore o l'ottimizzatore di query non può utilizzare il tipo di piano di scansione dell'indice quando è disattivato.

Si consiglia di impostare il valore del parametro enable_indexscan su 1.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt029`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno il parametro enable_indexscan disattivato.

Operazione consigliata

Imposta il parametro enable_indexscan su 1.

Risorse aggiuntive

Quando si disattiva il parametro enable_indexscan, si impedisce al pianificatore di query di selezionare un piano di esecuzione ottimale. Il pianificatore di query utilizza un tipo di piano diverso, come la scansione dell'indice, che può aumentare il costo delle query e i tempi di esecuzione.

Per ulteriori informazioni, vedere enable_indexscan (boolean) sul sito Web della documentazione di PostgreSQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro general_logging di Amazon RDS è attivato

Descrizione

La registrazione generale è attivata per l'istanza DB. Questa impostazione è utile per la risoluzione dei problemi del database. Tuttavia, l'attivazione della registrazione generale aumenta la quantità di operazioni di I/O e lo spazio di archiviazione allocato, il che potrebbe causare conflitti e un peggioramento delle prestazioni.

Verifica i tuoi requisiti per l'utilizzo generale della registrazione. Ti consigliamo di impostare il valore del parametro general_logging su 0.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt037`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno general_logging attivato.

Operazione consigliata

Verifica i tuoi requisiti per l'utilizzo generale della registrazione. Se non è obbligatorio, ti consigliamo di impostare il valore del parametro general_logging su 0.

Risorse aggiuntive

Il registro delle interrogazioni generali è attivato quando il valore del parametro general_logging è 1. Il registro delle interrogazioni generale contiene i record delle operazioni del server di database. Il server scrive informazioni in questo registro quando i client si connettono o si disconnettono e i log contengono ogni istruzione SQL ricevuta dai client. Il registro delle interrogazioni generale è utile quando si sospetta un errore in un client e si desidera trovare le informazioni che il client deve inviare al server del database.

Per ulteriori informazioni, vedere Panoramica dei log del database RDS for MySQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Parametro Amazon RDS Innodb_change_buffering che utilizza un valore inferiore a quello ottimale

Descrizione

Il buffering delle modifiche consente a un'istanza DB MySQL di posticipare alcune scritture, necessarie per mantenere gli indici secondari. Questa funzionalità era utile in ambienti con dischi lenti. La modifica della configurazione del buffering ha migliorato leggermente le prestazioni del DB, ma ha causato un ritardo nel ripristino in caso di arresto anomalo e lunghi tempi di spegnimento durante l'aggiornamento.

Ti consigliamo di impostare il valore del parametro innodb_change_buffering su NONE.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.

Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt021`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno il parametro innodb_change_buffering impostato su un valore ottimale basso.

Operazione consigliata

Imposta il valore del parametro innodb_change_buffering su NONE nei gruppi di parametri DB.

Risorse aggiuntive

Per ulteriori informazioni, consulta Best practice per la configurazione dei parametri per Amazon RDS for MySQL, parte 1: Parametri relativi alle prestazioni.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro innodb_open_files di Amazon RDS è basso

Descrizione

Il parametro innodb_open_files controlla il numero di file che InnoDB può aprire contemporaneamente. InnoDB apre tutti i file di log e di tablespace di sistema quando mysqld è in esecuzione.

Il valore del numero massimo di file dell'istanza database che InnoDB può aprire contemporaneamente non è sufficiente. Ti consigliamo di impostare il parametro innodb_open_files su un valore minimo di 65.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt033`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno l'impostazione dei file aperti di InnoDB non configurata correttamente.

Operazione consigliata

Imposta il parametro innodb_open_files su un valore minimo di 65.

Risorse aggiuntive

Il parametro innodb_open_files controlla il numero di file che InnoDB può aprire contemporaneamente. InnoDB mantiene aperti tutti i file di registro e i file del tablespace di sistema quando mysqld è in esecuzione. InnoDB deve anche aprire alcuni file.ibd, se viene utilizzato il modello di file-per-table archiviazione. Quando l'impostazione innodb_open_files è bassa, influisce sulle prestazioni del database e il server potrebbe non avviarsi.

Per ulteriori informazioni, consulta InnoDB Startup Options and System Variables - innodb_open_files sul sito Web della documentazione. MySql

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro innodb_stats_persistent di Amazon RDS è disattivato

Descrizione

L'istanza database non è configurata per memorizzare le statistiche InnoDB sul disco. Quando le statistiche non vengono archiviate, vengono ricalcolate ogni volta che l'istanza si riavvia e si accede alla tabella. Ciò porta a variazioni nel piano di esecuzione delle query. Puoi modificare il valore di questo parametro globale a livello di tabella.

Ti consigliamo di impostare il valore del parametro innodb_stats_persistent su ON.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt032`

Criteri di avviso

Giallo: i gruppi di parametri DB contengono statistiche di ottimizzazione che non sono persistenti sul disco.

Operazione consigliata

Imposta il valore del parametro innodb_stats_persistent su ON.

Risorse aggiuntive

Se il parametro innodb_stats_persistent è impostato su ON, le statistiche dell'ottimizzatore vengono mantenute al riavvio dell'istanza. Ciò migliora la stabilità del piano di esecuzione e le prestazioni coerenti delle query. È possibile modificare la persistenza delle statistiche globali a livello di tabella utilizzando la clausola STATS_PERSISTENT quando si crea o si modifica una tabella.

Per ulteriori informazioni, consulta Best practice per la configurazione dei parametri per Amazon RDS for MySQL, parte 1: Parametri relativi alle prestazioni.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Istanza Amazon RDS con capacità di sistema insufficiente

Descrizione

Verifica se l'istanza Amazon RDS o l'istanza Amazon Aurora DB ha la capacità di sistema richiesta per funzionare.

ID di controllo

`c1qf5bt039`

Criteri di avviso

Giallo:

Uccisioni in caso di esaurimento della memoria: quando un processo sull'host del database viene interrotto a causa della riduzione della memoria a livello del sistema operativo, il contatore di uccisioni della memoria esaurita (OOM) aumenta.

Scambio eccessivo: i valori delle metriche os.memory.swap.in e os.memory.swap.out erano elevati.

Operazione consigliata

Si consiglia di ottimizzare le query in modo da utilizzare meno memoria o utilizzare un tipo di istanza DB con una maggiore quantità di memoria allocata. Quando la memoria dell'istanza sta esaurendo, ciò influisce sulle prestazioni del database.

Risorse aggiuntive

Sono state rilevate ut-of-memory uccisioni O: il kernel Linux richiama l'Out of Memory (OOM) Killer quando i processi in esecuzione sull'host richiedono più della memoria fisicamente disponibile dal sistema operativo. In questo caso, OOM Killer esamina tutti i processi in esecuzione e arresta uno o più processi per liberare memoria di sistema e mantenere il sistema in funzione.

Viene rilevato lo scambio: quando la memoria sull'host del database non è sufficiente, il sistema operativo invia alcune pagine minime utilizzate al disco nello spazio di swap. Questo processo di offloading influisce sulle prestazioni del database.

Per ulteriori informazioni, consulta Tipi di istanze Amazon RDS e scalabilità dell'istanza Amazon RDS.

Colonne del report

- Stato
- Regione
- Risorsa
- O ut-of-memory uccide (conta)
- Scambio eccessivo (numero)
- Ultimo periodo di rilevamento
- Ora ultimo aggiornamento

Il volume magnetico Amazon RDS è in uso

Descrizione

Le tue istanze DB utilizzano lo storage magnetico. L'archiviazione magnetica non è consigliata per la maggior parte delle istanze DB. Scegli un tipo di storage diverso: General Purpose (SSD) o Provisioned IOPS.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt000`

Criteri di avviso

Giallo: le risorse Amazon RDS utilizzano lo storage magnetico.

Operazione consigliata

Scegli un tipo di storage diverso: General Purpose (SSD) o Provisioned IOPS.

Risorse aggiuntive

L'archiviazione magnetica è un tipo di archiviazione di generazione precedente. Il General Purpose (SSD) o Provisioned IOPS è il tipo di storage consigliato per i nuovi requisiti di

archiviazione. Questi tipi di storage offrono prestazioni più elevate e costanti e opzioni di dimensioni di archiviazione migliorate.

Per ulteriori informazioni, vedere Volumi di generazione precedente.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

I gruppi di parametri Amazon RDS non utilizzano pagine enormi

Descrizione

Le pagine di grandi dimensioni possono aumentare la scalabilità del database, ma l'istanza DB non utilizza pagine di grandi dimensioni. Ti consigliamo di impostare il valore del parametro use_large_pages su ONLY nel gruppo di parametri DB per la tua istanza DB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt024`

Criteri di avviso

Giallo: i gruppi di parametri DB non utilizzano pagine di grandi dimensioni.

Operazione consigliata

Imposta il valore del parametro use_large_pages su ONLY nei gruppi di parametri DB.

Risorse aggiuntive

Per ulteriori informazioni, consulta Attivazione di un'istanza RDS HugePages for Oracle.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro della cache delle query di Amazon RDS è attivato

Descrizione

Quando le modifiche richiedono l'eliminazione della cache delle query, l'istanza DB sembrerà bloccarsi. La maggior parte dei carichi di lavoro non beneficia della cache delle query. La cache delle query è stata rimossa da MySQL versione 8.0. Ti consigliamo di impostare il parametro query_cache_type su 0.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt022`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno la cache delle query attivata.

Operazione consigliata

Imposta il valore del parametro query_cache_type su 0 nei gruppi di parametri DB.

Risorse aggiuntive

Per ulteriori informazioni, consulta Best practice per la configurazione dei parametri per Amazon RDS for MySQL, parte 1: Parametri relativi alle prestazioni.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

È richiesto l'aggiornamento della classe di istanza delle risorse Amazon RDS

Descrizione

Il database esegue una classe di istanza DB di generazione precedente. Abbiamo sostituito le classi di istanze DB di una generazione precedente con classi di istanze DB con costi e

prestazioni migliori o entrambi. Ti consigliamo di eseguire l'istanza DB con una classe di istanza DB di nuova generazione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt015`

Criteri di avviso

Rosso: le istanze DB utilizzano una classe di istanze DB di fine supporto.

Operazione consigliata

Esegui l'aggiornamento alla classe di istanza DB più recente.

Risorse aggiuntive

Per ulteriori informazioni, consulta Motori di database supportati per tutte le classi di istanza database disponibili.

Colonne del report

- Stato
- Regione
- Risorsa

- Classe di istanza database
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Risorse Amazon RDS: è richiesto l'aggiornamento delle versioni principali

Descrizione

I database con l'attuale versione principale del motore DB non saranno supportati. Ti consigliamo di eseguire l'aggiornamento alla versione principale più recente che include nuove funzionalità e miglioramenti.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt014`

Criteri di avviso

Rosso: le risorse RDS utilizzano versioni principali di fine supporto.

Operazione consigliata

Effettua l'aggiornamento alla versione principale più recente per il motore DB.

Risorse aggiuntive

Amazon RDS rilascia nuove versioni per i motori di database supportati per mantenere i database con la versione più recente. Le nuove versioni rilasciate possono includere correzioni di bug, miglioramenti della sicurezza e altri miglioramenti per il motore di database. È possibile ridurre al minimo i tempi di inattività necessari per l'aggiornamento dell'istanza DB utilizzando una distribuzione blu/verde.

Per ulteriori informazioni, consulta le seguenti risorse:

- Aggiornamento di una versione del motore di istanze DB
- Aggiornamenti di Amazon Aurora
- Utilizzo di Amazon RDS Blue/Green Deployments per gli aggiornamenti del database

Colonne del report

- Stato
- Regione
- Risorsa
- Nome del motore
- Versione attuale del motore
- Valore consigliato
- Ora ultimo aggiornamento

Risorse Amazon RDS che utilizzano End of Support Engine Edition con licenza inclusa

Descrizione

Ti consigliamo di aggiornare la versione principale all'ultima versione del motore supportata da Amazon RDS per continuare con il supporto della licenza corrente. La versione del motore del database non sarà supportata con la licenza corrente.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt016`

Criteri di avviso

Rosso: le risorse Amazon RDS utilizzano l'edizione End of Support Engine nel modello con licenza inclusa.

Operazione consigliata

Ti consigliamo di aggiornare il database all'ultima versione supportata in Amazon RDS per continuare a utilizzare il modello con licenza.

Risorse aggiuntive

Per ulteriori informazioni, consulta gli aggiornamenti delle versioni principali di Oracle.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome del motore
- Versione del motore attuale
- Valore consigliato
- Nome del motore

- Ora ultimo aggiornamento

Set di registri delle risorse Alias Amazon Route 53

Descrizione

Controlla i set di registri delle risorse che possono essere modificati in set di registri delle risorse alias per migliorare le prestazioni e risparmiare.

Un set di record di risorse alias indirizza le query DNS verso una AWS risorsa (ad esempio, un sistema di bilanciamento del carico Elastic Load Balancing o un bucket Amazon S3) o verso un altro set di record di risorse Route 53. Quando utilizzi set di record di risorse alias, Route 53 indirizza le tue query DNS verso le risorse gratuitamente. AWS

Le zone ospitate create dai AWS servizi non verranno visualizzate nei risultati del controllo.

ID di controllo

`B913Ef6fb4`

Criteri di avviso

- Giallo: un set di record delle risorse è un CNAME per un sito Web Amazon S3.
- Giallo: un set di record di risorse è un CNAME per una CloudFront distribuzione Amazon.
- Giallo: un set di record delle risorse è un CNAME per un load balancer di Elastic Load Balancing.

Operazione consigliata

Sostituisci i set di registri delle risorse CNAME elencati con set di registri delle risorse alias. Consulta Scelta tra record alias e non alias.

È inoltre necessario modificare il tipo di record da CNAME a A o AAAA, a seconda della risorsa. AWS Consulta Valori che è necessario specificare durante la creazione o la modifica di set di registri delle risorse di Amazon Route 53.

Risorse aggiuntive

Instradamento delle interrogazioni alle risorse AWS

Colonne del report

- Stato
- Nome della zona ospitata

- ID della zona ospitata
- Nome del set di registri delle risorse
- Tipo di set di registri delle risorse
- Identificativo del set di record delle risorse
- Destinazione alias

Funzioni AWS Lambda con provisioning insufficiente per la dimensione della memoria

Descrizione

Controlla le AWS Lambda funzioni che sono state richiamate almeno una volta durante il periodo di lookback. Questo controllo ti avvisa se una qualsiasi delle funzioni Lambda è stata sottoposta a provisioning insufficiente per le dimensioni della memoria. Quando si dispone di funzioni Lambda sottoposte a provisioning insufficiente per le dimensioni della memoria, queste funzioni richiedono più tempo per essere completate.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`C0r6dfpM06`

Criteri di avviso

Giallo: una funzione Lambda sottoposta a provisioning insufficiente per le dimensioni della memoria durante il periodo di ricerca posticipata. Per determinare se il provisioning di una funzione Lambda è insufficiente, consideriamo tutte le metriche predefinite CloudWatch per quella funzione. L'algoritmo utilizzato per identificare le funzioni Lambda non sufficientemente fornite per quanto riguarda le dimensioni della memoria segue le best practice. AWS L'algoritmo viene aggiornato quando viene identificato un nuovo modello.

Operazione consigliata

Valuta la possibilità di aumentare le dimensioni della memoria delle funzioni Lambda.

Per ulteriori informazioni, consulta Attiva AWS Compute Optimizer i Trusted Advisor controlli.

Colonne del report

- Stato
- Regione
- Nome funzione
- Versione della funzione
- Dimensioni della memoria (MB)
- Dimensioni della memoria consigliate (MB)
- Periodo di ricerca posticipata (giorni)
- Rischio prestazioni
- Ora ultimo aggiornamento

AWS Lambda Funzioni senza limite di concorrenza configurate

Descrizione

Verifica se AWS Lambda le funzioni sono configurate con un limite di esecuzione simultanea a livello di funzione.

La simultaneità si riferisce al numero di richieste in corso che la funzione AWS Lambda può gestire contemporaneamente. Per ogni richiesta simultanea, Lambda fornisce un'istanza separata del tuo ambiente di esecuzione.

È possibile specificare il limite di concorrenza minimo e massimo utilizzando i parametri Concurrency LimitLow e ConcurrencyLimitHigh nelle regole. AWS Config

Per ulteriori informazioni, consulta Lambda function scaling (Dimensionamento della funzione Lambda).

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz181`

Origine

AWS Config Regola gestita: lambda-concurrency-check

Criteri di avviso

Giallo: per la funzione Lambda non sono configurati limiti di simultaneità.

Operazione consigliata

Assicurati che per le funzioni Lambda sia configurata la simultaneità. Un limite di simultaneità per le funzioni Lambda contribuisce a garantire che la funzione elabori le richieste in modo affidabile e prevedibile. Un limite di simultaneità riduce il rischio che la funzione venga sovraccaricata a causa di un improvviso aumento del traffico.

Per ulteriori informazioni, consulta Configurazione della simultaneità riservata.

Risorse aggiuntive

- Dimensionamento della funzione Lambda
- Configurazione della simultaneità riservata

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Problemi ad alto rischio di AWS Well-Architected per le prestazioni

Descrizione

Verifica problemi ad alto rischio (HRI) per i carichi di lavoro nel pilastro delle prestazioni. Questo controllo è basato sulle tue revisioni di AWS-Well Architected. I risultati dei controlli dipendono dal completamento della valutazione del carico di lavoro con AWS Well-Architected.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Wxdfp4B1L2`

Criteri di avviso

- Rosso: almeno un problema attivo ad alto rischio è stato identificato nel pilastro delle prestazioni di AWS Well-Architected.
- Verde: non sono stati rilevati problemi attivi ad alto rischio nel pilastro delle prestazioni di AWS Well-Architected.

Operazione consigliata

AWS Well-Architected ha rilevato problemi ad alto rischio durante la valutazione del carico di lavoro. Questi problemi offrono opportunità per ridurre i rischi e risparmiare denaro. Accedi allo strumento AWS Well-Architected per rivedere le tue risposte e risolvere i problemi attivi.

Colonne del report

- Stato
- Regione
- ARN del carico di lavoro
- Nome del carico di lavoro
- Nome del revisore
- Tipo di carico di lavoro
- Data di inizio del carico di lavoro
- Data dell'ultima modifica del carico di lavoro
- Numero di HRI identificati per Prestazioni
- Numero di HRI risolti per Prestazioni
- Numero di domande risposte per Prestazioni

- Numero totale di domande nel pilastro Prestazioni
- Ora ultimo aggiornamento

CloudFront Nomi di dominio alternativi

Descrizione

Verifica la presenza di nomi di dominio alternativi (CNAMES) CloudFront nelle distribuzioni Amazon con impostazioni DNS configurate in modo errato.

Se una CloudFront distribuzione include nomi di dominio alternativi, la configurazione DNS per i domini deve indirizzare le query DNS a quella distribuzione.

> **Note**
>
> Questo controllo presuppone che il DNS di Amazon Route 53 e la CloudFront distribuzione Amazon siano configurati nello stesso modo. Account AWS Pertanto, l'elenco di avvisi potrebbe includere risorse altrimenti funzionanti come previsto a causa dell'impostazione DNS al di fuori di questo Account AWS.

ID di controllo

`N420c450f2`

Criteri di avviso

- Giallo: una CloudFront distribuzione include nomi di dominio alternativi, ma la configurazione DNS non è configurata correttamente con un record CNAME o un record di risorse alias Amazon Route 53.
- Giallo: una CloudFront distribuzione include nomi di dominio alternativi, ma non Trusted Advisor può valutare la configurazione DNS perché c'erano troppi reindirizzamenti.
- Giallo: una CloudFront distribuzione include nomi di dominio alternativi, ma non è stata in Trusted Advisor grado di valutare la configurazione DNS per qualche altro motivo, molto probabilmente a causa di un timeout.

Operazione consigliata

Aggiorna la configurazione DNS per indirizzare le query DNS alla CloudFront distribuzione; vedi Utilizzo di nomi di dominio alternativi (CNames).

Se utilizzi Amazon Route 53 come servizio DNS, consulta Routing del traffico verso una distribuzione CloudFront Web Amazon utilizzando il tuo nome di dominio. Se il controllo è scaduto, prova ad aggiornarlo.

Risorse aggiuntive

Guida per CloudFront sviluppatori Amazon

Colonne del report

- Stato
- ID distribuzione
- Nome di dominio della distribuzione
- Nome di dominio alternativo
- Motivo

CloudFront Ottimizzazione della distribuzione dei contenuti

Descrizione

Verifica i casi in cui il trasferimento di dati dai bucket Amazon Simple Storage Service (Amazon S3) potrebbe essere accelerato utilizzando CloudFront Amazon, AWS il servizio globale di distribuzione di contenuti.

Quando configuri la distribuzione dei contenuti, le richieste relative CloudFront ai contenuti vengono automaticamente indirizzate alla edge location più vicina in cui i contenuti vengono memorizzati nella cache. Questo routing consente di distribuire contenuti agli utenti con le migliori prestazioni possibili. Un rapporto elevato di dati trasferiti in uscita rispetto ai dati archiviati nel bucket indica che potresti trarre vantaggio dall'utilizzo di Amazon CloudFront per fornire i dati.

ID di controllo

`796d6f3D83`

Criteri di avviso

- Giallo: la quantità di dati trasferiti fuori dal bucket agli utenti dalle richieste GET nei 30 giorni precedenti il controllo è almeno 25 volte superiore alla quantità media di dati memorizzati nel bucket.
- Rosso: la quantità di dati trasferiti dal bucket agli utenti dalle richieste GET nei 30 giorni precedenti il controllo è almeno di 10 TB e 25 volte superiore alla quantità media di dati memorizzati nel bucket.

Operazione consigliata

Prendi in considerazione l'utilizzo CloudFront per prestazioni migliori. Vedi i dettagli CloudFront del prodotto Amazon.

Se i dati trasferiti sono pari o superiori a 10 TB al mese, consulta la pagina CloudFront dei prezzi di Amazon per scoprire i possibili risparmi sui costi.

Risorse aggiuntive

- Guida per CloudFront sviluppatori Amazon
- Caso di studio di AWS : PBS

Colonne del report

- Stato
- Regione
- Bucket Name (Nome bucket)
- Archiviazione S3 (GB)
- Trasferimento dati in uscita (GB)
- Rapporto tra trasferimento e archiviazione

CloudFront Inoltro delle intestazioni e rapporto di accesso alla cache

Descrizione

Controlla le intestazioni delle richieste HTTP CloudFront attualmente ricevute dal client e che le inoltra al server di origine.

Alcune intestazioni, come date o user-agent, riducono in modo significativo il rapporto di accessi alla cache (la percentuale di richieste che vengono servite da una CloudFront cache edge). Ciò aumenta il carico sull'origine e riduce le prestazioni, poiché è CloudFront necessario inoltrare più richieste all'origine.

ID di controllo

`N415c450f2`

Criteri di avviso

Giallo: una o più intestazioni di richiesta che vengono CloudFront inoltrate all'origine potrebbero ridurre in modo significativo il rapporto di accesso alla cache.

Operazione consigliata

Valuta se le intestazioni di richiesta forniscono vantaggi sufficienti per giustificare l'effetto negativo sul tasso di occorrenze della cache. Se la tua origine restituisce lo stesso oggetto indipendentemente dal valore di una determinata intestazione, ti consigliamo di non configurare l'inoltro dell'intestazione CloudFront all'origine. Per ulteriori informazioni, consulta Configurazione per memorizzare nella cache gli oggetti in base CloudFront alle intestazioni delle richieste.

Risorse aggiuntive

- Aumento della percentuale di richieste servite dalle CloudFront cache Edge
- CloudFront Rapporti statistici sulla cache
- Intestazioni e CloudFront comportamento delle richieste HTTP

Colonne del report

- ID distribuzione
- Nome di dominio della distribuzione
- Modello di percorso di comportamento della cache
- Headers

Istanze Amazon EC2 con utilizzo elevato

Descrizione

Controlla le istanze Amazon Elastic Compute Cloud (Amazon EC2) in esecuzione in qualsiasi momento durante gli ultimi 14 giorni. Un avviso viene inviato se l'utilizzo giornaliero della CPU è superiore al 90% in quattro o più giorni.

L'elevato utilizzo costante può indicare prestazioni ottimizzate e costanti. Tuttavia, può anche indicare che un'applicazione non dispone di risorse sufficienti. Per ottenere i dati di utilizzo giornaliero della CPU, scarica il report per questo controllo.

ID di controllo

`ZRxQlPsb6c`

Criteri di avviso

Giallo: un'istanza ha registrato un utilizzo medio giornaliero della CPU superiore al 90% in almeno 4 dei 14 giorni precedenti.

Operazione consigliata

Valuta la possibilità di aggiungere altre istanze. Per informazioni sul ridimensionamento del numero di istanze in base alla domanda, consulta la pagina Cos'è Auto Scaling?

Risorse aggiuntive

- Monitoraggio di Amazon EC2
- Metadati dell'istanza e dati utente
- Guida per CloudWatch l'utente di Amazon
- Guida per l'utente di Dimensionamento automatico Amazon EC2

Colonne del report

- Regione/AZ
- ID istanza
- Tipo di istanza
- Nome dell'istanza
- Utilizzo medio della CPU per 14 giorni
- Numero di giorni con utilizzo della CPU superiore al 90%

Sicurezza

Per la categoria di sicurezza, puoi utilizzare i seguenti controlli.

> **Note**
>
> Se hai abilitato Security Hub per il tuo Account AWS, puoi visualizzare i risultati nella Trusted Advisor console. Per informazioni, consulta Visualizzazione controlli AWS Security Hub in AWS Trusted Advisor.
> Puoi visualizzare tutti i controlli dello standard di sicurezza AWS Foundational Security Best Practices ad eccezione dei controlli che hanno la categoria: Recover > Resilience. Per un elenco dei controlli supportati, consulta Controlli AWS Foundational Security Best Practices nella Guida per l'utente di AWS Security Hub .

Controlla i nomi

- Periodo di conservazione di Amazon CloudWatch Log Group

- Fine del supporto per le istanze Amazon EC2 con Microsoft SQL Server
- Fine del supporto per le istanze Amazon EC2 con Microsoft Windows Server
- Fine del supporto standard per le istanze Amazon EC2 con Ubuntu LTS
- I client Amazon EFS non utilizzano data-in-transit la crittografia
- Snapshot pubblici Amazon EBS
- La crittografia dello storage Amazon RDS Aurora è disattivata
- È richiesto l'aggiornamento di una versione secondaria del motore Amazon RDS
- Snapshot pubblici di Amazon RDS
- Rischio accesso gruppo di sicurezza Amazon RDS
- La crittografia dello storage Amazon RDS è disattivata
- Record CNAME di Amazon Route 53 non corrispondenti che puntano direttamente ai bucket S3
- Set di registri delle risorse MX di Amazon Route 53 e Framework della Policy del mittente
- Autorizzazioni Bucket Amazon S3
- Registri di accesso Amazon S3Server abilitati
- Connessioni peering VPC di Amazon con risoluzione DNS disabilitata
- AWS Backup Vault senza policy basate sulle risorse per impedire l'eliminazione dei punti di ripristino
- AWS CloudTrail Registrazione
- AWS Lambda Funzioni che utilizzano runtime obsoleti
- AWS Well-Architected Problemi ad alto rischio di per la sicurezza
- CloudFrontCertificati SSL personalizzati nell'IAM Certificate Store
- CloudFront Certificato SSL sul server di origine
- Sicurezza del Listener ELB
- Gruppi di sicurezza ELB
- Exposed Access Keys
- Rotazione delle chiavi di accesso IAM
- Policy delle Password IAM
- MFA su Account Root
- Gruppi di sicurezza — Porte specifiche senza restrizioni

- Gruppi di sicurezza — Accesso illimitato

Periodo di conservazione di Amazon CloudWatch Log Group

Descrizione

Verifica se il periodo di conservazione dei gruppi di CloudWatch log di Amazon è impostato su 365 giorni o su un altro numero specificato.

Per impostazione predefinita, i log vengono conservati a tempo indeterminato e non scadono mai. Tuttavia, per ogni gruppo di log puoi modificare la policy di conservazione in modo da conformarla per un periodo specifico alle normative di settore o ai requisiti legali.

Puoi specificare il tempo minimo di conservazione e i nomi dei gruppi di log utilizzando LogGroupi parametri Names and MinRetentionTime nelle tue AWS Config regole.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz186`

Origine

`AWS Config Managed Rule: cw-loggroup-retention-period-check`

Criteri di avviso

Giallo: il periodo di conservazione di un gruppo di CloudWatch log Amazon è inferiore al numero minimo di giorni desiderato.

Operazione consigliata

Configura un periodo di conservazione di oltre 365 giorni per i dati di log archiviati in Amazon CloudWatch Logs per soddisfare i requisiti di conformità.

Per ulteriori informazioni, consulta Change log data retention in CloudWatch Logs.

Risorse aggiuntive

Alterazione della conservazione dei log CloudWatch

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Fine del supporto per le istanze Amazon EC2 con Microsoft SQL Server

Descrizione

Verifica le versioni di SQL Server per le istanze Amazon Elastic Compute Cloud (Amazon EC2) in esecuzione nelle ultime 24 ore. Questo controllo ti avvisa se le versioni sono vicine o hanno raggiunto la fine del supporto. Ogni versione di SQL Server offre 10 anni di supporto, inclusi 5 anni di supporto mainstream e 5 anni di supporto esteso. Dopo la fine del supporto, la versione di SQL Server non riceverà aggiornamenti di sicurezza regolari. L'esecuzione di applicazioni con versioni di SQL Server non supportate può comportare rischi per la sicurezza o la conformità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Qsdfp3A4L3`

Criteri di avviso

- Rosso: un'istanza EC2 ha una versione di SQL Server che ha raggiunto la fine del supporto.

- Giallo: un'istanza EC2 ha una versione di SQL Server che raggiungerà la fine del supporto in 12 mesi.

Operazione consigliata

Per modernizzare i carichi di lavoro di SQL Server, valuta la possibilità di rifattorizzare i database nativi di Cloud AWS come Amazon Aurora. Per ulteriori informazioni, consulta Modernizza i carichi di lavoro Windows con. AWS

Per passare a un database completamente gestito, valuta la possibilità di ridefinire la piattaforma su Amazon Relational Database Service (Amazon RDS). Per ulteriori informazioni, consulta Utilizzo di Amazon RDS per SQL Server.

Per aggiornare il tuo SQL Server su Amazon EC2, valuta la possibilità di utilizzare il runbook di automazione per semplificare l'aggiornamento. Per ulteriori informazioni, consulta la documentazione relativa ad AWS Systems Manager.

Se non riesci ad aggiornare il tuo SQL Server su Amazon EC2, valuta il programma EMP (End-of-Sport Migration Program) per Windows Server. Per ulteriori informazioni, consulta il sito Web di EMP.

Risorse aggiuntive

- Preparati alla fine del supporto per SQL Server con AWS
- Microsoft SQL Server in AWS

Colonne del report

- Stato
- Regione
- ID istanza
- Versione SQL Server:
- Cicli di supporto
- Fine del supporto
- Ora ultimo aggiornamento

Fine del supporto per le istanze Amazon EC2 con Microsoft Windows Server

Descrizione

Questo controllo ti avvisa se le versioni sono vicine o hanno raggiunto la fine del supporto. Ogni versione di Windows Server offre 10 anni di supporto. Ciò include 5 anni di supporto mainstream e 5 anni di supporto esteso. Dopo la fine del supporto, la versione di Windows Server non riceverà più i normali aggiornamenti di sicurezza. Se esegui applicazioni con versioni di Windows Server non supportate, la sicurezza o la conformità di tali applicazioni è a rischio.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Qsdfp3A4L4`

Criteri di avviso

- Rosso: un'istanza EC2 dispone di una versione di Windows Server che ha raggiunto la fine del supporto (Windows Server 2003, 2003 R2, 2008 e 2008 R2).
- Giallo: un'istanza EC2 dispone di una versione di Windows Server che raggiungerà la fine del supporto in meno di 18 mesi (Windows Server 2012 e 2012 R2).

Operazione consigliata

Per modernizzare i carichi di lavoro di Windows Server, prendi in considerazione le varie opzioni disponibili in Modernize Windows Workloads with. AWS

Per aggiornare i carichi di lavoro di Windows Server in modo da poterli eseguire su versioni più recenti di Windows Server, puoi utilizzare un runbook di automazione. Per ulteriori informazioni, consulta la documentazione di AWS Systems Manager.

Segui la procedura riportata di seguito:

- Aggiorna la versione di Windows Server

- Arresto difficile e avvio al momento dell'aggiornamento
- Se usi EC2Config, esegui la migrazione a EC2Launch

Colonne del report

- Stato
- Regione
- ID istanza
- Versione di Windows Server
- Cicli di supporto
- Fine del supporto
- Ora ultimo aggiornamento

Fine del supporto standard per le istanze Amazon EC2 con Ubuntu LTS

Descrizione

Questo controllo ti avvisa se le versioni sono prossime o hanno raggiunto la fine del supporto standard. È importante agire, migrando alla versione successiva di LTS o effettuando l'aggiornamento a Ubuntu Pro. Dopo la fine del supporto, le tue macchine LTS 18.04 non riceveranno alcun aggiornamento di sicurezza. Con un abbonamento a Ubuntu Pro, la tua distribuzione di Ubuntu 18.04 LTS può ricevere Expanded Security Maintenance (ESM) fino al 2028. Le vulnerabilità di sicurezza che rimangono prive di patch aprono i sistemi agli hacker e al potenziale di una grave violazione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch15`

Criteri di avviso

Rosso: un'istanza Amazon EC2 ha una versione di Ubuntu che ha raggiunto la fine del supporto standard (Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS e 18.04.6 LTS).

Giallo: un'istanza Amazon EC2 ha una versione di Ubuntu che raggiungerà la fine del supporto standard in meno di 6 mesi (Ubuntu 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS e 20.04.6 LTS).

Verde: tutte le istanze Amazon EC2 sono conformi.

Operazione consigliata

Per aggiornare le istanze LTS di Ubuntu 18.04 a una versione LTS supportata, segui i passaggi indicati in questo articolo. Per aggiornare le istanze di Ubuntu 18.04 LTS a Ubuntu Pro, visita la AWS License Manager console e segui i passaggi indicati nella guida per l'utente.AWS License Manager Puoi anche fare riferimento al blog di Ubuntu che mostra una demo dettagliata sull'aggiornamento delle istanze di Ubuntu a Ubuntu Pro.

Risorse aggiuntive

Per informazioni sui prezzi, contatta. AWS Support

Colonne del report

- Stato
- Regione
- Versione Ubuntu Lts
- Data prevista di fine del supporto
- ID istanza
- Cicli di supporto
- Ora ultimo aggiornamento

I client Amazon EFS non utilizzano data-in-transit la crittografia

Descrizione

Verifica se il file system Amazon EFS è montato utilizzando data-in-transit la crittografia. AWS consiglia ai clienti di utilizzare data-in-transit la crittografia per tutti i flussi di dati per proteggere i

dati dall'esposizione accidentale o dall'accesso non autorizzato. Amazon EFS consiglia ai client di utilizzare l'impostazione di montaggio '-o tls' utilizzando l'helper di montaggio Amazon EFS per crittografare i dati in transito utilizzando TLS v1.2.

ID di controllo

`c1dfpnchv1`

Criteri di avviso

Giallo: uno o più client NFS per il tuo file system Amazon EFS non utilizzano le impostazioni di montaggio consigliate che forniscono la data-in-transit crittografia.

Verde: tutti i client NFS per il tuo file system Amazon EFS utilizzano le impostazioni di montaggio consigliate che forniscono la data-in-transit crittografia.

Operazione consigliata

Per sfruttare la funzionalità di data-in-transit crittografia su Amazon EFS, ti consigliamo di rimontare il file system utilizzando l'helper di montaggio di Amazon EFS e le impostazioni di montaggio consigliate.

> **Note**
>
> Alcune distribuzioni di Linux non includono una versione di stunnel che supporta le funzionalità TLS per impostazione predefinita. Se utilizzi una distribuzione Linux non supportata (vedi le distribuzioni supportate qui), ti consigliamo di aggiornarla prima di rimontarla con l'impostazione di montaggio consigliata.

Risorse aggiuntive

- Crittografia dei dati in transito

Colonne del report

- Stato
- Regione
- ID dei file system EFS
- AZ con connessioni non crittografate
- Ora ultimo aggiornamento

Snapshot pubblici Amazon EBS

Descrizione

Verifica le impostazioni di autorizzazione per gli snapshot del volume Amazon Elastic Block Store (Amazon EBS) e ti avvisa se alcune istantanee sono accessibili pubblicamente.

Quando rendi pubblica un'istantanea, consenti a tutti Account AWS e agli utenti l'accesso a tutti i dati in essa contenuti. Per condividere un'istantanea solo con utenti o account specifici, contrassegna l'istantanea come privata. Quindi, specifica l'utente o gli account con cui desideri condividere i dati dell'istantanea. Tieni presente che se hai abilitato Block Public Access in modalità «blocca tutte le condivisioni», le tue istantanee pubbliche non sono accessibili pubblicamente e non compaiono nei risultati di questo controllo.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate.

ID di controllo

`ePs02jT06w`

Criteri di avviso

Rosso: l'istantanea del volume EBS è accessibile al pubblico.

Operazione consigliata

A meno che tu non sia sicuro di voler condividere tutti i dati dell'istantanea con tutti gli utenti, modifica Account AWS le autorizzazioni: contrassegna l'istantanea come privata, quindi specifica gli account a cui desideri concedere le autorizzazioni. Per ulteriori informazioni, consulta Condivisione di uno snapshot Amazon EBS. Usa Block Public Access for EBS Snapshots per controllare le impostazioni che consentono l'accesso pubblico ai tuoi dati. Questo controllo non può essere escluso dalla visualizzazione nella Trusted Advisor console.

Per modificare direttamente le autorizzazioni per le istantanee, utilizza un runbook nella console. AWS Systems Manager Per ulteriori informazioni, consulta `AWSSupport-ModifyEBSSnapshotPermission`.

Risorse aggiuntive

Snapshot Amazon EBS

Colonne del report

- Stato
- Regione
- ID volume
- ID snapshot
- Descrizione

La crittografia dello storage Amazon RDS Aurora è disattivata

Descrizione

Amazon RDS supporta la crittografia a riposo per tutti i motori di database utilizzando le chiavi da te gestite. AWS Key Management Service Su un'istanza DB attiva con crittografia Amazon RDS, i dati archiviati a riposo nello storage sono crittografati, in modo simile ai backup automatici, alle repliche di lettura e alle istantanee.

Se la crittografia non è attivata durante la creazione di un cluster Aurora DB, è necessario ripristinare un'istantanea decrittografata in un cluster DB crittografato.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.

Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt005`

Criteri di avviso

Rosso: per le risorse Amazon RDS Aurora non è abilitata la crittografia.

Operazione consigliata

Attiva la crittografia dei dati inattivi per il tuo cluster DB.

Risorse aggiuntive

È possibile attivare la crittografia durante la creazione di un'istanza DB o utilizzare una soluzione alternativa per attivare la crittografia su un'istanza DB attiva. Non è possibile modificare un cluster DB decrittografato in un cluster DB crittografato. Tuttavia, è possibile ripristinare un'istantanea decrittografata in un cluster DB crittografato. Quando si esegue il ripristino da un'istantanea decrittografata, è necessario specificare una chiave. AWS KMS

Per ulteriori informazioni, consulta Crittografia delle risorse Amazon Aurora.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

È richiesto l'aggiornamento di una versione secondaria del motore Amazon RDS

Descrizione

Le risorse del tuo database non eseguono l'ultima versione secondaria del motore DB. L'ultima versione secondaria contiene le ultime correzioni di sicurezza e altri miglioramenti.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt003`

Criteri di avviso

Rosso: le risorse Amazon RDS non eseguono l'ultima versione secondaria del motore DB.

Operazione consigliata

Esegui l'upgrade alla versione più recente del motore.

Risorse aggiuntive

Ti consigliamo di mantenere il tuo database con la versione minore più recente del motore DB poiché questa versione include le ultime correzioni di sicurezza e funzionalità. Gli aggiornamenti delle versioni secondarie del motore DB contengono solo le modifiche retrocompatibili con le versioni secondarie precedenti della stessa versione principale del motore DB.

Per ulteriori informazioni, consulta Aggiornamento di una versione del motore delle istanze DB.

Colonne del report

- Stato

- Regione
- Risorsa
- Nome del motore
- Versione del motore attuale
- Valore consigliato
- Ora ultimo aggiornamento

Snapshot pubblici di Amazon RDS

Descrizione

Controlla le impostazioni di autorizzazione per gli snapshot DB Amazon Relational Database Service (Amazon RDS) e avvisa se eventuali snapshot sono contrassegnati come pubblici.

Quando si rende pubblica un'istantanea, si concede a tutti Account AWS e agli utenti l'accesso a tutti i dati dell'istantanea. Se desideri condividere uno snapshot solo con utenti o account specifici, contrassegna lo snapshot come privato. Specifica quindi l'utente o gli account con cui desideri condividere i dati dello snapshot.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate.

ID di controllo

`rSs93HQwa1`

Criteri di avviso

Rosso: lo snapshot Amazon RDS è contrassegnato come pubblico.

Operazione consigliata

A meno che tu non sia sicuro di voler condividere tutti i dati dell'istantanea con tutti gli utenti, modifica Account AWS le autorizzazioni: contrassegna l'istantanea come privata, quindi specifica gli account a cui desideri concedere le autorizzazioni. Per ulteriori informazioni, consulta

Condivisione di uno snapshot DB o DB cluster. Questo controllo non può essere escluso dalla visualizzazione nella console. Trusted Advisor

Per modificare direttamente le autorizzazioni per le istantanee, è possibile utilizzare un runbook nella console. AWS Systems Manager Per ulteriori informazioni, consulta `AWSSupport-ModifyRDSSnapshotPermission`.

Risorse aggiuntive

Backup e ripristino di istanze DB di Amazon RDS

Colonne del report

- Stato
- Regione
- Istanza DB o ID cluster
- ID snapshot

Rischio accesso gruppo di sicurezza Amazon RDS

Descrizione

Controlla le configurazioni dei gruppi di sicurezza per Amazon Relational Database Service (Amazon RDS) e avverte quando una regola del gruppo di sicurezza concede un accesso troppo permissivo al tuo database. La configurazione consigliata per una regola di gruppo di sicurezza consiste nel consentire l'accesso solo da specifici gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) o da un indirizzo IP specifico.

ID di controllo

`nNauJisYIT`

Criteri di avviso

- Giallo: una regola del gruppo di sicurezza DB fa riferimento a un gruppo di sicurezza Amazon EC2 che concede l'accesso globale a una di queste porte: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Giallo: una regola del gruppo di sicurezza DB concede l'accesso a più di un singolo indirizzo IP (il suffisso della regola CIDR non è /0 o /32).
- Rosso: una regola del gruppo di sicurezza DB concede l'accesso globale (il suffisso della regola CIDR è /0).

Operazione consigliata

Rivedi le regole del gruppo di sicurezza e limita l'accesso agli indirizzi IP o agli intervalli IP autorizzati. Per modificare un gruppo di sicurezza, usa l'API AuthorizeDB Ingress o SecurityGroup il. AWS Management Console Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza database.

Risorse aggiuntive

- Gruppi di sicurezza Amazon RDS
- Classless Inter-Domain Routing
- Elenco dei numeri di porta TCP e UDP

Colonne del report

- Stato
- Regione
- Nome del gruppo di sicurezza RDS
- Regola in ingresso
- Motivo

La crittografia dello storage Amazon RDS è disattivata

Descrizione

Amazon RDS supporta la crittografia a riposo per tutti i motori di database utilizzando le chiavi da te gestite. AWS Key Management Service Su un'istanza DB attiva con crittografia Amazon RDS, i dati archiviati a riposo nello storage sono crittografati, in modo simile ai backup automatici, alle repliche di lettura e alle istantanee.

Se la crittografia non è attivata durante la creazione di un'istanza DB, è necessario ripristinare una copia crittografata dello snapshot decrittografato prima di attivare la crittografia.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt006`

Criteri di avviso

Rosso: per le risorse Amazon RDS non è abilitata la crittografia.

Operazione consigliata

Attiva la crittografia dei dati inattivi per la tua istanza DB.

Risorse aggiuntive

È possibile crittografare un'istanza DB solo quando si crea l'istanza DB. Per crittografare un'istanza DB attiva esistente:

Crea una copia crittografata dell'istanza DB originale

1. Creare una snapshot di un'istanza database.
2. Crea una copia crittografata dell'istantanea creata nel passaggio 1.
3. Ripristina un'istanza DB dallo snapshot crittografato.

Per ulteriori informazioni, consulta le seguenti risorse:

- Crittografia delle risorse Amazon RDS
- Copia di uno snapshot DB

Colonne del report

- Stato
- Regione

- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Record CNAME di Amazon Route 53 non corrispondenti che puntano direttamente ai bucket S3

Descrizione

Controlla le zone ospitate di Amazon Route 53 con record CNAME che puntano direttamente ai nomi host dei bucket Amazon S3 e avvisa se il CNAME non corrisponde al nome del bucket S3.

ID di controllo

`c1ng44jvbm`

Criteri di avviso

Rosso: Amazon Route 53 Hosted Zone contiene record CNAME che indicano nomi host dei bucket S3 non corrispondenti.

Verde: nessun record CNAME non corrispondente trovato nella tua Amazon Route 53 Hosted Zone.

Operazione consigliata

Quando indirizzi i record CNAME ai nomi host dei bucket S3, devi assicurarti che esista un bucket corrispondente per ogni record CNAME o alias che configuri. In questo modo, eviti il rischio che i tuoi record CNAME vengano falsificati. Inoltre, impedisci a qualsiasi AWS utente non autorizzato di ospitare contenuti web difettosi o dannosi con il tuo dominio.

Per evitare di indirizzare i record CNAME direttamente ai nomi host dei bucket S3, prendi in considerazione l'utilizzo di Origin Access Control (OAC) per accedere alle tue risorse web del bucket S3 tramite Amazon. CloudFront

Per ulteriori informazioni sull'associazione di CNAME a un nome host del bucket Amazon S3, consulta Personalizzazione degli URL di Amazon S3 con i record CNAME.

Risorse aggiuntive

- Come associare un nome host a un bucket Amazon S3
- Limitazione dell'accesso a un'origine Amazon S3 con CloudFront

Colonne del report

- Stato
- ID della zona ospitata
- ARN della zona ospitata
- Record CNAME corrispondenti
- Record CNAME non corrispondenti
- Ora ultimo aggiornamento

Set di registri delle risorse MX di Amazon Route 53 e Framework della Policy del mittente

Descrizione

Per ogni set di registri delle risorse MX, verifica che il set di registri delle risorse TXT o SPF contenga un record SPF valido. Il registro deve iniziare con "`v=spf1`". Il registro SPF specifica i server autorizzati a inviare messaggi di posta elettronica per il dominio, che consente di rilevare e interrompere lo spoofing degli indirizzi di posta elettronica e di ridurre lo spam. Route 53 consiglia di utilizzare un record TXT anziché un record SPF. Trusted Advisor riporta questo controllo in verde purché ogni set di record di risorse MX abbia almeno un record SPF o TXT.

ID di controllo

`c9D319e7sG`

Criteri di avviso

Giallo: un set di record delle risorse MX non dispone di un record delle risorse TXT o SPF contenente un valore SPF valido.

Operazione consigliata

Per ogni set di registri delle risorse MX, creane uno TXT contenente un valore SPF valido. Per ulteriori informazioni, consulta Sender Policy Framework: sintassi record SPF e Creazione di set di record delle risorse utilizzando la console Amazon Route 53.

Risorse aggiuntive

- Sender Policy Framework
- Registro MX

Colonne del report

- Nome della zona ospitata
- ID della zona ospitata
- Nome del set di registri delle risorse
- Stato

Autorizzazioni Bucket Amazon S3

Descrizione

Controlla i bucket in Amazon Simple Storage Service (Amazon S3) che dispongono di autorizzazioni di accesso aperto o che consentono l'accesso a qualsiasi utente autenticato. AWS

Questo controllo esamina le autorizzazioni del bucket esplicite nonché le policy bucket che potrebbero sovrascrivere tali autorizzazioni. È sconsigliato concedere autorizzazioni di accesso alla lista a tutti gli utenti di un bucket Amazon S3. Queste autorizzazioni possono portare a utenti non intenzionali che elencano oggetti nel bucket ad alta frequenza, il che può comportare costi superiori a quelli previsti. Le autorizzazioni che concedono il caricamento ed eliminano l'accesso a chiunque possono causare vulnerabilità di sicurezza nel tuo bucket.

ID di controllo

`Pfx0RwqBli`

Criteri di avviso

- Giallo: l'ACL del bucket consente l'accesso all'elenco a Everyone (Chiunque) oppure a Any Authenticated AWS User (Qualsiasi utente autenticato).
- Giallo: una policy del bucket consente qualsiasi tipo di accesso aperto.
- Giallo: la policy del bucket contiene dichiarazioni che concedono l'accesso pubblico. L'impostazione Block public and cross-account access to buckets that have public policies (Blocca accesso pubblico e multi-account a bucket che dispongono di policy pubbliche) è attivata e limita l'accesso solo agli utenti autorizzati di tale account fino alla rimozione delle dichiarazioni pubbliche.
- Giallo: Trusted Advisor non dispone dell'autorizzazione per verificare la politica o la politica non può essere valutata per altri motivi.
- Rosso: l'ACL del bucket consente l'accesso per il caricamento e l'eliminazione per Tutti o Qualsiasi utente AWS autenticato.

Operazione consigliata

Se un bucket consente l'accesso aperto, determina se è veramente necessario. In caso contrario, aggiorna le autorizzazioni del bucket per limitare l'accesso al proprietario o a utenti specifici. Utilizza l'impostazione per bloccare l'accesso pubblico di Amazon S3 per controllare le impostazioni che consentono l'accesso pubblico ai tuoi dati. Consulta Impostazione delle autorizzazioni di accesso al bucket e agli oggetti.

Risorse aggiuntive

Gestione delle autorizzazioni di accesso alle risorse di Amazon S3

Colonne del report

- Stato
- Nome della regione
- Parametri dell'API della regione
- Bucket Name (Nome bucket)
- ACL consente la creazione di elenchi
- ACL consente il caricamento e l'eliminazione
- Accesso consentito dalla policy

Registri di accesso Amazon S3Server abilitati

Descrizione

Verifica la configurazione di registrazione dei bucket di Amazon Simple Storage Service.

Quando la registrazione degli accessi al server è abilitata, i registri di accesso dettagliati vengono recapitati ogni ora a un bucket scelto dall'utente. Un registro dei log di accesso contiene dettagli su ogni richiesta, ad esempio il tipo di richiesta, le risorse specificate nella richiesta e l'ora e la data di elaborazione della richiesta. Per impostazione predefinita, la registrazione dei bucket non è abilitata. È consigliabile abilitare la registrazione se si desidera eseguire controlli di sicurezza od ottenere ulteriori informazioni sugli utenti e sui modelli di utilizzo.

Quando la registrazione è inizialmente abilitata, la configurazione viene convalidata automaticamente. Tuttavia, le modifiche future possono causare errori di registrazione. Questo controllo esamina le autorizzazioni esplicite dei bucket Amazon S3. È consigliabile utilizzare le policy dei bucket per controllare le autorizzazioni dei bucket, tuttavia è possibile utilizzare anche gli ACL.

ID di controllo

`c1fd6b96l4`

Criteri di avviso

- Giallo: il bucket non ha la registrazione degli accessi al server abilitata.
- Giallo: le autorizzazioni del bucket di destinazione non includono l'account root, quindi Trusted Advisor non può controllarlo.
- Rosso: il bucket di destinazione non esiste.
- Rosso: il bucket di destinazione e di origine hanno proprietari diversi.
- Rosso: il deliverer del log non dispone dei permessi di scrittura per il bucket di destinazione.
- Verde: Bucket ha la registrazione degli accessi al server abilitata, la destinazione esiste ed esistono le autorizzazioni per scrivere sulla destinazione

Operazione consigliata

Abilita la registrazione per la maggior parte dei bucket. Consulta Abilitazione della registrazione tramite la console e Abilitazione della registrazione a livello di programmazione.

Se le autorizzazioni del bucket di destinazione non includono l'account root e desideri che Trusted Advisor verifichi lo stato della registrazione, aggiungi l'account root come beneficiario. Consulta Modifica delle autorizzazioni del bucket.

Se il bucket di destinazione non esiste, seleziona un bucket esistente come destinazione o creane uno nuovo e selezionalo. Consulta Gestione della registrazione del bucket.

Se la destinazione e l'origine hanno proprietari diversi, modifica il bucket di destinazione con uno che abbia lo stesso proprietario del bucket di origine. Consulta Gestione della registrazione del bucket.

Se il log deliverer non dispone delle autorizzazioni di scrittura per la destinazione (Write not enabled), concedi le autorizzazioni di Upload/Delete al gruppo Log Delivery. Si consiglia di utilizzare le policy dei bucket sugli ACL. Vedi Modifica delle autorizzazioni dei bucket e delle autorizzazioni per la consegna dei log.

Risorse aggiuntive

Lavorare con i bucket

Server access logging (Registrazione degli accessi al server)

Formato del registro di accesso al server

Eliminazione dei file di registro

Colonne del report

- Stato
- Regione
- ARN risorsa
- Bucket Name (Nome bucket)
- Nome destinazione
- Destinazione esistente
- Stesso proprietario
- Scrittura abilitata
- Motivo
- Ora ultimo aggiornamento

Connessioni peering VPC di Amazon con risoluzione DNS disabilitata

Descrizione

Controlla se per le connessioni peering VPC la risoluzione DNS è attivata sia per i VPC accettanti che per quelli richiedenti.

La risoluzione DNS per una connessione peering VPC consente la risoluzione di nomi host DNS pubblici in indirizzi IPv4 privati quando vengono eseguite query dal tuo VPC. Ciò consente l'uso di nomi DNS per la comunicazione tra risorse su VPC in peering. La risoluzione DNS nelle connessioni peering VPC semplifica lo sviluppo e la gestione delle applicazioni e le rende meno soggette a errori; garantisce, inoltre, che le risorse comunichino sempre in modo privato tramite la connessione peering VPC.

Puoi specificare gli ID VPC utilizzando i parametri VPCIds nelle tue regole. AWS Config

Per ulteriori informazioni, consulta Abilitazione della risoluzione DNS per una connessione peering VPC.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz124`

Origine

`AWS Config Managed Rule: vpc-peering-dns-resolution-check`

Criteri di avviso

Giallo: la risoluzione DNS non è abilitata sia per i VPC accettanti che per quelli richiedenti in una connessione peering VPC.

Operazione consigliata

Attiva la risoluzione DNS per le tue connessioni peering VPC.

Risorse aggiuntive

- Modifica delle opzioni di connessione peering VPC
- Attributi DNS nel VPC

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Backup Vault senza policy basate sulle risorse per impedire l'eliminazione dei punti di ripristino

Descrizione

Verifica se ai AWS Backup vault è associata una politica basata sulle risorse che impedisce l'eliminazione dei punti di ripristino.

La policy basata sulle risorse impedisce l'eliminazione imprevista dei punti di ripristino, per cui è possibile applicare il controllo degli accessi con privilegi minimi sui dati di backup.

Puoi specificare gli AWS Identity and Access Management ARN che non desideri vengano controllati dalla regola nel parametro principale ArnList delle tue regole. AWS Config

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz152`

Origine

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

Criteri di avviso

Giallo: alcuni AWS Backup vault non dispongono di una politica basata sulle risorse per impedire l'eliminazione dei punti di ripristino.

Operazione consigliata

Crea politiche basate sulle risorse per i tuoi AWS Backup vault per prevenire l'eliminazione inaspettata dei punti di ripristino.

La policy deve includere un'istruzione «Deny» con le autorizzazioni backup: DeleteRecovery Point, backup: e backup: UpdateRecoveryPointLifecycle. PutBackupVaultAccessPolicy

Per ulteriori informazioni, consulta Impostazione delle policy di accesso su vault di backup.

Colonne del report

- Stato
- Regione
- Risorsa

- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS CloudTrail Registrazione

Descrizione

Verifica l'utilizzo di. AWS CloudTrail CloudTrail offre una maggiore visibilità sull'attività dell'utente Account AWS registrando le informazioni sulle chiamate AWS API effettuate sull'account. È possibile utilizzare questi registri per determinare, ad esempio, quali azioni ha eseguito un determinato utente durante un periodo di tempo specificato o quali utenti hanno eseguito azioni su una determinata risorsa durante un periodo di tempo specificato.

Poiché CloudTrail invia i file di log a un bucket Amazon Simple Storage Service (Amazon S3) CloudTrail , deve disporre delle autorizzazioni di scrittura per il bucket. Se un trail si applica a tutte le Regioni (impostazione predefinita quando si crea un nuovo trail), esso appare più volte nel report Trusted Advisor .

ID di controllo

`vjafUGJ9H0`

Criteri di avviso

- Giallo: CloudTrail segnala gli errori di consegna dei log per una traccia.
- Rosso: non è stato creato un percorso per una regione o la registrazione è disattivata per un percorso.

Operazione consigliata

Per creare un percorso e avviare la registrazione dalla console, vai alla Console AWS CloudTrail.

Per avviare la registrazione, consulta Interruzione e avvio della registrazione per un percorso.

Se si ricevono errori di consegna del registro, verifica che il bucket esista e che la policy necessaria sia collegata al bucket. Consulta Policy del bucket Amazon S3.

Risorse aggiuntive

- AWS CloudTrail Guida per l'utente
- Regioni supportate

- Servizi supportati

Colonne del report

- Stato
- Regione
- Nome del percorso
- Stato della registrazione
- Bucket Name (Nome bucket)
- Data ultima consegna

AWS Lambda Funzioni che utilizzano runtime obsoleti

Descrizione

Verifica le funzioni Lambda la cui versione $LATEST è configurata per utilizzare un runtime prossimo all'obsolescenza o obsoleto. I runtime obsoleti non sono idonei per gli aggiornamenti di sicurezza o il supporto tecnico

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

Le versioni delle funzioni Lambda pubblicate sono immutabili, il che significa che possono essere richiamate ma non aggiornate. Solo la versione `$LATEST` di una funzione Lambda può essere aggiornata. Per ulteriori informazioni, consulta Versioni delle funzioni Lambda.

ID di controllo

`L4dfs2Q4C5`

Criteri di avviso

- Rosso: la versione $LATEST della funzione è configurata per utilizzare un runtime già obsoleto.
- Giallo: la versione $LATEST della funzione è in esecuzione su un runtime che sarà obsoleto entro 180 giorni.

Operazione consigliata

Se si dispone di funzioni in esecuzione su un runtime che verrà reso obsoleto, devi prepararti per la migrazione a un runtime supportato. Per ulteriori informazioni, consulta Policy di supporto per il runtime.

Ti consigliamo di eliminare le versioni delle funzioni precedenti che non stai più utilizzando.

Risorse aggiuntive

Runtime Lambda

Colonne del report

- Stato
- Regione
- ARN della funzione
- Runtime
- Giorni all'impostazione come obsoleta
- Data di deprecazione
- Media richiami giornalieri
- Ora ultimo aggiornamento

AWS Well-Architected Problemi ad alto rischio di per la sicurezza

Descrizione

Verifica problemi ad alto rischio (HRI) per i carichi di lavoro nel pilastro della sicurezza. Questo controllo è basato sulle revisioni di AWS-Well Architected. I risultati dei controlli dipendono dal completamento della valutazione del carico di lavoro con AWS Well-Architected.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Wxdfp4B1L3`

Criteri di avviso

- Rosso: almeno un problema attivo ad alto rischio è stato identificato nel pilastro di sicurezza di AWS Well-Architected.
- Verde: non sono stati rilevati problemi attivi ad alto rischio nel pilastro di sicurezza di AWS Well-Architected.

Operazione consigliata

AWS Well-Architected ha rilevato problemi ad alto rischio durante la valutazione del carico di lavoro. Questi problemi offrono opportunità per ridurre i rischi e risparmiare denaro. Accedi allo strumento AWS Well-Architected per rivedere le tue risposte e risolvere i problemi attivi.

Colonne del report

- Stato
- Regione
- ARN del carico di lavoro
- Nome del carico di lavoro
- Nome del revisore
- Tipo di carico di lavoro
- Data di inizio del carico di lavoro
- Data dell'ultima modifica del carico di lavoro
- Numero di HRI identificati per Sicurezza
- Numero di HRI risolti per Sicurezza
- Numero di domande per Sicurezza
- Numero totale di domande nel pilastro Sicurezza
- Ora ultimo aggiornamento

CloudFrontCertificati SSL personalizzati nell'IAM Certificate Store

Descrizione

Verifica la presenza di nomi di dominio CloudFront alternativi nei certificati SSL nell'archivio certificati IAM. Questo controllo avvisa l'utente se un certificato è scaduto, scadrà presto, utilizza una crittografia obsoleta o non è configurato correttamente per la distribuzione.

Quando scade un certificato personalizzato per un nome di dominio alternativo, i browser che visualizzano i tuoi CloudFront contenuti potrebbero mostrare un messaggio di avviso sulla sicurezza del tuo sito web. I certificati crittografati utilizzando l'algoritmo di hashing SHA-1 vengono resi obsoleti da browser web come Chrome e Firefox.

Un certificato deve contenere un nome di dominio che corrisponda al nome di dominio di origine o al nome di dominio nell'intestazione host di una richiesta di visualizzatore. Se non corrisponde, CloudFront restituisce all'utente un codice di stato HTTP 502 (gateway non valido). Per ulteriori informazioni, consulta Utilizzo di HTTPS e di nomi di dominio alternativi.

ID di controllo

`N425c450f2`

Criteri di avviso

- Rosso: un certificato SSL personalizzato è scaduto.
- Giallo: un certificato SSL personalizzato scade nei prossimi sette giorni.
- Giallo: un certificato SSL personalizzato è stato crittografato utilizzando l'algoritmo di hashing SHA-1.
- Giallo: uno o più nomi di dominio alternativi che non appaiono anche nel campo Common Name (Nome comune) o Subject Alternative Names (Nomi alternativi oggetto) del certificato SSL personalizzato.

Operazione consigliata

Rinnova un certificato scaduto o che sta per scadere.

Sostituisci un certificato crittografato utilizzando l'algoritmo di hashing SHA-1 con uno crittografato utilizzando l'algoritmo di hashing SHA-256.

Sostituisci il certificato con uno che contiene i valori applicabili nei campi Common Name (Nome comune) o Subject Alternative Domain (Nomi alternativi oggetto).

Risorse aggiuntive

Utilizzo di una connessione HTTPS per accedere agli oggetti

Colonne del report

- Stato
- ID distribuzione
- Nome di dominio della distribuzione
- Nome del certificato
- Motivo

CloudFront Certificato SSL sul server di origine

Descrizione

Controlla il server di origine per i certificati SSL che sono scaduti, stanno per scadere, sono mancanti o che utilizzano una crittografia obsoleta. Se un certificato presenta uno di questi problemi, CloudFront risponde alle richieste relative ai tuoi contenuti con il codice di stato HTTP 502, Bad Gateway.

I certificati crittografati utilizzando l'algoritmo di hashing SHA-1 vengono resi obsoleti da browser web come Chrome e Firefox. A seconda del numero di certificati SSL che hai associato alle tue CloudFront distribuzioni, questo controllo potrebbe aggiungere qualche centesimo al mese alla tua fattura con il tuo provider di web hosting, ad esempio, AWS se utilizzi Amazon EC2 o Elastic Load Balancing come origine per la tua distribuzione. CloudFront Questo controllo non convalida la catena di certificati di origine o le autorità di certificazione. Puoi verificarli nella tua configurazione. CloudFront

ID di controllo

`N430c450f2`

Criteri di avviso

- Rosso: un certificato SSL sull'origine è scaduto o non è disponibile.
- Giallo: un certificato SSL sull'origine scade nei prossimi trenta giorni.
- Giallo: un certificato SSL personalizzato sull'origine è stato crittografato utilizzando l'algoritmo di hashing SHA-1.
- Giallo: non è possibile individuare un certificato SSL sull'origine. La connessione potrebbe non essere riuscita a causa di timeout o altri problemi di connessione HTTPS.

Operazione consigliata

Rinnova il certificato sull'origine se è scaduto o sta per scadere.

Aggiungi un certificato se non ne esiste già uno.

Sostituisci un certificato crittografato utilizzando l'algoritmo di hashing SHA-1 con uno crittografato utilizzando l'algoritmo di hashing SHA-256.

Risorse aggiuntive

Utilizzo di HTTPS e di nomi di dominio alternativi

Colonne del report

- Stato
- ID distribuzione
- Nome di dominio della distribuzione
- Origin
- Motivo

Sicurezza del Listener ELB

Descrizione

Verifica la presenza di sistemi di bilanciamento del carico con listener che non utilizzano le configurazioni di sicurezza consigliate per le comunicazioni crittografate. AWS consiglia di utilizzare un protocollo sicuro (HTTPS o SSL), politiche di up-to-date sicurezza, nonché cifrari e protocolli sicuri.

Quando utilizzi un protocollo sicuro per una connessione front-end (dal client al load balancer), le richieste vengono crittografate tra i client e il load balancer, rendendo il sistema molto più sicuro. Elastic Load Balancing fornisce politiche di sicurezza predefinite con cifrari e protocolli che aderiscono alle migliori pratiche di sicurezza. AWS Le nuove versioni delle policy predefinite vengono rilasciate man mano che sono disponibili nuove configurazioni.

ID di controllo

`a2sEc6ILx`

Criteri di avviso

- Giallo: un load balancer non ha un listener che utilizzi un protocollo sicuro (HTTPS o SSL).

- Giallo: un listener del load balancer utilizza una policy di sicurezza SSL predefinita obsoleta.
- Giallo: un listener del load balancer utilizza crittografia o protocolli sconsigliati.
- Rosso: un listener del load balancer utilizza crittografia o protocolli non sicuri.

Operazione consigliata

Se il traffico verso il load balancer deve essere sicuro, utilizza il protocollo HTTPS o SSL per la connessione front-end.

Aggiorna il load balancer alla versione più recente della policy di sicurezza SSL predefinita.

Utilizza solo crittografie e protocolli consigliati.

Per ulteriori informazioni, consulta Configurazioni del listener per Elastic Load Balancing.

Risorse aggiuntive

- Riferimento rapido sulle configurazioni dei listener
- Aggiornamento della configurazione di negoziazione SSL del load balancer
- Configurazioni della negoziazione SSL per Elastic Load Balancing
- Tabella della policy di sicurezza SSL

Colonne del report

- Stato
- Regione
- Nome del load balancer
- Porta del load balancer
- Motivo

Gruppi di sicurezza ELB

Descrizione

Controlla i load balancer configurati con un gruppo di sicurezza mancante o un gruppo di sicurezza che consente l'accesso alle porte non configurate per il load balancer.

Se un gruppo di sicurezza associato a un load balancer viene eliminato, il load balancer non funzionerà come previsto. Se un gruppo di sicurezza consente l'accesso a porte non configurate per il load balancer, aumenta il rischio di perdita di dati o attacchi dannosi.

ID di controllo

xSqX82fQu

Criteri di avviso

- Giallo: le regole in entrata di un gruppo di sicurezza Amazon VPC associato a un load balancer consentono l'accesso a porte non definite nella configurazione del listener del load balancer.
- Rosso: non esiste un gruppo di sicurezza associato a un load balancer.

Operazione consigliata

Configura le regole del gruppo di sicurezza per limitare l'accesso solo alle porte e ai protocolli definiti nella configurazione del listener del load balancer e il protocollo ICMP per supportare Path MTU Discovery. Consulta Listener per Classic Load Balancer e Gruppi di sicurezza per load balancer in un VPC.

Se un gruppo di sicurezza non è disponibile, applicane uno nuovo al load balancer. Crea regole del gruppo di sicurezza che limitano l'accesso solo alle porte e ai protocolli definiti nella configurazione del listener del load balancer. Consulta Gruppi di sicurezza per load balancer in un VPC.

Risorse aggiuntive

- Guida per l'utente di Elastic Load Balancing
- Configurazione di un Classic Load Balancer

Colonne del report

- Stato
- Regione
- Nome del load balancer
- ID gruppo di sicurezza
- Motivo

Exposed Access Keys

Descrizione

Controlla che i repository del codice più diffusi non contengano chiavi di accesso che sono state esposte al pubblico e che Amazon Elastic Compute Cloud (Amazon EC2) non sia stato utilizzato irregolarmente, generando la compromissione di una chiave di accesso.

Una chiave di accesso è composta da un ID chiave di accesso e la relativa chiave di accesso segreta. Le chiavi di accesso esposte rappresentano un rischio per la sicurezza del tuo account e degli altri utenti. Potrebbero comportare addebiti eccessivi derivanti da attività non autorizzate o abusi e violare l'Accordo con il cliente AWS.

Se la chiave di accesso è esposta, agisci immediatamente per proteggere il tuo account. Per proteggere il tuo account da addebiti eccessivi, limita AWS temporaneamente la tua capacità di creare alcune risorse. AWS Questo non rende sicuro il tuo account. Limita solo parzialmente l'utilizzo non autorizzato che ti potrebbe essere addebitato.

> **Note**
>
> Questo controllo non garantisce l'identificazione di chiavi di accesso esposte o istanze EC2 compromesse. L'utente è in ultima istanza responsabile della sicurezza e della protezione delle proprie chiavi di accesso e AWS risorse.
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno; le richieste di aggiornamento non sono consentite. Al momento, non è possibile escludere le risorse da questo controllo.

Se viene indicata una scadenza per una chiave di accesso, AWS può sospendere l'accesso Account AWS se l'utilizzo non autorizzato non viene interrotto entro tale data. Se ritieni che un avviso sia errato, contatta AWS Support.

Le informazioni visualizzate Trusted Advisor potrebbero non riflettere lo stato più recente del tuo account. Nessuna chiave di accesso esposta viene contrassegnata come risolta fino a quando tutte le chiavi di accesso esposte sull'account non sono state risolte. Questa sincronizzazione dei dati può richiedere fino a una settimana.

ID di controllo

`12Fnkpl8Y5`

Criteri di avviso

- Rosso: potenzialmente compromesso: AWS ha identificato l'ID di una chiave di accesso e la corrispondente chiave di accesso segreta che sono stati esposti su Internet e potrebbero essere stati compromessi (utilizzati).
- Rosso: esposto: AWS ha identificato l'ID di una chiave di accesso e la corrispondente chiave di accesso segreta che sono stati esposti su Internet.

- Rosso: Sospetto: l'uso irregolare di Amazon EC2 indica che una chiave di accesso potrebbe essere stata compromessa, ma non è stata identificata come esposta su Internet.

Operazione consigliata

Elimina la chiave di accesso interessata il prima possibile. Se la chiave è associata a un utente IAM, consulta Gestione delle chiavi di accesso per gli utenti IAM.

Verifica la presenza di un utilizzo non autorizzato sul tuo account. Esegui l'accesso alla AWS Management Console e verifica la presenza di risorse sospette su ogni console di servizio. Presta particolare attenzione all'esecuzione delle istanze Amazon EC2, le richieste di istanze spot, le chiavi di accesso e gli utenti IAM. Puoi anche verificare l'utilizzo complessivo sulla Console di gestione fatturazione e costi.

Risorse aggiuntive

- Migliori pratiche per la gestione delle chiavi di AWS accesso
- AWS Linee guida per il controllo della

Colonne del report

- ID chiave di accesso
- Nome utente (IAM o Root)
- Tipo di frode
- ID del caso
- Ora aggiornamento
- Ubicazione
- Scadenza
- Utilizzo (USD al giorno)

Rotazione delle chiavi di accesso IAM

Descrizione

Controlla le chiavi di accesso IAM attive che non sono state ruotate negli ultimi 90 giorni.

Quando si ruotano regolarmente le chiavi di accesso, si riduce la possibilità che una chiave compromessa possa essere utilizzata a tua insaputa per accedere alle risorse. Ai fini di questo controllo, la data e l'ora dell'ultima rotazione coincidono con quelle della creazione o dell'attivazione più recente della chiave di accesso. Il numero e la data della

chiave di accesso provengono dalle informazioni `access_key_1_last_rotated` e `access_key_2_last_rotated` nel registro delle credenziali IAM più recente.

Poiché la frequenza di rigenerazione di un registro delle credenziali è limitata, l'aggiornamento di questo controllo potrebbe non riflettere le modifiche recenti. Per ulteriori informazioni, consulta Generare registri delle credenziali per il tuo Account AWS.

Per creare e ruotare le chiavi di accesso, un utente deve disporre delle autorizzazioni appropriate. Per ulteriori informazioni, consulta Consentire agli utenti di gestire le proprie password, le chiavi di accesso e le chiavi SSH.

ID di controllo

`DqdJqYeRm5`

Criteri di avviso

- Verde: la chiave di accesso è attiva ed è stata ruotata negli ultimi 90 giorni.
- Giallo: la chiave di accesso è attiva ed è stata ruotata negli ultimi 2 anni, ma più di 90 giorni fa.
- Rosso: la chiave di accesso è attiva ed è stata ruotata negli ultimi 2 anni.

Operazione consigliata

Ruota le chiavi di accesso regolarmente. Consulta Rotazione delle chiavi di accesso e Gestione delle chiavi di accesso per gli utenti IAM.

Risorse aggiuntive

- Best practice di IAM
- Come ruotare le chiavi di accesso per gli utenti IAM

Colonne del report

- Stato
- Utente IAM
- Chiave di accesso
- Ultima chiave ruotata
- Motivo

Policy delle Password IAM

Descrizione

Controlla la policy delle password per l'account e avverte quando una policy di password non è abilitata o se i requisiti relativi al contenuto della password non sono stati abilitati.

I requisiti relativi ai contenuti delle password aumentano la sicurezza complessiva dell'ambiente AWS mediante la creazione forzata di password utente complesse. Quando crei o modifichi una policy sulle password, la modifica viene applicata immediatamente per i nuovi utenti ma non richiede agli utenti esistenti di modificare le password.

ID di controllo

`Yw2K9puPzl`

Criteri di avviso

- Giallo: una policy sulle password è abilitata, ma almeno un requisito relativo al contenuto non è abilitato.
- Rosso: nessuna policy sulle password è abilitata.

Operazione consigliata

Se alcuni requisiti relativi al contenuto non sono abilitati, valuta la possibilità di abilitarli. Se nessuna policy sulle password è abilitata, creane e configurane una. Consulta Impostazione di una policy delle password dell'account per utenti IAM.

Risorse aggiuntive

La gestione delle password

Colonne del report

- Policy sulle password
- Maiuscolo
- Minuscolo
- Numero
- Non alfanumerico

MFA su Account Root

Descrizione

Controlla l'account root e avverte se l'autenticazione a più fattori (MFA) non è abilitata.

Per una maggiore sicurezza, ti consigliamo di proteggere il tuo account utilizzando la MFA, che richiede all'utente di inserire un codice di autenticazione univoco dal proprio hardware o dispositivo virtuale MFA quando interagisce con il sito Web e i siti Web associati. AWS Management Console

ID di controllo

`7DAFEmoDos`

Criteri di avviso

Rosso: l'MFA non è abilitata sull'account root.

Operazione consigliata

Accedi al tuo account root e attiva un dispositivo MFA. Consulta Verifica dello stato MFA e Configurazione di un dispositivo MFA.

Risorse aggiuntive

Utilizzo di dispositivi Multi-Factor Authentication (MFA) con AWS

Gruppi di sicurezza — Porte specifiche senza restrizioni

Descrizione

Controlla i gruppi di protezione per le regole che consentono l'accesso illimitato (0.0.0.0/0) a porte specifiche.

L'accesso illimitato aumenta le opportunità di attività dannose (pirateria informatica, denial-of-service attacchi, perdita di dati). Le porte con più alto rischio sono contrassegnate in rosso e quelle con meno rischio sono contrassegnate in giallo. Le porte contrassegnate in verde sono in genere utilizzate da applicazioni che richiedono un accesso illimitato, ad esempio HTTP e SMTP (Simple Mail Transfer Protocol).

Se i gruppi di sicurezza sono stati configurati intenzionalmente in questo modo, si consiglia di utilizzare misure di protezione aggiuntive per proteggere l'infrastruttura (ad esempio tabelle IP).

> **Note**
>
> Questo controllo valuta solo i gruppi di sicurezza creati e le relative regole in ingresso per gli indirizzi IPv4. I gruppi di sicurezza creati da AWS Directory Service sono contrassegnati in rosso o in giallo, ma non rappresentano un rischio per la sicurezza e possono essere ignorati in modo sicuro o esclusi. Per ulteriori informazioni, consultare la pagina relativa alle domande frequenti su Trusted Advisor.

> **Note**
>
> Questo controllo non include il caso d'uso in cui un elenco di prefissi gestito dal cliente concede l'accesso a 0.0.0.0/0 e viene utilizzato come fonte con un gruppo di sicurezza.

ID di controllo

`HCP4007jGY`

Criteri di avviso

- Verde: l'accesso alle porte 80, 25, 443 o 465 è illimitato.
- Rosso: l'accesso alle porte 20, 21, 1433, 1434, 3306, 3389, 4333, 5432 o 5500 è illimitato.
- Giallo: l'accesso a qualsiasi altra porta è illimitato.

Operazione consigliata

Limita l'accesso solo agli indirizzi IP che lo richiedono. Per limitare l'accesso a un indirizzo IP specifico, imposta il suffisso su /32 (ad esempio 192.0.2.10/32). Assicurati di eliminare le regole eccessivamente permissive dopo aver creato quelle più restrittive.

Risorse aggiuntive

- Gruppi di sicurezza Amazon EC2

  Elenco dei numeri di porta TCP e UDP
- Classless Inter-Domain Routing

Colonne del report

- Stato
- Regione

- Nome del gruppo di sicurezza
- ID gruppo di sicurezza
- Protocollo
- Dalla porta
- Alla porta

Gruppi di sicurezza — Accesso illimitato

Descrizione

Controlla i gruppi di sicurezza per le regole che consentono l'accesso illimitato a una risorsa.

L'accesso senza restrizioni aumenta le opportunità di attività dannose (pirateria informatica, attacchi, perdita di dati). denial-of-service

> **Note**
>
> Questo controllo valuta solo i gruppi di sicurezza creati e le relative regole in ingresso per gli indirizzi IPv4. I gruppi di sicurezza creati da AWS Directory Service sono contrassegnati in rosso o in giallo, ma non rappresentano un rischio per la sicurezza e possono essere ignorati in modo sicuro o esclusi. Per ulteriori informazioni, consultare la pagina relativa alle domande frequenti su Trusted Advisor.

> **Note**
>
> Questo controllo non include il caso d'uso in cui un elenco di prefissi gestito dal cliente concede l'accesso a 0.0.0.0/0 e viene utilizzato come fonte con un gruppo di sicurezza.

ID di controllo

`1iG5NDGVre`

Criteri di avviso

Rosso: una regola del gruppo di sicurezza ha un indirizzo IP di origine con un suffisso /0 per porte diverse da 25, 80 o 443.

Operazione consigliata

Limita l'accesso solo agli indirizzi IP che lo richiedono. Per limitare l'accesso a un indirizzo IP specifico, imposta il suffisso su /32 (ad esempio 192.0.2.10/32). Assicurati di eliminare le regole eccessivamente permissive dopo aver creato quelle più restrittive.

Risorse aggiuntive

- Gruppi di sicurezza Amazon EC2
- Classless Inter-Domain Routing

Colonne del report

- Stato
- Regione
- Nome del gruppo di sicurezza
- ID gruppo di sicurezza
- Protocollo
- Dalla porta
- Alla porta
- Intervallo IP

Tolleranza ai guasti

È possibile utilizzare i seguenti controlli per la categoria di tolleranza ai guasti.

Controlla i nomi

- ALB Multi-AZ
- Backtracking del cluster MySQL di Amazon Aurora non abilitato
- Accessibilità dell'istanza DB Amazon Aurora
- Failover Amazon CloudFront Origin
- Rischio di accesso agli endpoint Amazon Comprehend
- Cluster Amazon DocumentDB Single AZ
- Ripristino Amazon DynamoDB oint-in-time P
- Tabella di Amazon DynamoDB non inclusa nel piano di backup
- Amazon EBS non incluso nel piano AWS Backup

- Snapshot Amazon EBS
- Per il dimensionamento automatico Amazon EC2 non è abilitato il controllo dell'integrità ELB
- Per il gruppo con dimensionamento automatico Amazon EC2 è abilitato il ribilanciamento della capacità
- Il dimensionamento automatico Amazon EC2 non è distribuito in più AZ o non soddisfa il numero minimo di AZ
- Bilanciamento della zona di disponibilità Amazon EC2
- Monitoraggio dettagliato di Amazon EC2 non abilitato
- Driver Amazon ECS AWS Logs in modalità di blocco
- Servizio Amazon ECS con un'unica AZ
- Strategia di collocazione Multi-AZ di Amazon ECS
- Amazon EFS senza ridondanza di destinazione di montaggio
- Amazon EFS non è incluso nel AWS Backup piano
- Cluster Amazon ElastiCache Multi-AZ
- Backup automatico dei cluster Amazon ElastiCache Redis
- Cluster Multi-AZ Amazon MemoryDB
- Broker Amazon MSK che ospitano un numero eccessivo di partizioni
- Domini Amazon OpenSearch Service con meno di tre nodi di dati
- Backup Amazon RDS
- I cluster Amazon RDS DB dispongono di un'istanza DB
- Cluster Amazon RDS DB con tutte le istanze nella stessa zona di disponibilità
- Cluster Amazon RDS DB con tutte le istanze di lettura nella stessa zona di disponibilità
- Monitoraggio avanzato delle istanze DB Amazon RDS non abilitato
- La scalabilità automatica dello storage sulle istanze DB di Amazon RDS è disattivata
- Istanze database Amazon RDS che non utilizzano la distribuzione Multi-AZ
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- Il parametro log_output di Amazon RDS è impostato su tabella
- L'impostazione del parametro innodb_default_row_format di Amazon RDS non è sicura
- Il parametro innodb_flush_log_at_trx_commit di Amazon RDS non è 1
- Il parametro max_user_connections di Amazon RDS è basso

- Amazon RDS Multi-AZ
- Amazon RDS non è previsto AWS Backup
- Le repliche di lettura di Amazon RDS sono aperte in modalità scrivibile
- I backup automatici delle risorse Amazon RDS sono disattivati
- Il parametro sync_binlog di Amazon RDS è disattivato
- Per il cluster DB RDS non è abilitata la replica Multi-AZ
- Istanza di standby RDS Multi-AZ non abilitata
- Amazon RDS ReplicaLag
- Il parametro Amazon RDS synchronous_commit è disattivato
- Snapshot automatiche del cluster di Amazon Redshift
- Amazon Route 53 ha eliminato i Controlli dell'integrità
- Set di registri delle risorse di Failover Amazon Route 53
- Set di registri delle risorse TTL (Time-to-Live) alto di Amazon Route 53
- Deleghe del Server dei nomi Amazon Route 53
- Amazon Route 53 Resolver Ridondanza della zona di disponibilità degli endpoint
- Registrazione di Bucket Amazon S3
- Replica di bucket Amazon S3 non abilitata
- Amazon S3 Bucket Versioning
- I sistemi di bilanciamento del carico (Application, Network e Gateway Load Balancer) non si estendono su più zone di disponibilità
- Dimensionamento automatico degli IP disponibili nelle sottoreti
- Controllo dell'integrità del gruppo Auto Scaling
- Risorse dei gruppi Auto Scaling
- Cluster AWS CloudHSM che eseguono istanze HSM in una singola zona di disponibilità
- AWS Direct Connect Resilienza della posizione
- AWS Lambda funzioni senza una coda di lettere non scritte configurata
- AWS Lambda Sulle destinazioni degli eventi di fallimento
- Funzioni AWS Lambda abilitate per VPC senza ridondanza Multi-AZ
- AWS Resilience Hub Controllo dei componenti dell'applicazione
- AWS Resilience Hub politica violata

- AWS Resilience Hub punteggi di resilienza
- AWS Resilience Hub età di valutazione
- AWS Site-to-Site VPN ha almeno un tunnel in stato DOWN
- AWS Well-ArchitectedProblemi ad alto rischio di per l'affidabilità
- Per Classic Load Balancer non sono state configurate più AZ
- Svuotamento connessione ELB
- Ottimizzazione del load balancer
- Indipendenza dell'AZ disponibilità dal Gateway NAT
- Bilanciamento del carico tra zone di Network Load Balancer
- NLB: risorsa rivolta a Internet in sottorete privata
- NLB Multi-AZ
- Numero di componenti Regioni AWS in un set di repliche di Incident Manager
- Controllo dell'applicazione in una singola AZ
- Interfaccia VPC: interfacce di rete endpoint in più AZ
- Ridondanza del Tunnel VPN
- Ridondanza della zona di disponibilità ActiveMQ
- Ridondanza della zona di disponibilità RabbitMQ

ALB Multi-AZ

Descrizione

Verifica se gli Application Load Balancer sono configurati per utilizzare più di una zona di disponibilità (AZ). Un'AZ è una posizione distinta che è isolata da errori presenti in altre zone. Configura il tuo load balancer in più AZ nella stessa regione per migliorare la disponibilità del carico di lavoro.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch08`

Criteri di avviso

Giallo: ALB si trova in un'unica AZ.

Verde: ALB ha due o più AZ.

Operazione consigliata

Assicurati che il tuo sistema di bilanciamento del carico sia configurato con almeno due zone di disponibilità.

Per ulteriori informazioni, consulta Zone di disponibilità per l'Application Load Balancer.

Risorse aggiuntive

Per ulteriori informazioni, consulta la seguente documentazione :

- Come funziona Elastic Load Balancing
- Regioni, zone di disponibilità e zone locali

Colonne del report

- Stato
- Regione
- Nome ALB
- Regola ALB
- ARN BIANCO
- Numero di AZ
- Ora ultimo aggiornamento

Backtracking del cluster MySQL di Amazon Aurora non abilitato

Descrizione

Controlla se per un cluster MySQL di Amazon Aurora è abilitato il backtracking.

Il backtracking del cluster MySQL di Amazon Aurora è una funzionalità che consente di ripristinare un cluster di database Aurora a un momento precedente nel tempo senza creare un

nuovo cluster. Consente di ripristinare il database a un momento specifico nel tempo entro un determinato periodo di conservazione, senza la necessità di eseguire il ripristino da una snapshot.

È possibile regolare la finestra temporale del backtracking (ore) nel BacktrackWindowInHoursparametro delle regole. AWS Config

Per ulteriori informazioni, consulta la pagina relativa al backtrack di un cluster di database Aurora.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz131`

Origine

`AWS Config Managed Rule: aurora-mysql-backtracking-enabled`

Criteri di avviso

Giallo: il backtracking del cluster MySQL di Amazon Aurora non è abilitato

Operazione consigliata

Attiva il backtracking per il tuo cluster MySQL di Amazon Aurora.

Per ulteriori informazioni, consulta la pagina relativa al backtrack di un cluster di database Aurora.

Risorse aggiuntive

Backtracking di un cluster di database Aurora

Colonne del report

- Stato
- Regione
- Risorsa

- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Accessibilità dell'istanza DB Amazon Aurora

Descrizione

Controlla i casi in cui un cluster Amazon Aurora DB ha istanze sia private che pubbliche.

Se l'istanza database primaria non va a buon fine, una replica viene promossa a istanza primaria. Se la replica è privata, gli utenti che dispongono solo di accesso pubblico non saranno più in grado di connettersi al database dopo il failover. È consigliabile che tutte le istanze DB in un cluster abbiano la stessa accessibilità.

ID di controllo

`xuy7H1avtl`

Criteri di avviso

Giallo: le istanze in un cluster Aurora DB hanno un'accessibilità diversa (un mix di pubblica e privata).

Operazione consigliata

Modifica l'impostazione `Publicly Accessible` delle istanze nel cluster DB in modo che siano tutte pubbliche o private. Per informazioni dettagliate, consulta le istruzioni per le istanze di MySQL su Modifica di un'istanza DB con il motore di database di MySQL.

Risorse aggiuntive

Tolleranza ai guasti di un cluster Aurora DB

Colonne del report

- Stato
- Regione
- Cluster
- Istanze DB pubbliche
- Istanze DB private
- Motivo

Failover Amazon CloudFront Origin

Descrizione

Verifica che un gruppo di origine sia configurato per le distribuzioni che includono due origini in Amazon CloudFront.

Per ulteriori informazioni, consulta Ottimizzazione dell'alta disponibilità con il failover di CloudFront origine.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz112`

Origine

`AWS Config Managed Rule: cloudfront-origin-failover-enabled`

Criteri di avviso

Giallo: il failover di CloudFront origine di Amazon non è abilitato.

Operazione consigliata

Assicurati di attivare la funzionalità di failover di origine per le tue CloudFront distribuzioni per garantire un'elevata disponibilità della distribuzione dei contenuti agli utenti finali. Quando attivi questa funzionalità, il traffico viene indirizzato automaticamente al server di origine di backup se il server di origine principale non è disponibile. Ciò riduce al minimo i potenziali tempi di inattività e garantisce una disponibilità continua dei contenuti.

Colonne del report

- Stato
- Regione
- Risorsa

- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Rischio di accesso agli endpoint Amazon Comprehend

Descrizione

Verifica le autorizzazioni della chiave AWS Key Management Service (AWS KMS) per un endpoint in cui il modello sottostante è stato crittografato utilizzando chiavi gestite dal cliente. Se la chiave gestita dal cliente è disattivata, oppure la policy della chiave è stata cambiata per modificare le autorizzazioni consentite per Amazon Comprehend, la disponibilità degli endpoint potrebbe essere compromessa.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`Cm24dfsM13`

Criteri di avviso

Rosso: se la chiave gestita dal cliente è disattivata, oppure la policy della chiave è stata cambiata per modificare le autorizzazioni consentite per l'accesso ad Amazon Comprehend.

Operazione consigliata

Se la chiave gestita dal cliente è stata disabilitata, ti consigliamo di abilitarla. Per ulteriori informazioni, consulta Abilitazione delle chiavi. Se la policy chiave è stata modificata e desideri continuare a utilizzare l'endpoint, ti consigliamo di aggiornare la policy chiave. AWS KMS Per ulteriori informazioni, vedere Modifica di una policy delle chiavi.

Risorse aggiuntive

AWS KMS Autorizzazioni

Colonne del report

- Stato
- Regione
- ARN endpoint
- ARN modello
- KMS KeyId
- Ora ultimo aggiornamento

Cluster Amazon DocumentDB Single AZ

Descrizione

Verifica se esistono cluster Amazon DocumentDB configurati come Single-AZ.

L'esecuzione di carichi di lavoro Amazon DocumentDB in un'architettura Single-AZ non è sufficiente per carichi di lavoro altamente critici e il ripristino in caso di guasto di un componente può richiedere fino a 10 minuti. I clienti devono distribuire le istanze di replica in zone di disponibilità aggiuntive per garantire la disponibilità durante la manutenzione, i guasti delle istanze, i guasti dei componenti o i guasti delle zone di disponibilità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente una o più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c15vnddn2x`

Criteri di avviso

Giallo: il cluster Amazon DocumentDB ha istanze in meno di tre zone di disponibilità.

Verde: il cluster Amazon DocumentDB ha istanze in tre zone di disponibilità.

Operazione consigliata

Se la tua applicazione richiede un'elevata disponibilità, modifica l'istanza DB per abilitare Multi-AZ utilizzando istanze di replica. Scopri Amazon DocumentDB High Availability e Replica

Risorse aggiuntive

Comprendere la tolleranza agli errori del cluster Amazon DocumentDB

Regioni e zone di disponibilità

Colonne del report

- Stato
- Regione
- Zona di disponibilità
- DB Cluster Identifier (Identificatore cluster database)
- ARN del cluster DB
- Ora ultimo aggiornamento

Ripristino Amazon DynamoDB oint-in-time P

Descrizione

Controlla se per le tabelle di Amazon DynamoDB è abilitato il ripristino point-in-time.

Il ripristino point-in-time contribuisce a proteggere le tabelle di DynamoDB da operazioni di scrittura o eliminazione accidentali. Grazie al ripristino point-in-time, non devi preoccuparti di creare, gestire o pianificare i backup on demand. Il ripristino point-in-time ripristina le tabelle a qualunque momento nel tempo degli ultimi 35 giorni. DynamoDB conserva i backup incrementali della tabella.

Per ulteriori informazioni, consulta P oint-in-time recovery for DynamoDB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

```
c18d2gz138
```

Origine

```
AWS Config Managed Rule: dynamodb-pitr-enabled
```

Criteri di avviso

Giallo: oint-in-time il ripristino P non è abilitato per le tabelle DynamoDB.

Operazione consigliata

Attiva il point-in-time ripristino in Amazon DynamoDB per eseguire il backup continuo dei dati delle tabelle.

Per ulteriori informazioni, consulta P oint-in-time recovery: How it Works.

Risorse aggiuntive

oint-in-time Ripristino P per DynamoDB

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Tabella di Amazon DynamoDB non inclusa nel piano di backup

Descrizione

Verifica se le tabelle Amazon DynamoDB fanno parte di un piano. AWS Backup

AWS Backup fornisce backup incrementali per le tabelle DynamoDB che acquisiscono le modifiche apportate dall'ultimo backup. L'inclusione delle tabelle DynamoDB in AWS Backup un piano aiuta a proteggere i dati da scenari di perdita accidentale dei dati e automatizza il processo di backup. Ciò fornisce una soluzione di backup affidabile e scalabile per le tabelle di DynamoDB, contribuendo alla protezione dei dati importanti e alla loro disponibilità per un eventuale ripristino.

Per ulteriori informazioni, consulta Creazione di backup di tabelle DynamoDB con AWS Backup

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz107`

Origine

`AWS Config Managed Rule: dynamodb-in-backup-plan`

Criteri di avviso

Giallo: la tabella Amazon DynamoDB non è inclusa nel piano. AWS Backup

Operazione consigliata

Assicurati che le tue tabelle Amazon DynamoDB facciano parte di un piano. AWS Backup

Risorse aggiuntive

Backup pianificati

Che cos'è? AWS Backup

Creazione di piani di backup tramite la console Backup AWS

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Amazon EBS non incluso nel piano AWS Backup

Descrizione

Verifica se i volumi Amazon EBS sono presenti nei piani di backup per AWS Backup.

Includi i volumi Amazon EBS in un AWS Backup piano per automatizzare i backup regolari dei dati archiviati su tali volumi. Ciò ti protegge dalla perdita di dati, semplifica la gestione dei dati e consente il ripristino dei dati quando necessario. Un piano di backup contribuisce a garantire la sicurezza dei dati e a soddisfare gli obiettivi in termini di tempi e punti di ripristino (RTO/RPO) per la tua applicazione e i tuoi servizi.

Per ulteriori informazioni, consulta Creazione di un piano di backup

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz106`

Origine

`AWS Config Managed Rule: ebs-in-backup-plan`

Criteri di avviso

Giallo: il volume Amazon EBS non è incluso nel AWS Backup piano.

Operazione consigliata

Assicurati che i tuoi volumi Amazon EBS facciano parte di un AWS Backup piano.

Risorse aggiuntive

Creazione di piani di backup utilizzando la console AWS Backup

Che cos'è AWS Backup?

Nozioni di base 3: creazione di un backup pianificato

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Snapshot Amazon EBS

Descrizione

Controlla l'età degli snapshot per i volumi Amazon Elastic Block Store (Amazon EBS) (disponibili o in uso).

Anche se i volumi Amazon EBS vengono replicati, possono verificarsi fallimenti. Le istantanee vengono salvate in modo persistente su Amazon Simple Storage Service (Amazon S3) per uno storage e un ripristino durevoli. point-in-time

ID di controllo

`H7IgTzjTYb`

Criteri di avviso

- Giallo: lo snapshot più recente del volume risale a un periodo compreso tra 7 e 30 giorni fa.
- Rosso: lo snapshot più recente del volume risale a più di 30 giorni fa.
- Rosso: il volume non ha uno snapshot.

Operazione consigliata

Crea snapshot settimanali o mensili dei tuoi volumi. Per ulteriori informazioni, consulta Creazione di uno snapshot Amazon EBS.

Risorse aggiuntive

Amazon Elastic Block Store (Amazon EBS)

Colonne del report

- Stato

- Regione
- ID volume
- Nome volume
- ID snapshot
- Nome snapshot
- Età snapshot
- Allegato volume
- Motivo

Per il dimensionamento automatico Amazon EC2 non è abilitato il controllo dell'integrità ELB

Descrizione

Verifica se i gruppi con dimensionamento automatico Amazon EC2 associati a un Classic Load Balancer utilizzano i controlli dell'integrità di Elastic Load Balancing. I controlli dell'integrità predefiniti per un gruppo con dimensionamento automatico sono solamente controlli dello stato di Amazon EC2. Se un'istanza non supera i controlli dello stato, viene contrassegnata come non integra e viene interrotta. In questo caso, il dimensionamento automatico Amazon EC2 avvia una nuova istanza sostitutiva. Il controllo dell'integrità di Elastic Load Balancing monitora periodicamente le istanze di Amazon EC2 per rilevare e terminare le istanze non integre, e per avviare nuove istanze.

Per ulteriori informazioni, consulta Aggiungere i controlli di integrità di Elastic Load Balancing.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz104`

Origine

`AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required`

Criteri di avviso

Giallo: un gruppo con dimensionamento automatico Amazon EC2 collegato a un Classic Load Balancer non ha abilitato i controlli dell'integrità di Elastic Load Balancing.

Operazione consigliata

Assicurati che i gruppi con dimensionamento automatico associati a un Classic Load Balancer utilizzino i controlli dell'integrità di Elastic Load Balancing.

I controlli dell'integrità di Elastic Load Balancing segnalano se il sistema di bilanciamento del carico è integro e disponibile alla gestione delle richieste. Ciò garantisce una disponibilità elevata per l'applicazione.

Per ulteriori informazioni, consulta Aggiunta dei controlli dell'integrità di Elastic Load Balancing a un gruppo con dimensionamento automatico

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Per il gruppo con dimensionamento automatico Amazon EC2 è abilitato il ribilanciamento della capacità

Descrizione

Controlla se il ribilanciamento della capacità è abilitato per i gruppi con dimensionamento automatico Amazon EC2 che utilizzano più tipi di istanze.

La configurazione dei gruppi con dimensionamento automatico Amazon EC2 con ribilanciamento della capacità contribuisce a garantire che le istanze Amazon EC2 siano distribuite uniformemente

tra le zone di disponibilità, indipendentemente dai tipi di istanze e dalle opzioni di acquisto. Utilizza una policy di tracciamento degli obiettivi associata al gruppo, ad esempio l'utilizzo della CPU o il traffico di rete.

Per ulteriori informazioni, consulta Gruppi con dimensionamento automatico con più tipi di istanze e opzioni di acquisto.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`AWS Config c18d2gz103`

Origine

AWS Config Regola gestita: autoscaling-capacity-rebalancing

Criteri di avviso

Giallo: il ribilanciamento della capacità dei gruppi con dimensionamento automatico Amazon EC2 non è abilitato.

Operazione consigliata

Assicurati che il ribilanciamento della capacità sia abilitato per i gruppi con dimensionamento automatico Amazon EC2 che utilizzano più tipi di istanze.

Per ulteriori informazioni, consulta Abilitazione del ribilanciamento della capacità (console)

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input

- Ora ultimo aggiornamento

Il dimensionamento automatico Amazon EC2 non è distribuito in più AZ o non soddisfa il numero minimo di AZ

Descrizione

Controlla se il gruppo con dimensionamento automatico Amazon EC2 è distribuito in più zone di disponibilità o il numero minimo di zone di disponibilità specificato. Implementa le istanze di Amazon EC2 in più zone di disponibilità per garantire una disponibilità elevata.

Puoi modificare il numero minimo di zone di disponibilità utilizzando il AvailibilityZones parametro min nelle tue AWS Config regole.

Per ulteriori informazioni, consulta Gruppi con dimensionamento automatico con più tipi di istanze e opzioni di acquisto.

ID di controllo

`c18d2gz101`

Origine

`AWS Config Managed Rule: autoscaling-multiple-az`

Criteri di avviso

Rosso: per il gruppo con dimensionamento automatico Amazon EC2 non sono configurate diverse AZ o il gruppo non soddisfa il numero minimo di AZ specificato.

Operazione consigliata

Assicurati che il gruppo con dimensionamento automatico Amazon EC2 sia configurato con più AZ. Implementa le istanze di Amazon EC2 in più zone di disponibilità per garantire una disponibilità elevata.

Risorse aggiuntive

Creazione di un gruppo con dimensionamento automatico utilizzando un modello di avvio

Creare un gruppo con dimensionamento automatico utilizzando una configurazione di avvio

Colonne del report

- Stato

- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Bilanciamento della zona di disponibilità Amazon EC2

Descrizione

Controlla la distribuzione delle istanze Amazon Elastic Compute Cloud (Amazon EC2) tra le zone di disponibilità in una regione.

Le zone di disponibilità sono ubicazioni distinte all'interno di una regione isolata dai fallimenti che si verificano in altre zone di disponibilità. Ciò offre una connettività di rete non costosa e a bassa latenza tra zone di disponibilità nella stessa Regione. Avviando istanze in più zone di disponibilità nella stessa Regione, potrai proteggere le tue applicazioni da un solo punto di fallimento.

ID di controllo

`wuy7G1zxql`

Criteri di avviso

- Giallo: la regione ha istanze in più zone, ma la distribuzione non è uniforme (la differenza tra il numero di istanze più alto e più basso nelle zone di disponibilità utilizzate è maggiore del 20%).
- Rosso: la regione ha istanze solo in un'unica zona di disponibilità.

Operazione consigliata

Bilancia in modo uniforme le istanze Amazon EC2 in più zone di disponibilità. Puoi farlo avviando le istanze manualmente o usando Auto Scaling per farlo automaticamente. Per ulteriori informazioni, consulta Avvio dell'istanza e Bilanciamento del carico del gruppo con scalabilità automatica.

Risorse aggiuntive

Guida per l'utente di Dimensionamento automatico Amazon EC2

Colonne del report

- Stato

- Regione
- Istanze della zona a
- Istanze della zona b
- Istanze della zona c
- Istanze della zona e
- Istanze della zona f
- Motivo

Monitoraggio dettagliato di Amazon EC2 non abilitato

Descrizione

Controlla se il monitoraggio dettagliato è abilitato per le istanze di Amazon EC2.

Il monitoraggio dettagliato di Amazon EC2 fornisce parametri più frequenti, pubblicati a intervalli di un minuto, diversamente dagli intervalli di cinque minuti utilizzati nel monitoraggio di base di Amazon EC2. L'utilizzo di un monitoraggio dettagliato per Amazon EC2 facilita e migliora la gestione delle risorse di Amazon EC2, consentendoti di individuare le tendenze e intervenire più rapidamente.

Per ulteriori informazioni, consulta Monitoraggio di base e monitoraggio dettagliato.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`AWS Config c18d2gz144`

Origine

AWS Config Regola gestita: ec2-instance-detailed-monitoring-enabled

Criteri di avviso

Giallo: il monitoraggio dettagliato non è abilitato per le istanze di Amazon EC2.

Operazione consigliata

Attiva il monitoraggio dettagliato per le tue istanze Amazon EC2 per aumentare la frequenza con cui i dati metrici di Amazon EC2 vengono pubblicati su Amazon CloudWatch (da 5 a intervalli di 1 minuto).

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Driver Amazon ECS AWS Logs in modalità di blocco

Descrizione

Verifica le definizioni delle attività di Amazon ECS configurate con il driver di registrazione AWS Logs in modalità di blocco. Un driver configurato in modalità di blocco mette a rischio la disponibilità del sistema.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente una o più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dvkm4z6b`

Criteri di avviso

Giallo: la modalità dei parametri di configurazione della registrazione del driver awslogs è impostata su blocco o mancante. Un parametro di modalità mancante indica una configurazione di blocco predefinita.

Verde: la definizione delle attività di Amazon ECS non utilizza il driver awslogs o il driver awslogs è configurato in modalità non bloccante.

Operazione consigliata

Per mitigare il rischio di disponibilità, prendi in considerazione la possibilità di modificare la configurazione del driver Logs per la definizione dell'attività da bloccante a non bloccante. AWS Con la modalità non bloccante, è necessario impostare un valore per il parametro. max-buffer-size Per ulteriori informazioni e indicazioni sui parametri di configurazione, vedere. Vedi Prevenzione della perdita di log con la modalità non bloccante nel driver di AWS log del contenitore Logs

Risorse aggiuntive

Utilizzo del driver AWS Logs Log

Scelta delle opzioni di registrazione dei container per evitare la contropressione

Prevenzione della perdita di log con la modalità non bloccante nel driver di AWS registro del contenitore Logs

Colonne del report

- Stato
- Regione
- ARN di definizione dell'attività
- Nomi di definizione dei contenitori
- Ora ultimo aggiornamento

Servizio Amazon ECS con un'unica AZ

Descrizione

Controlla se la configurazione del servizio utilizza un'unica zona di disponibilità (AZ).

Un'AZ è una distinta posizione che è isolata da errori presenti in altre zone. Ciò supporta una connettività di rete poco costosa e a bassa latenza tra diverse AZ nella stessa Regione AWS.

Avviando istanze in più AZ nella stessa regione, puoi facilitare la protezione delle applicazioni da un solo punto di errore.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1z7dfpz01`

Criteri di avviso

- Giallo: un servizio di Amazon ECS esegue tutte le attività in un'unica AZ.
- Verde: un servizio di Amazon ECS esegue attività in almeno due AZ diverse.

Operazione consigliata

Crea almeno un'altra attività per il servizio in un’AZ diversa.

Risorse aggiuntive

Capacità e disponibilità di Amazon ECS

Colonne del report

- Stato
- Regione
- Nome cluster ECS / Nome servizio ECS
- Numero delle zone di disponibilità
- Ora ultimo aggiornamento

Strategia di collocazione Multi-AZ di Amazon ECS

Descrizione

Controlla se il tuo servizio di Amazon ECS utilizza la strategia di collocazione distribuita basata sulla zona di disponibilità (AZ). Questa strategia distribuisce le attività tra le zone di

disponibilità all'interno delle stesse zone di disponibilità Regione AWS e può aiutare a proteggere le applicazioni da un singolo punto di errore.

Per le attività eseguite nell'ambito di un servizio di Amazon ECS, la strategia predefinita per la collocazione delle attività è quella distribuita.

Questo controllo verifica anche che la strategia distribuita sia la prima o l'unica nell'elenco delle strategie di collocazione abilitate.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1z7dfpz02`

Criteri di avviso

- Giallo: la collocazione distribuita in base alla zona di disponibilità è disabilitata o non è la prima strategia nell'elenco di strategie di collocazione abilitate per il servizio di Amazon ECS.
- Verde: la collocazione distribuita in base alla zona di disponibilità è la prima strategia nell'elenco di strategie di collocazione abilitate o l'unica strategia di collocazione abilitata per il tuo servizio di Amazon ECS.

Operazione consigliata

Abilita la strategia di collocazione distribuita delle attività per distribuire le attività su più AZ. Verifica che la distribuzione per zona di disponibilità sia l'unica strategia utilizzata o la prima strategia per tutte le strategie di collocazione delle attività abilitate. Se scegli di gestire la collocazione delle AZ, puoi utilizzare un servizio con mirroring in un'altra AZ per ridurre questi rischi.

Risorse aggiuntive

Strategie di collocazione delle attività di Amazon ECS

Colonne del report

- Stato

- Regione
- Nome cluster ECS / Nome servizio ECS
- Strategia di collocazione distribuita delle attività abilitata e applicata correttamente
- Ora ultimo aggiornamento

Amazon EFS senza ridondanza di destinazione di montaggio

Descrizione

Controlla se esistono destinazioni di montaggio in più zone di disponibilità per un file system di Amazon EFS.

Una zona di disponibilità è una posizione distinta che è isolata da errori presenti in altre zone. Creando destinazioni di montaggio in più zone di disponibilità geograficamente separate in una regione AWS, puoi ottenere i massimi livelli di disponibilità e durabilità per i tuoi file system di Amazon EFS.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch01`

Criteri di avviso

- Giallo: per il file system è stata creata 1 destinazione di montaggio in un'unica zona di disponibilità.

  Verde: per il file system sono state create almeno 2 destinazioni di montaggio in più zone di disponibilità.

Operazione consigliata

Per i file system EFS che utilizzano classi di archiviazione One Zone, è preferibile creare nuovi file system che utilizzano classi di archiviazione standard ripristinando un backup su un nuovo file system. Crea, quindi, destinazioni di montaggio in più zone di disponibilità.

Per i file system EFS che utilizzano classi di archiviazione standard, è preferibile creare destinazioni di montaggio in più zone di disponibilità.

Risorse aggiuntive

- Gestione delle destinazione di montaggio utilizzando la console di Amazon EFS
- Quote e limiti di Amazon EFS

Colonne del report

- Stato
- Regione
- ID dei file system EFS
- Numero di destinazioni di montaggio
- Numero di AZ
- Ora ultimo aggiornamento

Amazon EFS non è incluso nel AWS Backup piano

Descrizione

Verifica se i file system Amazon EFS sono inclusi nei piani di backup con AWS Backup.

AWS Backup è un servizio di backup unificato progettato per semplificare la creazione, la migrazione, il ripristino e l'eliminazione dei backup, fornendo al contempo report e audit migliorati.

Per ulteriori informazioni, consulta Backing up your Amazon EFS file systems (Backup dei file system Amazon EFS).

ID di controllo

```
c18d2gz117
```

Origine

```
AWS Config Managed Rule: EFS_IN_BACKUP_PLAN
```

Criteri di avviso

Rosso: Amazon EFS non è incluso nel AWS Backup piano.

Operazione consigliata

Assicurati che i tuoi file system Amazon EFS siano inclusi nel tuo AWS Backup piano per proteggerli dalla perdita accidentale o dal danneggiamento dei dati.

Risorse aggiuntive

Backup dei file system di Amazon EFS

Backup e ripristino di Amazon EFS utilizzando AWS Backup.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Cluster Amazon ElastiCache Multi-AZ

Descrizione

Verifica la presenza di ElastiCache cluster distribuiti in un'unica zona di disponibilità (AZ). Questo controllo avvisa quando Multi-AZ è inattivo in un cluster.

Le implementazioni in più AZ migliorano la disponibilità dei ElastiCache cluster mediante la replica asincrona su repliche di sola lettura in una zona di disponibilità diversa. Quando viene effettuata una manutenzione pianificata del cluster o un nodo primario non è disponibile, promuove automaticamente una replica a principale. ElastiCache Questo failover consente la ripresa delle operazioni di scrittura del cluster e non richiede l'intervento di un amministratore.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`ECHdfsQ402`

Criteri di avviso

- Verde: Multi-AZ è attivo nel cluster.
- Giallo: Multi-AZ non è attivo nel cluster.

Operazione consigliata

Crea almeno una replica per partizione, in una zona di disponibilità diversa da quella primaria.

Risorse aggiuntive

Per ulteriori informazioni, consulta Ridurre al minimo i tempi di inattività in ElastiCache Redis with Multi-AZ.

Colonne del report

- Stato
- Regione
- Nome del cluster
- Ora ultimo aggiornamento

Backup automatico dei cluster Amazon ElastiCache Redis

Descrizione

Verifica se i cluster Amazon ElastiCache for Redis hanno attivato il backup automatico e se il periodo di conservazione degli snapshot è superiore al limite predefinito specificato o di 15 giorni. Quando i backup automatici sono abilitati, ElastiCache crea un backup del cluster su base giornaliera.

È possibile specificare il limite di conservazione delle istantanee desiderato utilizzando i RetentionPeriod parametri delle istantanee delle regole. AWS Config

Per ulteriori informazioni, consulta Backup e ripristino ElastiCache per Redis.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz178`

Origine

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

Criteri di avviso

Rosso: nei cluster Amazon ElastiCache for Redis non è attivato il backup automatico o il periodo di conservazione degli snapshot è inferiore al limite.

Operazione consigliata

Assicurati che i cluster Amazon ElastiCache for Redis abbiano attivato il backup automatico e che il periodo di conservazione degli snapshot sia superiore al limite predefinito specificato o di 15 giorni. I backup automatici possono fornire protezione da perdita di dati. In caso di esito negativo, puoi creare un nuovo cluster, ripristinando i dati dal backup più recente.

Per ulteriori informazioni, consulta Backup e ripristino ElastiCache per Redis.

Risorse aggiuntive

Per ulteriori informazioni, consulta Pianificazione di backup automatici.

Colonne del report

- Stato
- Regione
- Nome del cluster
- Ora ultimo aggiornamento

Cluster Multi-AZ Amazon MemoryDB

Descrizione

Controlla cluster MemoryDB implementati in una singola zona di disponibilità (AZ). Questo controllo avvisa quando Multi-AZ è inattivo in un cluster.

Le implementazioni in più AZ migliorano la disponibilità dei cluster MemoryDB eseguendo la replica asincrona in repliche di sola lettura in un'AZ diversa. Quando si verifica una manutenzione pianificata dei cluster o se un nodo primario non è disponibile, MemoryDB promuove automaticamente una replica a primaria. Questo failover consente la ripresa delle operazioni di scrittura del cluster e non richiede l'intervento di un amministratore.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`MDBdfsQ401`

Criteri di avviso

- Verde: Multi-AZ è attivo nel cluster.
- Giallo: Multi-AZ non è attivo nel cluster.

Operazione consigliata

Crea almeno una replica per partizione, in una zona di disponibilità diversa da quella primaria.

Risorse aggiuntive

Per ulteriori informazioni, consulta Riduzione dei tempi di inattività in MemoryDB con Multi-AZ.

Colonne del report

- Stato
- Regione
- Nome del cluster
- Ora ultimo aggiornamento

Broker Amazon MSK che ospitano un numero eccessivo di partizioni

Descrizione

Controlla se ai broker di un cluster Managed Streaming for Kafka (MSK) è assegnato un numero di partizioni maggiore rispetto a quello consigliato.

ID di controllo

`Cmsvnj8vf1`

Criteri di avviso

- Rosso: il broker MSK ha raggiunto o superato il 100% del limite di partizione massimo consigliato
- Giallo: MSK ha raggiunto l'80% del limite di partizione massimo consigliato

Operazione consigliata

Segui le procedure consigliate per MSK per dimensionare il cluster MSK o eliminare le partizioni inutilizzate.

Risorse aggiuntive

- Dimensionamento corretto del cluster

Colonne del report

- Stato
- Regione
- ARN del cluster
- ID del broker
- Conteggio partizioni

Domini Amazon OpenSearch Service con meno di tre nodi di dati

Descrizione

Verifica se i domini Amazon OpenSearch Service sono configurati con almeno tre nodi di dati e se ZoneAwarenessEnabled sono veri. ZoneAwarenessEnabled Se abilitato, Amazon OpenSearch Service garantisce che ogni shard primario e la replica corrispondente siano allocati in diverse zone di disponibilità.

Per ulteriori informazioni, consulta Configurazione di un dominio Multi-AZ in Amazon OpenSearch Service.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz183`

Origine

`AWS Config Managed Rule: opensearch-data-node-fault-tolerance`

Criteri di avviso

Giallo: i domini Amazon OpenSearch Service sono configurati con meno di tre nodi di dati.

Operazione consigliata

Assicurati che i domini Amazon OpenSearch Service siano configurati con un minimo di tre nodi di dati. Configura un dominio Multi-AZ per migliorare la disponibilità del cluster Amazon OpenSearch Service allocando nodi e replicando i dati su tre zone di disponibilità all'interno della stessa regione. Ciò previene la perdita di dati e riduce al minimo i tempi di inattività in caso di errore (nella AZ) di un nodo o del data center (AZ).

Per ulteriori informazioni, consulta Aumentare la disponibilità per Amazon OpenSearch Service implementandolo in tre zone di disponibilità.

Risorse aggiuntive

- Aumenta la disponibilità di Amazon OpenSearch Service implementandolo in tre zone di disponibilità

Colonne del report

- Stato
- Regione
- Risorsa

- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Backup Amazon RDS

Descrizione

Verifica la disponibilità di backup automatici delle istanze DB Amazon RDS.

Per impostazione predefinita, i backup sono abilitati con un periodo di conservazione di un giorno. I backup riducono il rischio di perdita imprevista dei dati e consentono il point-in-time ripristino.

ID di controllo

`opQPADkZvH`

Criteri di avviso

Rosso: il periodo di conservazione del backup di un'istanza DB è impostato su 0 giorni.

Operazione consigliata

Imposta il periodo di conservazione per il backup automatico dell'istanza DB da 1 a 35 giorni in base ai requisiti dell'applicazione. Consulta Utilizzo di backup automatici.

Risorse aggiuntive

Nozioni di base su Amazon RDS

Colonne del report

- Stato
- Regione/AZ
- Istanza database
- ID VPC
- Periodo di retention dei backup

I cluster Amazon RDS DB dispongono di un'istanza DB

Descrizione

Aggiungi almeno un'altra istanza DB al cluster DB per migliorare la disponibilità e le prestazioni.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt011`

Criteri di avviso

Giallo: i cluster DB hanno una sola istanza DB.

Operazione consigliata

Aggiungi un'istanza DB reader al cluster DB.

Risorse aggiuntive

Nella configurazione corrente, viene utilizzata un'istanza DB per le operazioni di lettura e scrittura. È possibile aggiungere un'altra istanza DB per consentire la ridistribuzione della lettura e un'opzione di failover.

Per ulteriori informazioni, consulta Alta disponibilità per Amazon Aurora.

Colonne del report

- Stato
- Regione
- Risorsa

- Nome del motore
- Classe di istanza database
- Ora ultimo aggiornamento

Cluster Amazon RDS DB con tutte le istanze nella stessa zona di disponibilità

Descrizione

I cluster DB si trovano attualmente in un'unica zona di disponibilità. Utilizza più zone di disponibilità per migliorare la disponibilità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt007`

Criteri di avviso

Giallo: i cluster DB hanno tutte le istanze nella stessa zona di disponibilità.

Operazione consigliata

Aggiungi le istanze DB a più zone di disponibilità del tuo cluster DB.

Risorse aggiuntive

Ti consigliamo di aggiungere le istanze DB a più zone di disponibilità in un cluster DB. L'aggiunta di istanze DB a più zone di disponibilità migliora la disponibilità del cluster DB.

Per ulteriori informazioni, consulta Alta disponibilità per Amazon Aurora.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Cluster Amazon RDS DB con tutte le istanze di lettura nella stessa zona di disponibilità

Descrizione

Tutte le istanze di lettura del cluster di database sono nella stessa zona di disponibilità. Ti consigliamo di distribuire le istanze Reader su più zone di disponibilità del tuo cluster DB.

La distribuzione aumenta la disponibilità del database e migliora i tempi di risposta riducendo la latenza di rete tra i client e il database.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.

Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt018`

Criteri di avviso

Rosso: i cluster DB hanno le istanze di lettura nella stessa zona di disponibilità.

Operazione consigliata

Distribuisci le istanze del lettore su più zone di disponibilità.

Risorse aggiuntive

Le zone di disponibilità (AZ) sono località distinte l'una dall'altra per garantire l'isolamento in caso di interruzioni all'interno di ciascuna regione. AWS Si consiglia di distribuire l'istanza primaria e le istanze di lettura nel cluster DB su più AZ per migliorare la disponibilità del cluster DB. Puoi creare un cluster Multi-AZ utilizzando l' AWS Management Console API Amazon RDS o Amazon RDS al momento della creazione del cluster. AWS CLIÈ possibile modificare il cluster Aurora esistente in un cluster Multi-AZ aggiungendo una nuova istanza di lettura e specificando una AZ diversa.

Per ulteriori informazioni, consulta Alta disponibilità per Amazon Aurora.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Monitoraggio avanzato delle istanze DB Amazon RDS non abilitato

Descrizione

Controlla se per le istanze DB di Amazon RDS è abilitato il monitoraggio avanzato.

Il monitoraggio avanzato di Amazon RDS fornisce parametri in tempo reale per il sistema operativo (OS) su cui viene eseguita l'istanza DB. Tutti i parametri di sistema e le informazioni sui

processi per le istanze DB di Amazon RDS possono essere visualizzati sulla console di Amazon RDS. Puoi anche personalizzare il pannello di controllo. Con il monitoraggio avanzato ottieni la visibilità dello stato operativo dell'istanza di Amazon RDS quasi in tempo reale, per cui puoi di reagire più rapidamente in caso di problemi operativi.

È possibile specificare l'intervallo di monitoraggio desiderato utilizzando il parametro monitoringInterval delle regole. AWS Config

Per ulteriori informazioni, consulta Panoramica sul monitoraggio avanzato e Metriche OS nel monitoraggio avanzato.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz158`

Origine

`AWS Config Managed Rule: rds-enhanced-monitoring-enabled`

Criteri di avviso

Giallo: per le istanze DB di Amazon RDS non è abilitato il monitoraggio avanzato o le istanze non sono configurate con l'intervallo desiderato.

Operazione consigliata

Abilita il monitoraggio avanzato per le istanze DB di Amazon RDS per migliorare la visibilità dello stato operativo delle istanze di Amazon RDS.

Per ulteriori informazioni, consulta Monitoraggio delle metriche OS con il monitoraggio avanzato.

Risorse aggiuntive

Metriche OS nel monitoraggio avanzato

Colonne del report

- Stato

- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

La scalabilità automatica dello storage sulle istanze DB di Amazon RDS è disattivata

Descrizione

La scalabilità automatica dello storage Amazon RDS non è attivata per l'istanza DB. In caso di aumento del carico di lavoro del database, la scalabilità automatica di RDS Storage ridimensiona automaticamente la capacità di storage senza tempi di inattività.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt013`

Criteri di avviso

Rosso: sulle istanze DB non è attivata la scalabilità automatica dello storage.

Operazione consigliata

Attiva la scalabilità automatica dello storage Amazon RDS con una soglia di storage massima specificata.

Risorse aggiuntive

La scalabilità automatica dello storage Amazon RDS ridimensiona automaticamente la capacità di storage senza tempi di inattività quando il carico di lavoro del database aumenta. La scalabilità automatica dello storage monitora l'utilizzo dello storage e aumenta automaticamente la capacità quando l'utilizzo è vicino alla capacità di storage fornita. Puoi specificare un limite massimo per lo storage che Amazon RDS può allocare all'istanza DB. Non sono previsti costi aggiuntivi per la scalabilità automatica dello storage. Paghi solo per le risorse Amazon RDS allocate alla tua istanza DB. Ti consigliamo di attivare la scalabilità automatica dello storage Amazon RDS.

Per ulteriori informazioni, consulta Gestione automatica della capacità con scalabilità automatica Amazon RDS dello storage.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Istanze database Amazon RDS che non utilizzano la distribuzione Multi-AZ

Descrizione

Consigliamo di usare l'implementazione multi-AZ. Le implementazioni multi-AZ migliorano la disponibilità e la durabilità dell'istanza database.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt019`

Criteri di avviso

Giallo: le istanze DB non utilizzano la distribuzione Multi-AZ.

Operazione consigliata

Configura Multi-AZ per le istanze DB interessate.

Risorse aggiuntive

In una distribuzione Amazon RDS Multi-AZ, Amazon RDS crea automaticamente un'istanza di database principale e replica i dati su un'istanza in una zona di disponibilità diversa. Quando rileva un errore, Amazon RDS esegue automaticamente il failover su un'istanza di standby senza intervento manuale.

Per ulteriori informazioni, consulta la sezione Prezzi di .

Colonne del report

- Stato

- Regione
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Amazon RDS DiskQueueDepth

Descrizione

Verifica se la CloudWatch metrica DiskQueueDepth mostra che il numero di scritture in coda sullo storage del database dell'istanza RDS è cresciuto a un livello tale da richiedere un'indagine operativa.

ID di controllo

`Cmsvnj8db3`

Criteri di avviso

- Rosso: DiskQueueDepth CloudWatch la metrica ha superato i 10
- Giallo: la DiskQueueDepth CloudWatch metrica è maggiore di 5 ma minore o uguale a 10
- Verde: la DiskQueueDepth CloudWatch metrica è minore o uguale a 5

Operazione consigliata

Prendi in considerazione il passaggio a istanze e volumi di archiviazione che supportano le caratteristiche di lettura/scrittura.

Colonne del report

- Stato
- Regione
- ARN dell’istanza DB
- DiskQueueDepth Metrico

Amazon RDS FreeStorageSpace

Descrizione

Verifica se la FreeStorageSpace CloudWatch metrica per un'istanza di database RDS è aumentata al di sopra di una soglia ragionevole dal punto di vista operativo.

ID di controllo

`Cmsvnj8db2`

Criteri di avviso

- Rosso: FreeStorageSpace ha raggiunto o superato il 90% della capacità totale
- Giallo: FreeStorageSpace è compreso tra l'80% e il 90% della capacità totale
- Verde: FreeStorageSpace è inferiore all'80% della capacità totale

Operazione consigliata

Aumenta lo spazio di storage per l'istanza di database RDS che sta esaurendo lo spazio di archiviazione gratuito utilizzando la console di gestione Amazon RDS, l'API Amazon RDS o l'interfaccia a riga di comando AWS.

Colonne del report

- Stato
- Regione
- ARN dell'istanza DB
- FreeStorageSpace Metrica (MB)
- Archiviazione allocata delle istanze DB (MB)
- Percentuale di archiviazione utilizzata dalle istanze DB

Il parametro log_output di Amazon RDS è impostato su tabella

Descrizione

Quando log_output è impostato su TABLE, viene utilizzato più spazio di archiviazione rispetto a quando log_output è impostato su FILE. Si consiglia di impostare il parametro su FILE per evitare di raggiungere il limite di dimensione di archiviazione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt023`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno il parametro log_output impostato su TABLE.

Operazione consigliata

Imposta il valore del parametro log_output su FILE nei gruppi di parametri DB.

Risorse aggiuntive

Per ulteriori informazioni, consulta File di registro del database MySQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

L'impostazione del parametro innodb_default_row_format di Amazon RDS non è sicura

Descrizione

L'istanza DB presenta un problema noto: una tabella creata in una versione di MySQL precedente alla 8.0.26 con row_format impostato su COMPACT o REDUNDANT è inaccessibile e irrecuperabile quando l'indice supera i 767 byte.

Ti consigliamo di impostare il valore del parametro innodb_default_row_format su DYNAMIC.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt036`

Criteri di avviso

Rosso: i gruppi di parametri DB hanno un'impostazione non sicura per il parametro innodb_default_row_format.

Operazione consigliata

Imposta il parametro innodb_default_row_format su DYNAMIC.

Risorse aggiuntive

Quando viene creata una tabella con una versione di MySQL precedente alla 8.0.26 con row_format impostato su COMPACT o REDUNDANT, non viene applicata la creazione di indici con un prefisso chiave inferiore a 767 byte. Dopo il riavvio del database, non è possibile accedere o recuperare queste tabelle.

Per ulteriori informazioni, vedere Modifiche in MySQL 8.0.26 (2021-07-20, General Availability) n sul sito Web della documentazione di MySQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro innodb_flush_log_at_trx_commit di Amazon RDS non è 1

Descrizione

Il valore del parametro innodb_flush_log_at_trx_commit dell'istanza DB non è un valore sicuro. Questo parametro controlla la persistenza delle operazioni di commit su disco.

Ti consigliamo di impostare il parametro innodb_flush_log_at_trx_commit su 1.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt030`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno innodb_flush_log_at_trx_commit impostato su un valore diverso da 1.

Operazione consigliata

Imposta il valore del parametro innodb_flush_log_at_trx_commit su 1

Risorse aggiuntive

La transazione del database è duratura quando il buffer di log viene salvato nella memoria durevole. Tuttavia, il salvataggio su disco influisce sulle prestazioni. A seconda del valore impostato per il parametro innodb_flush_log_at_trx_commit, il comportamento del modo in cui i log vengono scritti e salvati sul disco può variare.

- Quando il valore del parametro è 1, i log vengono scritti e salvati sul disco dopo ogni transazione confermata.
- Quando il valore del parametro è 0, i log vengono scritti e salvati sul disco una volta al secondo.
- Quando il valore del parametro è 2, i log vengono scritti dopo il commit di ogni transazione e salvati sul disco una volta al secondo. I dati si spostano dal buffer di memoria InnoDB alla cache del sistema operativo, anch'essa in memoria.

> **Note**
>
> Quando il valore del parametro è diverso da 1, InnoDB non garantisce le proprietà ACID. Le transazioni recenti dell'ultimo secondo potrebbero andare perse quando il database si blocca.

Per ulteriori informazioni, consulta Best practice per la configurazione dei parametri per Amazon RDS for MySQL, parte 1: Parametri relativi alle prestazioni.

Colonne del report

- Stato
- Regione
- Risorsa

- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro max_user_connections di Amazon RDS è basso

Descrizione

Il valore del numero massimo di connessioni simultanee per ogni account di database dell'istanza database non è sufficiente.

Consigliamo di impostare il parametro max_user_connections su un numero maggiore di 5.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt034`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno max_user_connections configurato in modo errato.

Operazione consigliata

Aumentate il valore del parametro max_user_connections a un numero maggiore di 5.

Risorse aggiuntive

L'impostazione max_user_connections controlla il numero massimo di connessioni simultanee consentite per un account utente MySQL. Il raggiungimento di questo limite di connessione causa errori nelle operazioni di amministrazione delle istanze Amazon RDS, come backup, patch e modifiche dei parametri.

Per ulteriori informazioni, vedere Impostazione dei limiti delle risorse dell'account sul sito Web della documentazione MySQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Amazon RDS Multi-AZ

Descrizione

Controlla le istanze del DB implementate in una zona di disponibilità singola (AZ).

Le implementazioni Multi-AZ migliorano la disponibilità del database eseguendo una replica sincrona in un'istanza in standby in un'altra zona di disponibilità. Durante la manutenzione pianificata del database o il fallimento di un'istanza DB o di una zona di disponibilità, Amazon RDS esegue automaticamente il failover in modalità standby. Questo failover consente di riprendere rapidamente le operazioni del database senza intervento amministrativo. Poiché Amazon RDS non supporta l'implementazione Multi-AZ per Microsoft SQL Server, questo controllo non esamina le istanze di SQL Server.

ID di controllo

`f2iK5R6Dep`

Criteri di avviso

Giallo: un'istanza DB viene implementata in un'unica zona di disponibilità.

Operazione consigliata

Se l'applicazione richiede un'elevata disponibilità, modifica l'istanza DB per abilitare l'implementazione multi-AZ. Consulta Disponibilità elevata (multi-AZ).

Risorse aggiuntive

Regioni e zone di disponibilità

Colonne del report

- Stato
- Regione/AZ
- Istanza database
- ID VPC
- Multi-AZ

Amazon RDS non è previsto AWS Backup

Descrizione

Controlla se le istanze DB di Amazon RDS sono incluse in un piano di backup in AWS Backup.

AWS Backup è un servizio di backup completamente gestito che semplifica la centralizzazione e l'automazione del backup dei dati tra i servizi. AWS

Includere un'istanza DB di Amazon RDS in un piano di backup è importante per gli obblighi di conformità alle norme, il ripristino di emergenza, le policy aziendali per la protezione dei dati e gli obiettivi di continuità aziendale.

Per ulteriori informazioni, consulta Che cos'è Backup AWS?.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz159`

Origine

`AWS Config Managed Rule: rds-in-backup-plan`

Criteri di avviso

Giallo: un'istanza database Amazon RDS non è inclusa in un piano di backup con AWS Backup.

Operazione consigliata

Includi le tue istanze DB Amazon RDS in un piano di backup con. AWS Backup

Per ulteriori informazioni, consulta Backup e ripristino di Amazon RDS con Backup AWS.

Risorse aggiuntive

Assegnazione di risorse a un piano di backup

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Le repliche di lettura di Amazon RDS sono aperte in modalità scrivibile

Descrizione

L'istanza DB ha una replica di lettura in modalità scrivibile, che consente gli aggiornamenti dai client.

Ti consigliamo di impostare il parametro read_only su Replica in modo che le TrueIfrepliche di lettura non siano in modalità scrivibile.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt035`

Criteri di avviso

Giallo: i gruppi di parametri DB attivano la modalità scrivibile per le repliche di lettura.

Operazione consigliata

Imposta il valore del parametro read_only su Replica. TrueIf

Risorse aggiuntive

Il parametro read_only controlla l'autorizzazione di scrittura dai client a un'istanza di database. Il valore predefinito per questo parametro è TrueIf Replica. Per un'istanza di replica, TrueIfReplica imposta il valore read_only su ON (1) e disabilita qualsiasi attività di scrittura da parte dei client. Per un'istanza master/writer, TrueIfReplica imposta il valore su OFF (0) e abilita l'attività di scrittura dei client per l'istanza. Quando la replica di lettura viene aperta in modalità scrivibile, i

dati archiviati in questa istanza possono divergere dall'istanza principale, il che causa errori di replica.

Per ulteriori informazioni, consulta Best practice for configuration parameters for Amazon RDS for MySQL, parte 2: Parametri relativi alla replica sul sito Web di documentazione MySQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

I backup automatici delle risorse Amazon RDS sono disattivati

Descrizione

I backup automatici sono disabilitati sulle risorse del database. I backup automatici consentono point-in-time il ripristino dell'istanza DB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt001`

Criteri di avviso

Rosso: nelle risorse Amazon RDS non sono attivati i backup automatici

Operazione consigliata

Attiva i backup automatici con un periodo di conservazione fino a 14 giorni.

Risorse aggiuntive

I backup automatici consentono point-in-time il ripristino delle istanze DB. Ti consigliamo di attivare i backup automatici. Quando attivi i backup automatici per un'istanza DB, Amazon RDS esegue automaticamente un backup completo dei dati ogni giorno durante la finestra di backup preferita. Il backup acquisisce i log delle transazioni quando ci sono aggiornamenti all'istanza DB. Ottieni uno storage di backup all'altezza delle dimensioni di archiviazione dell'istanza DB senza costi aggiuntivi.

Per ulteriori informazioni, consulta le seguenti risorse:

- Abilitazione dei backup automatici
- Demistificazione dei costi dello storage di backup di Amazon RDS

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Il parametro sync_binlog di Amazon RDS è disattivato

Descrizione

La sincronizzazione del log binario con il disco non viene applicata prima che i commit delle transazioni vengano riconosciuti nell'istanza DB.

Si consiglia di impostare il valore del parametro sync_binlog su 1.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt031`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno la registrazione binaria sincrona disattivata.

Operazione consigliata

Imposta il parametro sync_binlog su 1.

Risorse aggiuntive

Il parametro sync_binlog controlla il modo in cui MySQL invia il log binario su disco. Quando il valore di questo parametro è impostato su 1, attiva la sincronizzazione del registro binario su disco prima che le transazioni vengano eseguite. Quando il valore di questo parametro è impostato su 0, disattiva la sincronizzazione del registro binario sul disco. In genere, il server MySQL dipende dal sistema operativo per inviare regolarmente il registro binario su disco, in modo simile ad altri file. Il valore del parametro sync_binlog impostato su 0 può migliorare le prestazioni. Tuttavia, durante un'interruzione dell'alimentazione o un arresto anomalo del sistema

operativo, il server perde tutte le transazioni impegnate che non sono state sincronizzate con i log binari.

Per ulteriori informazioni, consulta Best practice per la configurazione dei parametri per Amazon RDS for MySQL, parte 2: Parametri relativi alla replica.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Per il cluster DB RDS non è abilitata la replica Multi-AZ

Descrizione

Controlla se per i cluster DB di Amazon RDS è abilitata la replica Multi-AZ.

Un cluster di database Multi-AZ ha un'istanza database di scrittore e due istanze database di lettore in tre zone di disponibilità separate. I cluster di database multi-AZ offrono elevata disponibilità, maggiore capacità per i carichi di lavoro in lettura e minore latenza rispetto alle implementazioni Multi-AZ.

Per ulteriori informazioni, consulta Creazione di un cluster DB Multi-AZ.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz161`

Origine

```
AWS Config Managed Rule: rds-cluster-multi-az-enabled
```

Criteri di avviso

Giallo: per il cluster DB di Amazon RDS non è configurata la replica in più AZ

Operazione consigliata

Attiva l'implementazione del cluster DB Multi-AZ quando crei un cluster del database di Amazon RDS.

Per ulteriori informazioni, consulta Creazione di un cluster DB Multi-AZ.

Risorse aggiuntive

Implementazioni di cluster DB Multi-AZ

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Istanza di standby RDS Multi-AZ non abilitata

Descrizione

Controlla se per le istanze DB di Amazon RDS è configurata una replica in standby Multi-AZ.

Amazon RDS Multi-AZ offre disponibilità e durabilità elevate per le istanze del database tramite la replica dei dati su una replica in standby in una zona di disponibilità diversa. Ciò fornisce il failover automatico, aumenta le prestazioni e migliora la durabilità dei dati. In un'implementazione istanza database Multi-AZ, Amazon RDS effettua automaticamente il provisioning e mantiene una replica in standby sincrona in un'altra zona di disponibilità. L'istanza database primaria viene replicata in modo sincrono nelle zone di disponibilità su una replica in standby per fornire ridondanza dati e ridurre al minimo i picchi di latenza durante i backup di sistema. L'esecuzione di un'istanza DB

con disponibilità elevata migliora la disponibilità durante la manutenzione pianificata del sistema. Consente inoltre di proteggere i database da errori dell'istanza database e interruzioni relative alle zone di disponibilità.

Per ulteriori informazioni, consulta Implementazioni di istanze DB Multi-AZ.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz156`

Origine

`AWS Config Managed Rule: rds-multi-az-support`

Criteri di avviso

Giallo: per un'istanza DB di Amazon RDS non è configurata una replica Multi-AZ.

Operazione consigliata

Attiva l'implementazione multi-AZ quando crei un'istanza DB di Amazon RDS.

Questo controllo non può essere escluso dalla visualizzazione nella Trusted Advisor console.

Risorse aggiuntive

Implementazioni delle istanze DB Multi-AZ

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input

- Ora ultimo aggiornamento

Amazon RDS ReplicaLag

Descrizione

Verifica se la ReplicaLag CloudWatch metrica per un'istanza di database RDS è aumentata al di sopra di una soglia ragionevole dal punto di vista operativo nell'ultima settimana.

ReplicaLag metric misura il numero di secondi in cui una replica di lettura rimane indietro rispetto all'istanza principale. Il ritardo della replica si verifica quando gli aggiornamenti asincroni apportati alla replica di lettura non riescono a tenere il passo con gli aggiornamenti dell'istanza del database principale. In caso di errore dell'istanza principale, potrebbero mancare dei dati nella replica di lettura se questa supera una ReplicaLag soglia operativa ragionevole.

ID di controllo

`Cmsvnj8db1`

Criteri di avviso

- Rosso: la ReplicaLag metrica ha superato i 60 secondi almeno una volta alla settimana.
- Giallo: la ReplicaLag metrica ha superato i 10 secondi almeno una volta durante la settimana.
- Verde: ReplicaLag è inferiore a 10 secondi.

Operazione consigliata

Esistono diverse possibili cause ReplicaLag per il superamento dei livelli di sicurezza operativa. L'aumento, ad esempio, può essere determinato da istanze di replica sostituite/avviate di recente da backup precedenti poiché queste repliche richiedono molto tempo per "raggiungere" l'istanza del database principale e le transazioni in tempo reale. Ciò ReplicaLag potrebbe diminuire nel tempo man mano che si verifica il recupero. Un'altra delle possibili ragioni potrebbe essere la velocità delle transazioni raggiungibile sull'istanza del database principale che è superiore a quella raggiungibile dal processo di replica o dall'infrastruttura di replica. Ciò ReplicaLag può aumentare nel tempo, poiché la replica non riesce a tenere il passo con le prestazioni del database principale. Infine, il carico di lavoro può subire interruzioni in diversi periodi della giornata, del mese/ecc., con conseguente occasionale ritardo. ReplicaLag Il team dovrebbe indagare su quale possibile causa principale abbia contribuito alla crescita del database ed eventualmente modificare il tipo di istanza del database o altre caratteristiche del carico di lavoro ReplicaLag per garantire che la continuità dei dati sulla replica soddisfi i requisiti specifici.

Risorse aggiuntive

- Utilizzo delle repliche di lettura per Amazon RDS per PostgreSQL
- Utilizzo della replica MySQL in Amazon RDS
- Uso delle repliche di lettura MySQL

Colonne del report

- Stato
- Regione
- ARN dell'istanza DB
- ReplicaLag Metrica

Il parametro Amazon RDS synchronous_commit è disattivato

Descrizione

Quando il parametro synchronous_commit è disattivato, i dati possono andare persi in caso di arresto anomalo del database. La durabilità del database è a rischio.

Ti consigliamo di attivare il parametro synchronous_commit.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt026`

Criteri di avviso

Rosso: i gruppi di parametri DB hanno il parametro synchronous_commit disattivato.

Operazione consigliata

Attiva il parametro synchronous_commit nei tuoi gruppi di parametri DB.

Risorse aggiuntive

Il parametro synchronous_commit definisce il completamento del processo Write-Ahead Logging (WAL) prima che il server del database invii una notifica corretta al client. Questo commit viene chiamato commit asincrono perché il client riconosce il commit prima che WAL salvi la transazione sul disco. Se il parametro synchronous_commit è disattivato, le transazioni possono andare perse, la durabilità dell'istanza DB potrebbe essere compromessa e i dati potrebbero andare persi quando un database si blocca.

Per ulteriori informazioni, consulta File di registro del database MySQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Snapshot automatiche del cluster di Amazon Redshift

Descrizione

Controlla se le snapshot automatizzate sono abilitate per i cluster di Amazon Redshift.

Amazon Redshift acquisisce automaticamente snapshot incrementali che tengono traccia delle modifiche al cluster dal momento dell'esecuzione dello snapshot automatico precedente. Gli snapshot automatizzati conservano tutti i dati necessari per ripristinare un cluster da uno

snapshot. Per disabilitare gli snapshot automatici, imposta il periodo di conservazione su zero. Non è possibile disattivare gli snapshot automatici per i tipi di nodo RA3.

Puoi specificare il periodo di conservazione minimo e massimo desiderato utilizzando i parametri MinRetentionMaxRetentionPeriodo e Periodo delle tue AWS Config regole.

Snapshot e backup di Amazon Redshift

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz135`

Origine

`AWS Config Managed Rule: redshift-backup-enabled`

Criteri di avviso

Rosso: per Amazon Redshift non sono state configurate snapshot automatiche entro il periodo di conservazione desiderato.

Operazione consigliata

Assicurati che le snapshot automatiche siano abilitate per i cluster di Amazon Redshift.

Per ulteriori informazioni, consulta Gestione di snapshot tramite la console.

Risorse aggiuntive

Snapshot e backup di Amazon Redshift

Per ulteriori informazioni, consulta Utilizzo dei backup.

Colonne del report

- Stato
- Regione

- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Amazon Route 53 ha eliminato i Controlli dell'integrità

Descrizione

Controlla i set di registri delle associati ai controlli di integrità eliminati.

Route 53 non impedisce di eliminare un controllo di integrità associato a uno o più set di registri delle risorse. Se si elimina un controllo di integrità senza aggiornare i set di registri delle risorse associati, il routing delle query DNS per la configurazione di failover DNS non funzionerà come previsto.

Le zone ospitate create dai AWS servizi non verranno visualizzate nei risultati del controllo.

ID di controllo

`Cb877eB72b`

Criteri di avviso

Giallo: un set di record delle risorse è associato a un controllo dell'integrità che è stato eliminato.

Operazione consigliata

Crea un nuovo controllo dell'integrità e associalo al set di record delle risorse. Consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità e Aggiunta dei controlli dell'integrità ai set di record delle risorse.

Risorse aggiuntive

- Controlli dell'integrità e failover DNS di Amazon Route 53
- Funzionamento dei controlli dell'integrità in configurazioni semplici di Amazon Route 53

Colonne del report

- Nome della zona ospitata
- ID della zona ospitata
- Nome del set di registri delle risorse
- Tipo di set di registri delle risorse

- Identificativo del set di record delle risorse

Set di registri delle risorse di Failover Amazon Route 53

Descrizione

Controlla i set di registri delle risorse di failover Amazon Route 53 che presentano una configurazione errata.

Quando i controlli dello stato di Amazon Route 53 determinano che la risorsa principale non è integra, Amazon Route 53 risponde alle domande con un set secondario di registri delle risorse di backup. Affinché il failover funzioni, è necessario creare set di registri delle risorse primarie e secondarie correttamente configurati.

Le zone ospitate create dai AWS servizi non verranno visualizzate nei risultati del controllo.

ID di controllo

`b73EEdD790`

Criteri di avviso

- Giallo: un set di record delle risorse di failover primarie non dispone di un set di registri delle risorse secondarie corrispondente.
- Giallo: un set di registri delle risorse di failover secondarie non dispone di un set di registri delle risorse primarie corrispondente.
- Giallo: i set di record delle risorse primarie e secondarie con lo stesso nome sono associate allo stesso controllo dell'integrità.

Operazione consigliata

Se un set delle risorse di failover non è disponibile, crea il set di record delle risorse corrispondente. Consulta Creazione di set di record delle risorse di failover.

Se i set di record delle risorse sono associati allo stesso controllo dell'integrità, crea controlli dell'integrità separati per ciascuno di essi. Consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità.

Risorse aggiuntive

Controlli dell'integrità e failover DNS di Amazon Route 53

Colonne del report

- Nome della zona ospitata

- ID della zona ospitata
- Nome del set di registri delle risorse
- Tipo di set di registri delle risorse
- Motivo

Set di registri delle risorse TTL (Time-to-Live) alto di Amazon Route 53

Descrizione

Verifica la presenza di set di record di risorse che possono trarre vantaggio dall'avere un valore time-to-live (TTL) inferiore.

TTL indica il numero di secondi in cui un set di registri della risorsa viene memorizzato nella cache dai resolver DNS. Quando si specifica un TTL lungo, i resolver DNS hanno bisogno di più tempo per richiedere record DNS aggiornati, il che può causare ritardi inutili nel reindirizzamento del traffico. Ad esempio, un TTL lungo crea un ritardo tra il momento in cui il Failover DNS rileva un errore dell'endpoint e la risposta quando si reindirizza il traffico.

Le zone ospitate create dai AWS servizi non verranno visualizzate nei risultati del controllo.

ID di controllo

`C056F80cR3`

Criteri di avviso

- Giallo: un set di record delle risorse la cui policy di routing è Failover ha un TTL superiore a 60 secondi.
- Giallo: un set di record delle risorse con un controllo dell'integrità associato ha un TTL superiore a 60 secondi.

Operazione consigliata

Immetti un valore TTL di 60 secondi per i set di record delle risorse elencati. Per ulteriori informazioni, consulta Lavorare con set di registri delle risorse.

Risorse aggiuntive

Controlli dell'integrità e failover DNS di Amazon Route 53

Colonne del report

- Stato

- Nome della zona ospitata
- ID della zona ospitata
- Nome del set di registri delle risorse
- Tipo di set di registri delle risorse
- ID del set di registri delle risorse
- TTL

Deleghe del Server dei nomi Amazon Route 53

Descrizione

Controlla le zone ospitate di Amazon Route 53 per le quali il registrar del dominio o il DNS non utilizza i server dei nomi Route 53 corretti.

Quando crei una zona ospitata, Route 53 assegna un set di deleghe di quattro server di nomi. I nomi di questi server sono ns-###.awsdns-##.com, .net, .org e .co.uk, in cui ### e ## in genere rappresentano numeri diversi. Prima che Route 53 possa indirizzare le query DNS per il dominio, è necessario aggiornare la configurazione del server dei nomi del registrar per rimuovere i server dei nomi assegnati dal registrar. Quindi, è necessario aggiungere tutti e quattro i server dei nomi nel set di delega Route 53. Per ottenere la massima disponibilità, è necessario aggiungere tutti e quattro i server dei nomi Route 53.

Le zone ospitate create dai AWS servizi non verranno visualizzate nei risultati del controllo.

ID di controllo

`cF171Db240`

Criteri di avviso

Giallo: una zona ospitata per la quale il registrar del dominio non utilizza tutti e quattro i server dei nomi di Route 53 nel set di delega.

Operazione consigliata

Aggiungi o aggiorna i record del server dei nomi con il registrar o con il servizio DNS corrente per il tuo dominio in modo da includere tutti e quattro i server dei nomi nel set di delega di Route 53. Per trovare questi valori, consulta Ottenere i server dei nomi per una zona ospitata. Per informazioni sull'aggiunta o l'aggiornamento di record del server dei nomi, consulta Creazione e migrazione di domini e sottodomini su Amazon Route 53.

Risorse aggiuntive

Utilizzo delle zone ospitate

Colonne del report

- Nome della zona ospitata
- ID della zona ospitata
- Numero di deleghe del server dei nomi utilizzate

Amazon Route 53 Resolver Ridondanza della zona di disponibilità degli endpoint

Descrizione

Controlla se la configurazione del servizio include indirizzi IP specificati in almeno due zone di disponibilità (AZ) per la ridondanza. Un'AZ è una posizione distinta che è isolata da errori presenti in altre zone. La specifica di indirizzi IP in più zone di disponibilità nella stessa regione contribuisce alla protezione delle applicazioni da un unico punto di errore.

ID di controllo

`Chrv231ch1`

Criteri di avviso

- Giallo: gli indirizzi IP sono specificati in una sola AZ
- Verde: gli indirizzi IP sono specificati in almeno due AZ

Operazione consigliata

Specifica gli indirizzi IP in almeno due zone di disponibilità per la ridondanza.

Risorse aggiuntive

- Se necessiti che siano sempre disponibili più endpoint dell'interfaccia di rete elastica, ti suggeriamo di creare almeno un'interfaccia di rete in più del necessario, così da disporre di capacità aggiuntiva per gestire eventuali picchi di traffico. L'interfaccia di rete aggiuntiva garantisce inoltre la disponibilità durante le operazioni di servizio, come la manutenzione o gli aggiornamenti.
- Alta disponibilità di endpoint di Resolver

Colonne del report

- Stato

- Regione
- ARN risorsa
- Numero di AZ

Registrazione di Bucket Amazon S3

Descrizione

Controlla la configurazione di registrazione dei bucket Amazon Simple Storage Service (Amazon S3).

Quando la registrazione degli accessi al server è abilitata, i registri di accesso dettagliati vengono recapitati ogni ora a un bucket scelto dall'utente. Un registro dei log di accesso contiene dettagli su ogni richiesta, ad esempio il tipo di richiesta, le risorse specificate nella richiesta e l'ora e la data di elaborazione della richiesta. Per impostazione predefinita, la registrazione dei bucket non è abilitata. È consigliabile abilitare la registrazione se si desidera eseguire controlli di sicurezza od ottenere ulteriori informazioni sugli utenti e sui modelli di utilizzo.

Quando la registrazione è inizialmente abilitata, la configurazione viene convalidata automaticamente. Tuttavia, le modifiche future possono causare errori di registrazione. Questo controllo esamina le autorizzazioni esplicite del bucket di Amazon S3, ma non esamina le policy dei bucket associati che potrebbero sostituire le autorizzazioni del bucket.

ID di controllo

`BueAdJ7NrP`

Criteri di avviso

- Giallo: il bucket non ha la registrazione degli accessi al server abilitata.
- Giallo: le autorizzazioni del bucket di destinazione non includono l'account root, quindi non è possibile controllarlo. Trusted Advisor
- Rosso: il bucket di destinazione non esiste.
- Rosso: il bucket di destinazione e di origine hanno proprietari diversi.
- Rosso: il deliverer del log non dispone dei permessi di scrittura per il bucket di destinazione.

Operazione consigliata

Abilita la registrazione per la maggior parte dei bucket. Consulta Abilitazione della registrazione tramite la console e Abilitazione della registrazione a livello di programmazione.

Se le autorizzazioni del bucket di destinazione non includono l'account root e desideri Trusted Advisor controllare lo stato della registrazione, aggiungi l'account root come beneficiario. Consulta Modifica delle autorizzazioni del bucket.

Se il bucket di destinazione non esiste, seleziona un bucket esistente come destinazione o creane uno nuovo e selezionalo. Consulta Gestione della registrazione del bucket.

Se la destinazione e l'origine hanno proprietari diversi, modifica il bucket di destinazione con uno che abbia lo stesso proprietario del bucket di origine. Consulta Gestione della registrazione del bucket.

Se il deliverer del log non dispone delle autorizzazioni di scrittura per la destinazione (scrittura non abilitata), concedi le autorizzazioni per il caricamento e l'eliminazione al gruppo del log di consegna. Consulta Modifica delle autorizzazioni del bucket.

Risorse aggiuntive

- Utilizzo dei bucket
- Registrazione degli accessi al server
- Formato del log di accesso al server
- Eliminazione di file di log

Colonne del report

- Stato
- Regione
- Bucket Name (Nome bucket)
- Nome destinazione
- Destinazione esistente
- Stesso proprietario
- Scrittura abilitata
- Motivo

Replica di bucket Amazon S3 non abilitata

Descrizione

Controlla se per i bucket di Amazon S3 sono abilitate regole di replica per la replica tra regioni e/o nella stessa regione.

La replica è la copia automatica e asincrona di oggetti tra bucket nella stessa regione o in regioni diverse. AWS Il processo replica gli oggetti appena creati e gli aggiornamenti degli oggetti da un bucket di origine a uno o più bucket di destinazione. Utilizza la replica dei bucket di Amazon S3 per migliorare la resilienza e la conformità delle applicazioni e dell'archiviazione di dati.

Per ulteriori informazioni, consulta Replica di oggetti.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz119`

Origine

`AWS Config Managed Rule: s3-bucket-replication-enabled`

Criteri di avviso

Giallo: le regole di replica dei bucket di Amazon S3 non sono abilitate per la replica tra regioni e/o nella stessa regione.

Operazione consigliata

Attiva le regole di replica dei bucket di Amazon S3 per migliorare la resilienza e la conformità delle applicazioni e dell'archiviazione di dati.

Per ulteriori informazioni, consulta Visualizzazione dei processi di backup e dei punti di ripristino e Configurazione delle repliche.

Risorse aggiuntive

Procedure dettagliate: esempi di configurazione delle repliche

Colonne del report

- Stato
- Regione

- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Amazon S3 Bucket Versioning

Descrizione

Controlli per i bucket di Amazon Simple Storage Service per i quali il controllo delle versioni non è abilitato o è stato sospeso.

Se il controllo della versione è abilitato si può facilmente eseguire il ripristino dopo fallimenti di applicazioni e operazioni non intenzionali dell'utente. Il controllo delle versioni ti permette di mantenere, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. È possibile utilizzare le regole del ciclo di vita per gestire tutte le versioni degli oggetti e i relativi costi, archiviando automaticamente gli oggetti nella classe di archiviazione Glacier. È inoltre possibile configurare le regole per rimuovere le versioni degli oggetti dopo un periodo di tempo specificato. Per eliminare oggetti o modificare la configurazione dei bucket, è inoltre possibile richiedere l'autenticazione a più fattori (MFA).

Il controllo delle versioni non può essere disattivato dopo che è stato attivato. Tuttavia può essere sospeso, il che impedisce la creazione di nuove versioni di oggetti. L'utilizzo del controllo delle versioni può aumentare i costi per Amazon S3, dal momento che l'archiviazione di più versioni di un oggetto è un servizio a pagamento.

ID di controllo

`R365s2Qddf`

Criteri di avviso

- Verde: il controllo delle versioni è abilitato per il bucket.
- Giallo: il controllo delle versioni non è abilitato per il bucket.
- Giallo: il controllo delle versioni è sospeso per il bucket.

Operazione consigliata

Abilita il controllo delle versioni per la maggior parte dei bucket in modo da evitare l'eliminazione o la sovrascrittura accidentali. Consulta Uso del controllo delle versioni e Abilitazione del controllo delle versioni a livello programmatico.

Se il controllo delle versioni del bucket è sospeso, valuta la possibilità di riabilitarlo. Per informazioni su come lavorare con gli oggetti di un bucket con il controllo delle versioni sospeso, consulta Gestione degli oggetti di un bucket con il controllo delle versioni sospeso.

Quando il controllo delle versioni è abilitato o sospeso, puoi definire regole di configurazione del ciclo di vita per contrassegnare alcune versioni degli oggetti come scadute o per rimuovere definitivamente quelle non necessarie. Per ulteriori informazioni, consulta Gestione del ciclo di vita degli oggetti.

Eliminazione MFA richiede un'autenticazione aggiuntiva quando lo stato del controllo delle versioni del bucket viene modificato o quando le versioni di un oggetto vengono eliminate. Richiede all'utente di inserire le credenziali e un codice da un dispositivo di autenticazione approvato. Per ulteriori informazioni, consulta Eliminazione MFA.

Risorse aggiuntive

Utilizzo dei bucket

Colonne del report

- Stato
- Regione
- Bucket Name (Nome bucket)
- Controllo delle versioni
- Eliminazione MFA abilitata

I sistemi di bilanciamento del carico (Application, Network e Gateway Load Balancer) non si estendono su più zone di disponibilità

Descrizione

Controlla se i tuoi sistemi di bilanciamento del carico (Application, Network e Gateway Load Balancer) sono configurati con sottoreti su più zone di disponibilità.

È possibile specificare le zone di disponibilità minime desiderate nei AvailabilityZones parametri minimi delle AWS Config regole.

Per ulteriori informazioni, consulta Zone di disponibilità per Application Load Balancer, Zone di disponibilità - Network Load Balancer e Crea un sistema di bilanciamento del carico del gateway.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz169`

Origine

`AWS Config Managed Rule: elbv2-multiple-az`

Criteri di avviso

Giallo: i sistemi di bilanciamento del carico (Application, Network e Gateway Load Balancer) sono configurati con sottoreti in meno di due zone di disponibilità.

Operazione consigliata

Configura i sistemi di bilanciamento del carico (Application, Network e Gateway Load Balancer) con sottoreti su più zone di disponibilità.

Risorse aggiuntive

Zone di disponibilità per Application Load Balancer

Zone di disponibilità (Elastic Load Balancing)

Crea un sistema di bilanciamento del carico del gateway

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input

- Ora ultimo aggiornamento

Dimensionamento automatico degli IP disponibili nelle sottoreti

Descrizione

Controlla che rimangano sufficienti IP disponibili tra le sottoreti di destinazione. Un numero sufficiente di IP disponibili all'uso potrebbe rivelarsi utile quando il gruppo con dimensionamento automatico raggiunge la dimensione massima e deve avviare istanze aggiuntive.

ID di controllo

`Cjxm268ch1`

Criteri di avviso

- Rosso: il numero massimo di istanze e indirizzi IP che possono essere creati da un ASG supera il numero di indirizzi IP rimanenti nelle sottoreti configurate.
- Verde: gli indirizzi IP disponibili sono sufficienti per il possibile dimensionamento residuo nell'ASG.

Operazione consigliata

Aumento del numero degli indirizzi IP disponibili

Colonne del report

- Stato
- Regione
- ARN risorsa
- Numero massimo di istanze che è possibile creare
- Numero di istanze disponibili

Controllo dell'integrità del gruppo Auto Scaling

Descrizione

Esamina la configurazione del controllo di integrità per i gruppi Auto Scaling.

Se per un gruppo di Auto Scaling viene utilizzato Elastic Load Balancing, si consiglia di configurare l'abilitazione di un controllo di integrità Elastic Load Balancing. Se non viene utilizzato

un controllo di integrità per il Elastic Load Balancing, l'Auto Scaling può agire solo in base allo stato dell'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'Auto Scaling non agirà sull'applicazione in esecuzione sull'istanza.

ID di controllo

`CL0G40CD08`

Criteri di avviso

- Giallo: un gruppo con scalabilità automatica ha un load balancer associato, ma il controllo dell'integrità di Elastic Load Balancing non è abilitato.
- Giallo: un gruppo con scalabilità automatica non ha un load balancer associato, ma il controllo dell'integrità di Elastic Load Balancing è abilitato.

Operazione consigliata

Se al gruppo con scalabilità automatica è associato un load balancer, ma il controllo dell'integrità di Elastic Load Balancing non è abilitato, consulta Aggiunta di un controllo dell'integrità di Elastic Load Balancing al gruppo con scalabilità automatica.

Se il controllo dell'integrità di Elastic Load Balancing è abilitato, ma nessun load balancer è associato al gruppo con scalabilità automatica, consulta Configurazione di un'applicazione di scalabilità automatica e bilanciamento del carico.

Risorse aggiuntive

Guida per l'utente di Dimensionamento automatico Amazon EC2

Colonne del report

- Stato
- Regione
- Nome del gruppo con scalabilità automatica
- Load balancer associato
- Controllo dello stato

Risorse dei gruppi Auto Scaling

Descrizione

Verifica la disponibilità delle risorse associate alle configurazioni di avvio e ai gruppi Auto Scaling.

I gruppi Auto Scaling che puntano a risorse non disponibili non possono avviare nuove istanze Amazon Elastic Compute Cloud (Amazon EC2). Se configurato correttamente, l'Auto Scaling fa sì che il numero di istanze Amazon EC2 aumenti senza problemi durante i picchi di domanda e diminuisca automaticamente durante i periodi di chiusura della domanda. I gruppi Auto Scaling e le configurazioni di avvio che puntano a risorse non disponibili non funzionano come previsto.

ID di controllo

`8CNsSllI5v`

Criteri di avviso

- Rosso: un gruppo con scalabilità automatica è associato a un load balancer eliminato.
- Rosso: una configurazione di avvio è associata a un'Amazon Machine Image (AMI) eliminata.

Operazione consigliata

Se il sistema di bilanciamento del carico è stato eliminato, crea un nuovo sistema di bilanciamento del carico o un gruppo di destinazione, quindi associalo al gruppo con dimensionamento automatico, oppure crea un nuovo gruppo con dimensionamento automatico senza un sistema di bilanciamento del carico. Per informazioni sulla creazione di un nuovo gruppo con scalabilità automatica con un nuovo load balancer, consulta Configurazione di un'applicazione di scalabilità automatica e bilanciamento del carico. Per informazioni sulla creazione di un nuovo gruppo con scalabilità automatica senza un load balancer, consulta Creazione di un gruppo con scalabilità automatica in Nozioni di base su Auto Scaling tramite la console.

Se l'AMI è stata eliminata, crea un nuovo modello di avvio o una versione di modello di avvio utilizzando un'AMI valida, quindi associala a un gruppo con dimensionamento automatico. Consulta Creazione di una configurazione di avvio in Nozioni di base su Auto Scaling tramite la console.

Risorse aggiuntive

- Risoluzione dei problemi di Auto Scaling: AMI Amazon EC2
- Risoluzione dei problemi di Auto Scaling: configurazione del load balancer
- Guida per l'utente di Dimensionamento automatico Amazon EC2

Colonne del report

- Stato
- Regione
- Nome del gruppo con scalabilità automatica

- Tipo di lancio
- Tipo di risorsa
- Nome risorsa

Cluster AWS CloudHSM che eseguono istanze HSM in una singola zona di disponibilità

Descrizione

Controlla i cluster che eseguono le istanze HSM in una singola zona di disponibilità (AZ). Questo controllo avvisa se i cluster rischiano di non avere il backup più recente.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`hc0dfs7601`

Criteri di avviso

- Giallo: un cluster CloudHSM esegue tutte le istanze HSM in un'unica zona di disponibilità per più di 1 ora.
- Verde: un cluster CloudHSM esegue tutte le istanze HSM in almeno due diverse zone di disponibilità.

Operazione consigliata

Crea almeno un'altra istanza per il cluster in una zona di disponibilità diversa.

Risorse aggiuntive

Le migliori pratiche per AWS CloudHSM

Colonne del report

- Stato

- Regione
- ID cluster
- Numero di istanze HSM
- Ora ultimo aggiornamento

AWS Direct Connect Resilienza della posizione

Descrizione

Verifica la resilienza dell'utente AWS Direct Connect per connettere l'ambiente locale a ciascun gateway Direct Connect o gateway privato virtuale.

Questo controllo ti avvisa se un gateway Direct Connect o un gateway privato virtuale non è configurato con interfacce virtuali in almeno due posizioni Direct Connect distinte. La mancanza di resilienza della posizione può causare tempi di inattività imprevisti durante la manutenzione, un taglio della fibra, un guasto del dispositivo o un guasto completo della posizione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate.

> **Note**
>
> Direct Connect è implementato con Transit Gateway utilizzando il gateway Direct Connect.

ID di controllo

`c1dfpnchv2`

Criteri di avviso

Rosso: il gateway Direct Connect o il gateway privato virtuale è configurato con una o più interfacce virtuali su un singolo dispositivo Direct Connect.

Giallo: il gateway Direct Connect o gateway privato virtuale è configurato con interfacce virtuali su più dispositivi Direct Connect in un'unica posizione Direct Connect.

Verde: il gateway Direct Connect o il gateway privato virtuale è configurato con interfacce virtuali su due o più sedi Direct Connect distinte.

Operazione consigliata

Per aumentare la resilienza della posizione Direct Connect, puoi configurare il gateway Direct Connect o il gateway privato virtuale per connetterti ad almeno due posizioni Direct Connect distinte. Per ulteriori informazioni, consulta Raccomandazione sulla AWS Direct Connect resilienza.

Risorse aggiuntive

AWS Direct Connect Raccomandazioni sulla resilienza

AWS Direct Connect Test di failover

Colonne del report

- Stato
- Regione
- Ora ultimo aggiornamento
- Stato di resilienza
- Ubicazione
- ID connessione
- ID Gateway

AWS Lambda funzioni senza una coda di lettere non scritte configurata

Descrizione

Verifica se una AWS Lambda funzione è configurata con una coda di lettere non scritte.

Una coda di lettere morte è una funzionalità AWS Lambda che consente di acquisire e analizzare gli eventi non riusciti, fornendo un modo per gestirli di conseguenza. Il codice potrebbe generare un'eccezione, un timeout o esaurire la memoria, con conseguenti esecuzioni asincrone non riuscite della funzione Lambda. Una coda DLQ archivia i messaggi delle invocazioni non riuscite, offrendo un modo per gestire i messaggi e risolvere gli errori.

Puoi specificare la risorsa della coda di lettere morte che desideri controllare utilizzando il parametro DLQArns nelle tue regole. AWS Config

Per ulteriori informazioni, consulta Code DLQ.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz182`

Origine

`AWS Config Managed Rule: lambda-dlq-check`

Criteri di avviso

Giallo: la AWS Lambda funzione non ha una coda di lettere non scritte configurata.

Operazione consigliata

Assicurati che AWS Lambda le tue funzioni abbiano una coda di lettere non scritte configurata per controllare la gestione dei messaggi per tutte le chiamate asincrone non riuscite.

Per ulteriori informazioni, consulta Code DLQ.

Risorse aggiuntive

- Potente progettazione di applicazioni serverless con code DLQ AWS Lambda

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Lambda Sulle destinazioni degli eventi di fallimento

Descrizione

Controlla se nelle funzioni Lambda del tuo account è configurata una destinazione degli eventi non riusciti o una DLQ (Dead Letter Queue) per le chiamate asincrone, in modo che i record delle chiamate non riuscite possano essere indirizzati a una destinazione per ulteriori indagini o elaborazioni.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch05`

Criteri di avviso

- Giallo: per la funzione non è configurata una destinazione degli eventi non riusciti o una DLQ.

Operazione consigliata

Configura la destinazione degli eventi non riusciti o una DLQ per le tue funzioni Lambda per inviare le chiamate non riuscite insieme ad altri dettagli a uno dei servizi AWS di destinazione disponibili per ulteriori operazioni di debug o elaborazione.

Risorse aggiuntive

- Chiamata asincrona
- AWS Lambda Sulle destinazioni degli eventi di errore

Colonne del report

- Stato
- Regione
- La funzione con la versione contrassegnata.
- Richieste asincrone del giorno corrente diminuite in percentuale
- Richieste asincrone del giorno corrente

- Media giornaliera delle richieste asincrone diminuita in percentuale
- Media giornaliera delle richieste asincrone
- Ora ultimo aggiornamento

Funzioni AWS Lambda abilitate per VPC senza ridondanza Multi-AZ

Descrizione

Controlla la versione $LATEST delle funzioni Lambda abilitate per VPC che sono vulnerabili all'interruzione del servizio in una singola zona di disponibilità. È buona norma che le funzioni abilitate per VPC siano collegate a più zone di disponibilità per un'elevata disponibilità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`L4dfs2Q4C6`

Criteri di avviso

Giallo: la versione $LATEST di una funzione Lambda abilitata per VPC è connessa alle sottoreti in una singola zona di disponibilità.

Operazione consigliata

Quando si configurano le funzioni per l'accesso al VPC, scegli le sottoreti in più zone di disponibilità in modo da garantire un'elevata disponibilità.

Risorse aggiuntive

- Configurazione di una funzione Lambda per accedere alle risorse in un VPC
- Resilienza in AWS Lambda

Colonne del report

- Stato

- Regione
- ARN della funzione
- ID VPC
- Media richiami giornalieri
- Ora ultimo aggiornamento

AWS Resilience Hub Controllo dei componenti dell'applicazione

Descrizione

Verifica se un componente dell'applicazione (AppComponent) nell'applicazione è irrecuperabile. Se un AppComponent non si ripristina in caso di interruzione, potrebbero verificarsi perdite di dati sconosciute e tempi di inattività del sistema.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate.

ID di controllo

`RH23stmM04`

Criteri di avviso

Rosso: non AppComponent è recuperabile.

Operazione consigliata

Per assicurarti che il tuo AppComponent sia recuperabile, esamina e implementa i consigli sulla resilienza, quindi esegui una nuova valutazione. Per ulteriori informazioni sulla revisione dei consigli sulla resilienza, consulta Risorse aggiuntive.

Risorse aggiuntive

Revisione delle raccomandazioni sulla resilienza

Concetti di AWS Resilience Hub

AWS Resilience Hub Guida per l'utente

Colonne del report

- Stato
- Regione
- Nome applicazione
- AppComponent Nome
- Ora ultimo aggiornamento

AWS Resilience Hub politica violata

Descrizione

Controlla Resilience Hub per applicazioni che non soddisfano l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) definiti dalla policy. Il controllo ti avvisa se l'applicazione non soddisfa gli obiettivi RTO e RPO che hai impostato per un'applicazione in Resilience Hub.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno; le richieste di aggiornamento non sono consentite. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`RH23stmM02`

Criteri di avviso

- Verde: l'applicazione ha una policy e soddisfa gli obiettivi RTO e RPO.
- Giallo: l'applicazione non è stata ancora valutata.
- Rosso: l'applicazione ha una policy ma non soddisfa gli obiettivi RTO e RPO.

Operazione consigliata

Accedi alla console Resilience Hub ed esamina i consigli in modo che l'applicazione soddisfi gli obiettivi RTO e RPO.

Risorse aggiuntive

Concetti di Resilience Hub

Colonne del report

- Stato
- Regione
- Nome applicazione
- Ora ultimo aggiornamento

AWS Resilience Hub punteggi di resilienza

Descrizione

Controlla se hai eseguito una valutazione per le applicazioni in Resilience Hub. Questo controllo avvisa se i punteggi di resilienza sono inferiori a un valore specifico.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno; le richieste di aggiornamento non sono consentite. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`RH23stmM01`

Criteri di avviso

- Verde: l'applicazione ha un punteggio di resilienza pari o superiore a 70.
- Giallo: l'applicazione ha un punteggio di resilienza compreso tra 40 e 69.
- Giallo: l'applicazione non è stata ancora valutata.
- Rosso: l'applicazione ha un punteggio di resilienza inferiore a 40.

Operazione consigliata

Accedi alla console Resilience Hub ed esegui una valutazione per l'applicazione. Esamina i suggerimenti per migliorare il punteggio di resilienza.

Risorse aggiuntive

Concetti di Resilience Hub

Colonne del report

- Stato
- Regione
- Nome applicazione
- Punteggio di resilienza dell'applicazione
- Ora ultimo aggiornamento

AWS Resilience Hub età di valutazione

Descrizione

Controlla il tempo trascorso dall'ultima esecuzione di una valutazione dell'applicazione. Questo controllo ti avvisa se per un certo numero di giorni non hai eseguito una valutazione dell'applicazione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`RH23stmM03`

Criteri di avviso

- Verde: la valutazione dell'applicazione è stata eseguita negli ultimi 30 giorni.
- Giallo: la valutazione dell'applicazione non è stata eseguita negli ultimi 30 giorni.

Operazione consigliata

Accedi alla console Resilience Hub ed esegui una valutazione per l'applicazione.

Risorse aggiuntive

Concetti di Resilience Hub

Colonne del report

- Stato
- Regione
- Nome applicazione
- Giorni trascorsi dall'ultima valutazione
- Ora di esecuzione dell'ultima valutazione
- Ora ultimo aggiornamento

AWS Site-to-Site VPN ha almeno un tunnel in stato DOWN

Descrizione

Controlla il numero di tunnel attivi per ciascuno dei tuoi AWS Site-to-Site VPN.

Una VPN dovrebbe avere due tunnel configurati in ogni momento. Ciò fornisce ridondanza in caso di interruzione o manutenzione pianificata dei dispositivi nell'endpoint AWS. Per alcuni hardware, è attivo un solo tunnel alla volta. Se una VPN non dispone di tunnel attivi, potrebbero essere comunque addebitati dei costi per la VPN.

Per ulteriori informazioni, consulta Che cos'è VPN da sito a sito AWS?

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

```
c18d2gz123
```

Origine

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

Criteri di avviso

Giallo: una VPN site-to-site include almeno un tunnel DOWN.

Operazione consigliata

Assicurati che siano configurati due tunnel per le connessioni VPN. Se l'hardware lo supporta, inoltre, assicurati che entrambi i tunnel siano attivi. Se una connessione VPN non occorre più, eliminala per evitare l'addebito di costi.

Per ulteriori informazioni, consulta Dispositivo gateway del cliente e i contenuti disponibili su AWS Knowledge Center.

Risorse aggiuntive

- AWS Site-to-Site VPN Guida per l'utente
- Aggiunta di un gateway privato virtuale a una VPC

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Well-ArchitectedProblemi ad alto rischio di per l'affidabilità

Descrizione

Verifica problemi ad alto rischio (HRI) per i carichi di lavoro nel pilastro dell'affidabilità. Questo controllo è basato sulle tue revisioni di AWS-Well Architected. I risultati dei controlli dipendono dal completamento della valutazione del carico di lavoro con AWS Well-Architected.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

Wxdfp4B1L4

Criteri di avviso

- Rosso: almeno un problema attivo ad alto rischio è stato identificato nel pilastro di affidabilità di AWS Well-Architected.
- Verde: non sono stati rilevati problemi attivi ad alto rischio nel pilastro di affidabilità di AWS Well-Architected.

Operazione consigliata

AWS Well-Architected ha rilevato problemi ad alto rischio durante la valutazione del carico di lavoro. Questi problemi offrono opportunità per ridurre i rischi e risparmiare denaro. Accedi allo strumento AWS Well-Architected per rivedere le tue risposte e risolvere i problemi attivi.

Colonne del report

- Stato
- Regione
- ARN del carico di lavoro
- Nome del carico di lavoro
- Nome del revisore
- Tipo di carico di lavoro
- Data di inizio del carico di lavoro
- Data dell'ultima modifica del carico di lavoro
- Numero di HRI identificati per Affidabilità
- Numero di HRI risolti per Affidabilità
- Numero di domande risposte per Affidabilità
- Numero totale di domande nel pilastro Affidabilità
- Ora ultimo aggiornamento

Per Classic Load Balancer non sono state configurate più AZ

Descrizione

Controlla se Classic Load Balancer si estende su più zone di disponibilità (AZ).

Un sistema di bilanciamento del carico distribuisce automaticamente il traffico delle applicazioni in ingresso su più istanze di Amazon EC2 in più zone di disponibilità. Per impostazione predefinita, il load balancer distribuisce il traffico in modo uniforme su tutte le zone di disponibilità abilitate per il tuo load balancer. Se in una zona di disponibilità si verifica un'interruzione, i nodi del sistema di bilanciamento del carico inoltrano automaticamente le richieste alle istanze integre registrate in una o più zone di disponibilità.

Puoi modificare il numero minimo di zone di disponibilità utilizzando il AvailabilityZones parametro min nelle tue regole AWS Config

Per ulteriori informazioni, consulta Cos'è Classic Load Balancer?.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz154`

Origine

`AWS Config Managed Rule: clb-multiple-az`

Criteri di avviso

Giallo: Classic Load Balancer non include una configurazione Multi-AZ o non soddisfa il numero minimo di AZ specificato.

Operazione consigliata

Assicurati che per i Classic Load Balancer siano configurate più zone di disponibilità. Estendi il tuo sistema di bilanciamento del carico su più AZ per garantire un'elevata disponibilità dell'applicazione.

Per ulteriori informazioni, consulta Tutorial: creazione di un Classic Load Balancer.

Colonne del report

- Stato

- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Svuotamento connessione ELB

Descrizione

Controlla i bilanciatori del carico per i quali non è abilitato lo svuotamento della connessione.

Quando lo svuotamento della connessione non è abilitato e si annulla la registrazione di un'istanza Amazon EC2 da un load balancer, il load balancer interrompe il routing del traffico verso tale istanza e chiude la connessione. Quando lo svuotamento della connessione è abilitato, il load balancer interrompe l'invio di nuove richieste all'istanza annullata della registrazione, ma mantiene aperta la connessione per servire le richieste attive.

ID di controllo

`7qGXsKIUw`

Criteri di avviso

Giallo: lo svuotamento della connessione non è abilitato per un load balancer.

Operazione consigliata

Lo svuotamento della connessione è abilitato per il load balancer. Per ulteriori informazioni, consulta Svuotamento della connessione e Abilitazione o disabilitazione dello svuotamento della connessione per il load balancer.

Risorse aggiuntive

Concetti dell'Elastic Load Balancing

Colonne del report

- Stato
- Regione
- Nome del load balancer

- Motivo

Ottimizzazione del load balancer

Descrizione

Verifica la configurazione del load balancer.

Per aumentare il livello di tolleranza ai guasti in Amazon Elastic Compute Cloud (Amazon EC2) quando si utilizza Elastic Load Balancing, si consiglia di eseguire un numero uguale di istanze in più zone di disponibilità in una regione. Un load balancer configurato accumula gli addebiti, quindi questo è anche un controllo di ottimizzazione dei costi.

ID di controllo

`iqdCTZKCUp`

Criteri di avviso

- Giallo: un load balancer è abilitato per un'unica zona di disponibilità.
- Giallo: un load balancer è abilitato per una zona di disponibilità che non ha istanze attive.
- Giallo: le istanze Amazon EC2 registrate con un load balancer sono distribuite in modo non uniforme tra le zone di disponibilità. (La differenza tra il numero di istanze più alto e più basso nelle zone di disponibilità utilizzate è maggiore di 1 e la differenza è superiore del 20% del conteggio più alto.)

Operazione consigliata

Verifica che il load balancer punti a istanze attive e integre in almeno due zone di disponibilità. Per ulteriori informazioni, consulta Aggiunta di una zona di disponibilità.

Se il load balancer è configurato per una zona di disponibilità senza istanze integre o se vi è uno squilibrio di istanze tra le zone di disponibilità, determina se tutte le zone di disponibilità sono necessarie. Ometti eventuali zone di disponibilità non necessarie e assicurati che le istanze siano distribuite in modo equilibrato tra le restanti zone di disponibilità. Per ulteriori informazioni, consulta Rimozione delle zone di disponibilità.

Risorse aggiuntive

- Regioni e zone di disponibilità
- Gestione dei load balancer

- Best practice per la valutazione dell'Elastic Load Balancing

Colonne del report

- Stato
- Regione
- Nome del load balancer
- Numero di zone
- Istanze della zona a
- Istanze della zona b
- Istanze della zona c
- Istanze della zona d
- Istanze della zona e
- Istanze della zona f
- Motivo

Indipendenza dell’AZ disponibilità dal Gateway NAT

Descrizione

Controlla se i gateway NAT sono configurati in modo da soddisfare l'indipendenza della zona di disponibilità (AZ).

Un gateway NAT consente alle risorse della sottorete privata di connettersi in modo sicuro ai servizi esterni alla sottorete utilizzando gli indirizzi IP del gateway NAT ed elimina traffico in entrata non richiesto. Ogni gateway NAT opera all'interno di una zona di disponibilità (AZ) designata ed è costruito con ridondanza solo in tale AZ. Pertanto, le risorse in una determinata AZ devono utilizzare un gateway NAT nella stessa AZ in modo che un’eventuale interruzione di un gateway NAT o della relativa AZ non interessi le risorse in un'altra AZ.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfptbg10`

Criteri di avviso

- Rosso: il traffico proveniente dalla sottorete di una singola AZ viene indirizzato attraverso un NATGW in un'AZ diversa.
- Verde: il traffico proveniente dalla sottorete di una singola AZ viene indirizzato attraverso un NATGW nella stessa AZ.

Operazione consigliata

Controlla l'AZ della tua sottorete e indirizza il traffico attraverso un gateway NAT nella stessa AZ.

Se l'AZ non include alcun NATGW, creane uno e indirizza il traffico della sottorete attraverso tale gateway.

Se la stessa tabella di routing è associata a sottoreti in diverse AZ, mantieni questa tabella di routing associata alle sottoreti residenti nella stessa AZ del gateway NAT; per le sottoreti nell'altra AZ, associa una tabella di routing separata a un instradamento a un gateway NAT di quest'altra AZ.

È preferibile scegliere una finestra di manutenzione per le modifiche all'architettura nella VPC Amazon.

Risorse aggiuntive

- Come creare un gateway NAT
- Come configurare gli instradamenti per diversi casi d'uso del gateway NAT

Colonne del report

- Stato
- Regione
- Zona di disponibilità NAT
- ID del NAT
- Zona di disponibilità della sottorete
- ID sottorete
- ID della tabella di routing
- ARN del NAT

- Ora ultimo aggiornamento

Bilanciamento del carico tra zone di Network Load Balancer

Descrizione

Controlla se per i Network Load Balancer è abilitato il bilanciamento del carico tra zone.

Il bilanciamento del carico tra zone contribuisce a mantenere una distribuzione uniforme del traffico in entrata tra le istanze in diverse zone di disponibilità. Ciò impedisce al sistema di bilanciamento del carico di indirizzare tutto il traffico verso istanze presenti nella stessa zona di disponibilità, evitando il rischio di una distribuzione irregolare del traffico e di un potenziale sovraccarico. La funzionalità migliora anche l'affidabilità delle applicazioni, in quanto, in caso di errore di una singola zona di disponibilità, il traffico viene instradato in istanze integre di altre zone di disponibilità.

Per ulteriori informazioni, consulta Bilanciamento del carico tra zone.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz105`

Origine

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

Criteri di avviso

- Giallo: per Network Load Balancer non è abilitato il bilanciamento del carico tra zone.

Operazione consigliata

Assicurati che per i Network Load Balancer sia abilitato il bilanciamento del carico tra zone.

Risorse aggiuntive

Bilanciamento del carico tra zone (Network Load Balancer)

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

NLB: risorsa rivolta a Internet in sottorete privata

Descrizione

Verifica se un Network Load Balancer (NLB) con accesso a Internet è configurato con una sottorete privata. Un Network Load Balancer (NLB) con accesso a Internet deve essere configurato in sottoreti pubbliche per ricevere traffico. Una sottorete pubblica è definita come una sottorete che ha un percorso diretto verso un gateway Internet. Se la sottorete è configurata come privata, la zona di disponibilità (AZ) non riceve traffico, il che può causare problemi di disponibilità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfpnchv4`

Criteri di avviso

Rosso: NLB è configurato con una o più sottoreti private

Verde: nessuna sottorete privata è configurata per NLB con accesso a Internet

Operazione consigliata

Verifica che le sottoreti configurate in un sistema di bilanciamento del carico connesso a Internet siano pubbliche. Una sottorete pubblica è definita come una sottorete che ha un percorso diretto verso un gateway Internet. Utilizzate una delle seguenti opzioni:

- Crea un nuovo sistema di bilanciamento del carico e seleziona una sottorete diversa con un percorso diretto verso un gateway Internet.
- Cambia la sottorete attualmente collegata al load balancer da privata a pubblica. Per fare ciò, modifica la sua tabella di routing e associa un gateway Internet.

Risorse aggiuntive

- Configura un sistema di bilanciamento del carico e un listener
- Sottoreti per il tuo VPC
- Associa un gateway a una tabella di routing

Colonne del report

- Stato
- Regione
- NLB Arn
- Nome NLB
- ID sottorete
- Schema NLB
- Tipo di sottorete
- Ora ultimo aggiornamento

NLB Multi-AZ

Descrizione

Verifica se i Network Load Balancer sono configurati per utilizzare più di una zona di disponibilità (AZ). Un'AZ è una posizione distinta che è isolata da errori presenti in altre zone. Configura il tuo load balancer in più AZ nella stessa regione per migliorare la disponibilità del carico di lavoro.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch09`

Criteri di avviso

Giallo: NLB si trova in un'unica AZ.

Verde: NLB ha due o più AZ.

Operazione consigliata

Assicurati che il tuo sistema di bilanciamento del carico sia configurato con almeno due zone di disponibilità.

Risorse aggiuntive

Per ulteriori informazioni, consulta la seguente documentazione :

- Zone di disponibilità
- AWS Well-Architected: distribuisci il carico di lavoro in più sedi
- Regioni e zone di disponibilità

Colonne del report

- Stato
- Regione
- Numero di AZ
- NLB ARN
- Nome NLB
- Ora ultimo aggiornamento

Numero di componenti Regioni AWS in un set di repliche di Incident Manager

Descrizione

Verifica che la configurazione di un set di repliche di Incident Manager ne utilizzi più di uno Regione AWS per supportare il failover e la risposta regionali. Per gli incidenti creati da CloudWatch allarmi o EventBridge eventi, Incident Manager crea un incidente uguale Regione

AWS alla regola di allarme o evento. Se Incident Manager non è temporaneamente disponibile in tale regione, il sistema tenta di creare un incidente in un'altra regione nel set di repliche. Se il set di repliche include solo una regione, qualora Incident Manager non fosse disponibile, il sistema non è in grado di creare un record di incidente.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`cIdfp1js9r`

Criteri di avviso

- Verde: il set di repliche contiene più di una regione.
- Giallo: il set di repliche contiene una sola regione.

Operazione consigliata

Aggiungi almeno un'altra regione al set di repliche.

Risorse aggiuntive

Per ulteriori informazioni, consulta Gestione degli incidenti in più regioni.

Colonne del report

- Stato
- Multi-regione
- Set di repliche
- Ora ultimo aggiornamento

Controllo dell'applicazione in una singola AZ

Descrizione

Controlla, tramite i modelli di rete, se il traffico di rete in uscita viene indirizzato attraverso un'unica zona di disponibilità (AZ).

Un'AZ è una posizione distinta che isolata da eventuali impatti in altre zone. La distribuzione del servizio su più AZ limita il raggio di azione di un errore di un'AZ.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfptbg11`

Criteri di avviso

- Giallo: l'applicazione può essere implementata in una singola AZ in base ai modelli di rete in uscita osservati. In tal caso e se l'applicazione prevede un'elevata disponibilità, è preferibile fornire risorse all'applicazione e implementare i flussi di rete per utilizzare più zone di disponibilità.

Operazione consigliata

Se l'applicazione richiede un'elevata disponibilità, valuta l'opportunità di implementare un'architettura Multi-AZ per una maggiore disponibilità.

Colonne del report

- Stato
- Regione
- ID VPC
- Ora ultimo aggiornamento

Interfaccia VPC: interfacce di rete endpoint in più AZ

Descrizione

Verifica se gli endpoint dell'interfaccia AWS PrivateLink VPC sono configurati per utilizzare più di una zona di disponibilità (AZ). Un'AZ è una posizione distinta che è isolata da errori presenti in altre zone. Ciò supporta una connettività di rete economica e a bassa latenza tra AZ nella

stessa regione. AWS Seleziona le sottoreti in più AZ quando crei gli endpoint di interfaccia per proteggere le tue applicazioni da un singolo punto di errore.

> **Note**
>
> Attualmente questo controllo include solo gli endpoint di interfaccia.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch10`

Criteri di avviso

Giallo: l'endpoint VPC si trova in un'unica AZ.

Verde: l'endpoint VPC si trova in almeno due AZ.

Operazione consigliata

Assicurati che l'endpoint dell'interfaccia VPC sia configurato con almeno due zone di disponibilità.

Risorse aggiuntive

Per ulteriori informazioni, consulta la seguente documentazione :

- Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia
- Indirizzo IP privato dell'interfaccia di rete dell'endpoint
- AWS PrivateLink concetti
- Regioni e zone di disponibilità

Colonne del report

- Stato

- Regione
- ID endpoint VPC
- È Multi AZ
- Ora ultimo aggiornamento

Ridondanza del Tunnel VPN

Descrizione

Controlla il numero di tunnel attivi per ciascuna VPN.

Una VPN dovrebbe avere due tunnel configurati in ogni momento. Ciò fornisce ridondanza in caso di interruzione o manutenzione pianificata dei dispositivi presso l'endpoint AWS . Per alcuni hardware, è attivo un solo tunnel alla volta. Se una VPN non dispone di tunnel attivi, potrebbero essere comunque addebitati dei costi per la VPN. Per ulteriori informazioni, consulta la Guida per amministratori di AWS Client VPN.

ID di controllo

`S45wrEXrLz`

Criteri di avviso

- Giallo: una VPN ha un tunnel attivo (normale per alcuni hardware).
- Giallo: una VPN non ha tunnel attivi.

Operazione consigliata

Assicurati che due tunnel siano configurati per la connessione VPN e che entrambi siano attivi se il tuo hardware la supporta. Se non hai più bisogno di una connessione VPN, puoi eliminarla per evitare costi. Per ulteriori informazioni, consulta Gateway del cliente o Eliminazione di una connessione VPN.

Risorse aggiuntive

- AWS Guida per l'utente della VPN da sito a sito
- Aggiunta di un gateway privato virtuale hardware al proprio VPC

Colonne del report

- Stato
- Regione
- ID VPN

- VPC
- Gateway virtuale privato
- Gateway del cliente
- Tunnel attivi
- Motivo

Ridondanza della zona di disponibilità ActiveMQ

Descrizione

Controlla se i broker di Amazon MQ per ActiveMQ sono configurati per una disponibilità elevata con un broker attivo/in standby in più zone di disponibilità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1t3k8mqv1`

Criteri di avviso

- Giallo: un broker di Amazon MQ per ActiveMQ è configurato in un'unica zona di disponibilità.

  Verde: un broker di Amazon MQ per ActiveMQ è configurato in almeno due zone di disponibilità.

Operazione consigliata

Crea un nuovo broker con modalità di implementazione attiva/in standby.

Risorse aggiuntive

- Creazione di un broker ActiveMQ

Colonne del report

- Stato

- Regione
- ID del broker ActiveMQ
- Tipo di motore del broker
- Modalità di implementazione
- Ora ultimo aggiornamento

Ridondanza della zona di disponibilità RabbitMQ

Descrizione

Controlla se i broker di Amazon MQ per RabbitMQ sono configurati per una disponibilità elevata con istanze di cluster in più zone di disponibilità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1t3k8mqv2`

Criteri di avviso

- Giallo: un broker di Amazon MQ per RabbitMQ è configurato in un'unica zona di disponibilità.

  Verde: un broker di Amazon MQ per RabbitMQ è configurato in più zone di disponibilità.

Operazione consigliata

Crea un nuovo broker con la modalità di implementazione del cluster.

Risorse aggiuntive

- Creazione di un broker RabbitMQ

Colonne del report

- Stato

- Regione
- ID del broker RabbitMQ
- Tipo di motore del broker
- Modalità di implementazione
- Ora ultimo aggiornamento

Limiti del servizio

Consulta i seguenti controlli per la categoria dei limiti di servizio (noti anche come quote).

Tutti i controlli in questa categoria hanno le seguenti descrizioni:

Criteri di avviso

- Giallo: 80% del limite raggiunto.
- Rosso: 100% del limite raggiunto.
- Blu: Trusted Advisor non è stato in grado di recuperare l'utilizzo o i limiti in uno o più Regioni AWS.

Operazione consigliata

Se prevedi di superare un limite di servizio, richiedi un aumento direttamente alla console Service Quotas. Se Service Quotas non supporta ancora il tuo servizio, puoi creare un caso di supporto aperto in Centro assistenza.

Colonne del report

- Stato
- Servizio
- Region
- Limita importo
- Utilizzo attuale

> **Note**
>
> - I valori sono basati su uno snapshot, quindi l'utilizzo corrente potrebbe differire. La visualizzazione di eventuali modifiche sui dati relativi a quota e utilizzo può richiedere fino a

24 ore. Nei casi in cui le quote siano state recentemente aumentate, è possibile che venga temporaneamente visualizzato un utilizzo superiore alla quota.

Controlla i nomi

- Gruppi Auto Scaling
- Configurazioni di avvio per Auto Scaling
- CloudFormation Pile
- Capacità di lettura DynamoDB
- Capacità di scrittura DynamoDB
- Snapshot attivi EBS
- Archiviazione del Volume EBS Cold HDD (sc1)
- Archiviazione per volumi SSD (gp2) a scopo generico EBS
- Archiviazione per volumi SSD a scopo generico (gp3) EBS
- Archiviazione di volumi magnetici (standard) EBS
- IOPS aggregati dei volumi (SSD) IOPS con provisioning EBS
- Archiviazione per volumi SSD (io1) IOPS con provisioning EBS
- Archiviazione per volumi SSD IOPS con provisioning (io2) EBS
- Archiviazione volumi di velocità effettiva ottimizzati HDD (st1) EBS
- Istanze On Demand EC2
- Locazioni di istanze riservate EC2
- Indirizzi IP elastici EC2-Classic
- Indirizzo IP elastico EC2-VPC
- Application Load Balancer ELB
- Classic Load Balancer ELB
- Bilanciatori del carico di rete ELB
- Gruppo IAM
- Profili dell'istanza IAM
- Policy IAM
- Ruoli IAM
- Certificati del Server IAM

- Utenti IAM
- Partizioni Kinesis per regione
- Utilizzo dell'archiviazione di codice Lambda
- Gruppi di parametri del Cluster RDS
- Ruoli Cluster RDS
- Cluster RDS
- Istanze database RDS
- Snapshot manuali database RDS
- Gruppi parametri del database RDS
- Gruppi di sicurezza DB RDS
- Abbonamenti a eventi RDS
- Autorizzazioni massime RDS per ciascun gruppo di sicurezza
- Gruppi di opzioni RDS
- Repliche di lettura RDS per Master
- Istanze riservate RDS
- Gruppi di sottoreti RDS
- Sottoreti RDS per gruppo di sottoreti
- Quota di archiviazione totale RDS
- Zone ospitate Route 53
- Controllo di integrità massima Route 53
- Set di deleghe riutilizzabili Route 53
- Policy di traffico Route 53
- Istanze della Policy di traffico Route 53
- Quota di invio giornaliera SES
- VPC
- Gateway Internet VPC

Gruppi Auto Scaling

Description

Controlla l'utilizzo superiore all'80% della quota dei gruppi Auto Scaling.

ID di controllo

`fW7HH0l7J9`

Risorse aggiuntive

Quote dei gruppi con scalabilità automatica

Configurazioni di avvio per Auto Scaling

Description

Verifica l'utilizzo che corrisponde a oltre l'80% della quota delle configurazioni di avvio dell'Auto Scaling.

ID di controllo

`aW7HH0l7J9`

Risorse aggiuntive

Quote dei gruppi con scalabilità automatica

CloudFormation Pile

Description

Verifica che l'utilizzo superi l'80% della quota degli CloudFormation stack.

ID di controllo

`gW7HH0l7J9`

Risorse aggiuntive

Quote di AWS CloudFormation

Capacità di lettura DynamoDB

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% del limite di velocità effettiva assegnata di DynamoDB per le letture di ogni Account AWS.

ID di controllo

`6gtQddfEw6`

Risorse aggiuntive

Quote di DynamoDB

Capacità di scrittura DynamoDB

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% del limite di velocità effettiva assegnata di DynamoDB per le scritture di ogni Account AWS.

ID di controllo

`c5ftjdfkMr`

Risorse aggiuntive

Quote di DynamoDB

Snapshot attivi EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di snapshot attivi EBS.

ID di controllo

`eI7KK0l7J9`

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione del Volume EBS Cold HDD (sc1)

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione del volume EBS Cold HDD (sc1).

ID di controllo

gH5CC0e3J9

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione per volumi SSD (gp2) a scopo generico EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione del volume SSD (gp2) a scopo generico EBS.

ID di controllo

dH7RR0l6J9

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione per volumi SSD a scopo generico (gp3) EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di storage del volume SSD (gp3) a scopo generico EBS.

ID di controllo

dH7RR0l6J3

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione di volumi magnetici (standard) EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione del volume magnetico (standard) EBS.

ID di controllo

`cG7HH0l7J9`

Risorse aggiuntive

Limiti di Amazon EBS

IOPS aggregati dei volumi (SSD) IOPS con provisioning EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota IOPS aggregata del volume (SSD) IOPS con provisioning EBS.

ID di controllo

`tV7YY0l7J9`

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione per volumi SSD (io1) IOPS con provisioning EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione del volume SSD (io1) IOPS con provisioning EBS.

ID di controllo

`gI7MM0l7J9`

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione per volumi SSD IOPS con provisioning (io2) EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione del volume SSD (io2) IOPS con provisioning EBS.

ID di controllo

`gI7MM0l7J2`

Risorse aggiuntive

Limiti di Amazon EBS

Archiviazione volumi di velocità effettiva ottimizzati HDD (st1) EBS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione del volume ottimizzato HDD (st1) di velocità effettiva EBS.

ID di controllo

`wH7DD0l3J9`

Risorse aggiuntive

Limiti di Amazon EBS

Istanze On Demand EC2

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle Istanze On Demand EC2.

ID di controllo

`0Xc6LMYG8P`

Risorse aggiuntive

Quote di Amazon EC2

Locazioni di istanze riservate EC2

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota per le locazioni di istanze riservate EC2.

ID di controllo

`iH7PP0l7J9`

Risorse aggiuntive

Quote di Amazon EC2

Indirizzi IP elastici EC2-Classic

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota degli indirizzi IP elastici EC2-Classic.

ID di controllo

`aW9HH0l8J6`

Risorse aggiuntive

Quote di Amazon EC2

Indirizzo IP elastico EC2-VPC

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di indirizzo IP elastico EC2-VPC.

ID di controllo

`lN7RR0l7J9`

Risorse aggiuntive

Quote degli IP elastici VPC

Application Load Balancer ELB

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota Application Load Balancers ELB.

ID di controllo

`EM8b3yLRTr`

Risorse aggiuntive

Quote di Elastic Load Balancing

Classic Load Balancer ELB

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota Classic Load Balancer ELB.

ID di controllo

`iK70001J9`

Risorse aggiuntive

Quote di Elastic Load Balancing

Bilanciatori del carico di rete ELB

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di bilanciatori del traffico di rete ELB.

ID di controllo

`8wIqYSt25K`

Risorse aggiuntive

Quote di Elastic Load Balancing

Gruppo IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota del gruppo IAM.

ID di controllo

sU7XX0l7J9

Risorse aggiuntive

Quote di IAM

Profili dell'istanza IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei profili di istanza IAM.

ID di controllo

n07SS0l7J9

Risorse aggiuntive

Quote di IAM

Policy IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle policy IAM.

ID di controllo

pR7UU0l7J9

Risorse aggiuntive

Quote di IAM

Ruoli IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei ruoli IAM.

ID di controllo

oQ7TT0l7J9

Risorse aggiuntive

Quote di IAM

Certificati del Server IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei certificati del server IAM.

ID di controllo

`rT7WW0l7J9`

Risorse aggiuntive

Quote di IAM

Utenti IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota degli utenti IAM.

ID di controllo

`qS7VV0l7J9`

Risorse aggiuntive

Quote di IAM

Partizioni Kinesis per regione

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di partizioni Kinesis per regione.

ID di controllo

`bW7HH0l7J9`

Risorse aggiuntive

Quote di Kinesis

Utilizzo dell’archiviazione di codice Lambda

Description

Controlla eventuali occorrenze di utilizzo dell’archiviazione di codice superiori all'80% rispetto al limite dell'account.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c1dfprch07`

Criteri di avviso

- Giallo: 80% del limite raggiunto.

Operazione consigliata

Individua le funzioni o le versioni lambda inutilizzate e rimuovile per liberare lo spazio di archiviazione del codice per il tuo account nella regione. Se hai bisogno di spazio di archiviazione aggiuntivo, crea un caso di supporto nel Centro assistenza. Se prevedi di superare un limite di servizio, richiedi un aumento direttamente alla console Service Quotas. Se Service Quotas non supporta ancora il tuo servizio, puoi creare un caso di supporto aperto in Centro assistenza.

Risorse aggiuntive

- Utilizzo dell’archiviazione di codice Lambda

Colonne del report

- Stato
- Region
- L'ARN della funzione qualificata per tale risorsa.

- L'utilizzo della memorizzazione del codice della funzione MegaBytes con 2 decimali.
- La quantità delle versioni nella funzione
- Ora ultimo aggiornamento

Gruppi di parametri del Cluster RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei gruppi di parametri del cluster RDS.

ID di controllo

`jtlIMO3qZM`

Risorse aggiuntive

Quote di Amazon RDS

Ruoli Cluster RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di ruoli cluster RDS.

ID di controllo

`7fuccf1Mx7`

Risorse aggiuntive

Quote di Amazon RDS

Cluster RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota cluster RDS.

ID di controllo

`gjqMBn6pjz`

Risorse aggiuntive

Quote di Amazon RDS

Istanze database RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle istanze database RDS.

ID di controllo

`XG0aXHpIEt`

Risorse aggiuntive

Quote di Amazon RDS

Snapshot manuali database RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di snapshot manuali database RDS.

ID di controllo

`dV84wpqRUs`

Risorse aggiuntive

Quote di Amazon RDS

Gruppi parametri del database RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di gruppi parametri del database RDS.

ID di controllo

`jEECYg2YVU`

Risorse aggiuntive

Quote di Amazon RDS

Gruppi di sicurezza DB RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei gruppi di sicurezza DB RDS.

ID di controllo

`gfZAn3W7wl`

Risorse aggiuntive

Quote di Amazon RDS

Abbonamenti a eventi RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di abbonamenti a eventi RDS.

ID di controllo

`keAhfbH5yb`

Risorse aggiuntive

Quote di Amazon RDS

Autorizzazioni massime RDS per ciascun gruppo di sicurezza

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle autorizzazioni massime RDS per ciascun gruppo di sicurezza.

ID di controllo

`dBkuNCvqn5`

Risorse aggiuntive

Quote di Amazon RDS

Gruppi di opzioni RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei gruppi di opzioni RDS.

ID di controllo

`3Njm0DJQO9`

Risorse aggiuntive

Quote di Amazon RDS

Repliche di lettura RDS per Master

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle repliche di lettura RDS per master.

ID di controllo

`pYW8UkYz2w`

Risorse aggiuntive

Quote di Amazon RDS

Istanze riservate RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota istanze riservate RDS.

ID di controllo

`UUDv0a5r34`

Risorse aggiuntive

Quote di Amazon RDS

Gruppi di sottoreti RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di gruppi di sottoreti RDS.

ID di controllo

`dYWBaXaaMM`

Risorse aggiuntive

Quote di Amazon RDS

Sottoreti RDS per gruppo di sottoreti

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle sottoreti RDS per gruppo di sottoreti.

ID di controllo

`jEhCtdJK0Y`

Risorse aggiuntive

Quote di Amazon RDS

Quota di archiviazione totale RDS

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di archiviazione totale RDS.

ID di controllo

`P1jhKWEmLa`

Risorse aggiuntive

Quote di Amazon RDS

Zone ospitate Route 53

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di zone ospitate Route 53 per account.

ID di controllo

`dx3xfcdfMr`

Risorse aggiuntive

Quote di Route 53

Controllo di integrità massima Route 53

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei controlli di integrità Route 53 per account.

ID di controllo

`ru4xfcdfMr`

Risorse aggiuntive

Quote di Route 53

Set di deleghe riutilizzabili Route 53

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei set di deleghe Route 53 riutilizzabili per account.

ID di controllo

`ty3xfcdfMr`

Risorse aggiuntive

Quote di Route 53

Policy di traffico Route 53

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle policy di traffico Route 53 per account.

ID di controllo

`dx3xfbjfMr`

Risorse aggiuntive

Quote di Route 53

Istanze della Policy di traffico Route 53

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle istanze delle policy di traffico Route 53 per account.

ID di controllo

`dx8afcdfMr`

Risorse aggiuntive

Quote di Route 53

Quota di invio giornaliera SES

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota di invio giornaliera di Amazon SES.

ID di controllo

`hJ7NN0l7J9`

Risorse aggiuntive

Quote di Amazon SES

VPC

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota VPC.

ID di controllo

`jL7PP0l7J9`

Risorse aggiuntive

Quote VPC

Gateway Internet VPC

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei gateway Internet VPC.

ID di controllo

`kM7QQ0l7J9`

Risorse aggiuntive

Quote VPC

Eccellenza operativa

Per la categoria dell'eccellenza operativa, puoi utilizzare i controlli indicati di seguito.

Controlla i nomi

- Il Gateway Amazon API non registra log di esecuzione
- REST API di Gateway Amazon API senza tracciamento X-Ray abilitato
- Amazon CloudFront Access Log configurato

- L'azione CloudWatch di Amazon Alarm è disabilitata
- Istanza Amazon EC2 non gestita da AWS Systems Manager
- Repository di Amazon ECR con immutabilità dei tag disabilitata
- Cluster di Amazon ECS con approfondimenti sui container disabilitati
- La registrazione dei log delle attività di Amazon ECS non è abilitata
- Registrazione OpenSearch del servizio Amazon CloudWatch non configurata
- Istanze database Amazon RDS nei cluster con gruppi di parametri eterogenei
- Amazon RDS Enhanced Monitoring è disattivato
- Amazon RDS Performance Insights è disattivato
- Il parametro Amazon RDS track_counts è disattivato
- Registrazione dei log di controllo del cluster di Amazon Redshift
- Per Amazon S3 non sono abilitate le Notifiche di eventi
- Gli argomenti di Amazon SNS non registrano i log dello stato di consegna dei messaggi
- Amazon VPC senza log di flusso
- Application Load Balancer e Classic Load Balancer senza log di accesso abilitati
- AWS CloudFormation Notifica Stack
- AWS CloudTrail registrazione degli eventi relativi ai dati per gli oggetti in un bucket S3
- AWS CodeBuild Registrazione del progetto
- AWS CodeDeploy Rollback e monitoraggio automatici abilitati
- AWS CodeDeploy Lambda utilizza all-at-once la configurazione di distribuzione
- AWS Elastic Beanstalk Enhanced Health Reporting non è configurato
- AWS Elastic Beanstalk con gli aggiornamenti gestiti della piattaforma disattivati
- AWS Fargate la versione della piattaforma non è la più recente
- AWS Systems Manager State Manager Association in stato di non conformità
- CloudTrail i trail non sono configurati con Amazon CloudWatch Logs
- Protezione dall’eliminazione Elastic Load Balancing non abilitata per i sistemi di bilanciamento del carico
- Controllo della protezione dall’eliminazione del cluster DB di RDS
- Controllo automatico dell'aggiornamento delle versioni secondarie di istanze DB di RDS

Il Gateway Amazon API non registra log di esecuzione

Descrizione

Verifica se Amazon API Gateway ha attivato CloudWatch i log al livello di registrazione desiderato.

Attiva CloudWatch la registrazione per i metodi o i percorsi API REST in Amazon WebSocket API Gateway per raccogliere i log di esecuzione in CloudWatch Logs per le richieste ricevute dalle tue API. Le informazioni contenute nei log di esecuzione facilitano l'identificazione e la soluzione di problemi relativi all'API.

È possibile specificare l'ID del livello di registrazione (ERROR, INFO) nel parametro LoggingLevel nelle regole. AWS Config

Per ulteriori informazioni sulla CloudWatch registrazione in Amazon API Gateway, consulta l' WebSocket API REST o la documentazione dell'API.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz125`

Origine

`AWS Config Managed Rule: api-gw-execution-logging-enabled`

Criteri di avviso

Giallo: l'impostazione CloudWatch di registrazione per la raccolta dei log di esecuzione non è abilitata al livello di registrazione desiderato per un Amazon API Gateway.

Operazione consigliata

Attiva CloudWatch la registrazione per i log di esecuzione per le API o le API REST di Amazon API Gateway con il livello di registrazione appropriato (ERROR, INFOWebSocket).

Per ulteriori informazioni, consulta Creazione un log di flusso

Risorse aggiuntive

- Configurazione della CloudWatch registrazione per un'API REST in API Gateway
- Configurazione della registrazione per un'API WebSocket

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

REST API di Gateway Amazon API senza tracciamento X-Ray abilitato

Descrizione

Verifica se le API REST di Amazon API Gateway hanno il AWS X-Ray tracciamento attivato.

Attiva il tracciamento X-Ray per le REST API per consentire al Gateway API di campionare le richieste di invocazione dell'API con informazioni di traccia. In questo modo puoi trarre vantaggio dalla possibilità di AWS X-Ray tracciare e analizzare le richieste mentre viaggiano attraverso le API REST del tuo API Gateway verso i servizi downstream.

Per ulteriori informazioni, consulta Tracciamento delle richieste degli utenti alle REST API utilizzando X-Ray.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz126`

Origine

```
AWS Config Managed Rule: api-gw-xray-enabled
```

Criteri di avviso

Giallo: il tracciamento X-Ray non è attivato per la REST API del Gateway API.

Operazione consigliata

Attiva il tracciamento X-Ray per le REST API del Gateway API.

Per ulteriori informazioni, consulta Configurazione AWS X-Ray con le API REST di API Gateway.

Risorse aggiuntive

- Tracciamento delle richieste degli utenti alle REST API utilizzando X-Ray
- Che cos'è AWS X-Ray?

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Amazon CloudFront Access Log configurato

Descrizione

Verifica se CloudFront le distribuzioni Amazon sono configurate per acquisire informazioni dai log di accesso ai server Amazon S3. I log di accesso al server Amazon S3 contengono informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront

Puoi modificare il nome del bucket Amazon S3 per l'archiviazione dei log di accesso al server, utilizzando il parametro S3 BucketName nelle tue regole. AWS Config

Per ulteriori informazioni, consulta Configurazione e utilizzo dei log standard (log di accesso).

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz110`

Origine

`AWS Config Managed Rule: cloudfront-accesslogs-enabled`

Criteri di avviso

Giallo: la registrazione CloudFront degli accessi di Amazon non è abilitata

Operazione consigliata

Assicurati di attivare la registrazione degli CloudFront accessi per acquisire informazioni dettagliate su ogni richiesta utente che CloudFront riceve.

Puoi attivare i log standard quando crei o aggiorni una distribuzione.

Per ulteriori informazioni, consulta Valori da specificare durante la creazione o l'aggiornamento di una distribuzione.

Risorse aggiuntive

- Valori da specificare durante la creazione o l'aggiornamento di una distribuzione
- Configurazione e utilizzo di log standard (log di accesso)

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

L'azione CloudWatch di Amazon Alarm è disabilitata

Descrizione

Verifica se l'azione di CloudWatch allarme di Amazon è disattivata.

Puoi utilizzare il AWS CLI per abilitare o disabilitare la funzione di azione nel tuo allarme. In alternativa, puoi disabilitare o abilitare in modo programmatico la funzione di azione utilizzando l' AWS SDK. Quando la funzione di azione di allarme è disattivata, CloudWatch non esegue alcuna azione definita in nessuno stato (OK, INSUFFICIENT_DATA, ALARM).

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz109`

Origine

`AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check`

Criteri di avviso

Giallo: l'azione di CloudWatch allarme di Amazon non è abilitata. Nessuna operazione viene eseguita in alcuno stato di allarme.

Operazione consigliata

Abilita le azioni nei tuoi CloudWatch allarmi a meno che tu non abbia un motivo valido per disabilitarle, ad esempio a scopo di test.

Se l' CloudWatch allarme non è più necessario, eliminalo per evitare di incorrere in costi inutili.

Per ulteriori informazioni, consulta enable-alarm-actions nel AWS CLI Command Reference e func (*) nel riferimento all'API CloudWatch SDK EnableAlarmActions for Go. AWS

Colonne del report

- Stato

- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Istanza Amazon EC2 non gestita da AWS Systems Manager

Descrizione

Verifica se le istanze Amazon EC2 nel tuo account sono gestite da. AWS Systems Manager

Systems Manager facilita la comprensione e il controllo dello stato attuale dell'istanza di Amazon EC2 e delle configurazioni del sistema operativo. Con Systems Manager puoi raccogliere informazioni sulla configurazione del software e sull'inventario del tuo parco istanze, incluso il software installato su tali istanze. Ciò consente di tenere traccia della configurazione dettagliata del sistema, dei livelli di patch del sistema operativo, delle configurazioni delle applicazioni e di altri dettagli sull'implementazione.

Per ulteriori informazioni, consulta Configurazione di Systems Manager per istanze di EC2.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz145`

Origine

`AWS Config Managed Rule: ec2-instance-managed-by-systems-manager`

Criteri di avviso

Giallo: le istanze di Amazon EC2 non sono gestite da Systems Manager.

Operazione consigliata

Configura l'istanza di Amazon EC2 in modo che sia gestita da Systems Manager.

Questo controllo non può essere escluso dalla visualizzazione nella Trusted Advisor console.

Per ulteriori informazioni, consulta Perché la mia istanza di EC2 non viene visualizzata come nodo gestito o mostra lo stato "Connessione persa" in Systems Manager?.

Risorse aggiuntive

Configurazione di Systems Manager per istanze di EC2

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Repository di Amazon ECR con immutabilità dei tag disabilitata

Descrizione

Controlla se per un repository Amazon ECR privato è attivata l'immutabilità dei tag immagine.

Attiva l'immutabilità dei tag immagine in un repository di Amazon ECR privato per impedire la sovrascrittura dei tag immagine. In questo modo, puoi considerare i tag descrittivi un modo affidabile per tracciare e identificare in modo univoco le immagini. Ad esempio, se è attivata l'immutabilità dei tag immagine, gli utenti possono utilizzare in modo affidabile un tag immagine per correlare una versione dell'immagine distribuita al build che ha prodotto tale immagine.

Per ulteriori informazioni, consulta Mutabilità dei tag immagine.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz129`

Origine

`AWS Config Managed Rule: ecr-private-tag-immutability-enabled`

Criteri di avviso

Giallo: in un repository privato di Amazon ECR l'immutabilità dei tag non è attivata.

Operazione consigliata

Attiva l'immutabilità dei tag immagine per i repository privati di Amazon ECR.

Per ulteriori informazioni, consulta Mutabilità dei tag immagine.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Cluster di Amazon ECS con approfondimenti sui container disabilitati

Descrizione

Verifica se Amazon CloudWatch Container Insights è attivato per i tuoi cluster Amazon ECS.

CloudWatch Container Insights raccoglie, aggrega e riepiloga i parametri e i log delle applicazioni e dei microservizi containerizzati. I parametri includono l'utilizzo di risorse come CPU, memoria, dischi e rete.

Per ulteriori informazioni, consulta Amazon ECS CloudWatch Container Insights.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz173`

Origine

`AWS Config Managed Rule: ecs-container-insights-enabled`

Criteri di avviso

Giallo: per il cluster di Amazon ECS non sono abilitati approfondimenti sui container.

Operazione consigliata

Attiva CloudWatch Container Insights sui tuoi cluster Amazon ECS.

Per ulteriori informazioni, consulta Utilizzo degli approfondimenti sui container.

Risorse aggiuntive

Informazioni approfondite sui CloudWatch container Amazon ECS

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

La registrazione dei log delle attività di Amazon ECS non è abilitata

Descrizione

Controlla se la configurazione dei log è impostata su definizioni di attività di Amazon ECS attive.

Il controllo della configurazione dei log nelle definizioni delle attività di Amazon ECS assicura che i log generati dai container siano configurati e archiviati correttamente. Ciò facilita l'identificazione e la soluzione dei problemi in maniera più rapida, l'ottimizzazione delle prestazioni e l'adempimento dei requisiti di conformità.

Per impostazione predefinita, i log acquisiti mostrano l'output del comando che viene visualizzato normalmente in un terminale interattivo se il container è stato eseguito in locale. Il driver awslogs passa questi log da Docker ad Amazon Logs. CloudWatch

Per ulteriori informazioni, consulta Utilizzo del driver di log awslogs.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz175`

Origine

`AWS Config Managed Rule: ecs-task-definition-log-configuration`

Criteri di avviso

Giallo: la definizione delle attività di Amazon ECS non include una configurazione per la registrazione dei log.

Operazione consigliata

Valuta la possibilità di specificare la configurazione del driver di registro nella definizione del contenitore per inviare le informazioni di registro a Logs o a un altro driver di CloudWatch registrazione.

Per ulteriori informazioni, vedere. LogConfiguration

Risorse aggiuntive

Valuta la possibilità di specificare la configurazione del driver di registro nella definizione del contenitore per inviare le informazioni di registro a CloudWatch Logs o a un altro driver di registrazione.

Per ulteriori informazioni, consulta Esempio di definizioni di attività.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Registrazione OpenSearch del servizio Amazon CloudWatch non configurata

Descrizione

Verifica se i domini Amazon OpenSearch Service sono configurati per inviare log ad Amazon CloudWatch Logs.

Il monitoraggio dei log è fondamentale per mantenere l'affidabilità, la disponibilità e le prestazioni del servizio. OpenSearch

I log di ricerca lenti, i log di indicizzazione lenti e i log di errore sono utili per la risoluzione di problemi di prestazioni e stabilità del carico di lavoro. Per la raccolta dei dati, questi log devono essere abilitati.

È possibile specificare i tipi di registro che si desidera filtrare (errore, ricerca, indice) utilizzando il parametro LogTypes nelle regole. AWS Config

Per ulteriori informazioni, consulta Monitoraggio dei domini Amazon OpenSearch Service.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz184`

Origine

`AWS Config Managed Rule: opensearch-logs-to-cloudwatch`

Criteri di avviso

Giallo: Amazon OpenSearch Service non dispone di una configurazione di registrazione con Amazon CloudWatch Logs

Operazione consigliata

Configura i domini OpenSearch di servizio per pubblicare i log su Logs. CloudWatch

Per ulteriori informazioni, consulta Abilitazione della pubblicazione di log (console).

Risorse aggiuntive

- Monitoraggio delle metriche dei cluster di OpenSearch servizi con Amazon CloudWatch

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Istanze database Amazon RDS nei cluster con gruppi di parametri eterogenei

Descrizione

Consigliamo che tutte le istanze DB del cluster DB utilizzino lo stesso gruppo di parametri DB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt010`

Criteri di avviso

Giallo: i cluster DB hanno le istanze DB con gruppi di parametri eterogenei.

Operazione consigliata

Associate l'istanza DB al gruppo di parametri DB associato all'istanza writer nel vostro cluster DB.

Risorse aggiuntive

Quando le istanze DB del cluster DB utilizzano diversi gruppi di parametri DB, può verificarsi un comportamento incoerente durante un failover o problemi di compatibilità tra le istanze DB del cluster DB.

Per ulteriori informazioni, consulta la sezione Uso di gruppi di parametri.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Amazon RDS Enhanced Monitoring è disattivato

Descrizione

Le risorse del database non hanno attivato Enhanced Monitoring. Il monitoraggio avanzato offre i parametri del sistema operativo in tempo reale per il monitoraggio e la risoluzione dei problemi.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt004`

Criteri di avviso

Giallo: nelle risorse Amazon RDS non è attivato il monitoraggio avanzato.

Operazione consigliata

Attiva il monitoraggio avanzato.

Risorse aggiuntive

Enhanced Monitoring for Amazon RDS offre ulteriore visibilità sullo stato delle istanze DB. Ti consigliamo di attivare Enhanced Monitoring. Quando l'opzione Enhanced Monitoring è attivata per l'istanza DB, raccoglie le metriche fondamentali del sistema operativo e le informazioni di processo.

Per ulteriori informazioni, consulta Monitoraggio delle metriche OS con il monitoraggio avanzato.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Amazon RDS Performance Insights è disattivato

Descrizione

Amazon RDS Performance Insights monitora il carico dell'istanza DB per aiutarti ad analizzare e risolvere i problemi di prestazioni del database. Ti consigliamo di attivare Performance Insights.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt012`

Criteri di avviso

Giallo: sulle risorse Amazon RDS non è attivato Performance Insights.

Operazione consigliata

Attivare Performance Insights.

Risorse aggiuntive

Performance Insights utilizza un metodo di raccolta dati leggero che non influisce sulle prestazioni delle applicazioni. Performance Insights consente di valutare rapidamente il carico del database.

Per ulteriori informazioni, consulta Monitoraggio del carico del DB con Performance Insights su Amazon RDS.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Il parametro Amazon RDS track_counts è disattivato

Descrizione

Quando il parametro track_counts è disattivato, il database non raccoglie le statistiche sulle attività del database. La funzione di autovacuum richiede che queste statistiche funzionino correttamente.

Ti consigliamo di impostare il parametro track_counts su 1

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

> **Note**
>
> Quando un'istanza DB o un cluster DB viene interrotto, puoi visualizzare i consigli di Amazon RDS Trusted Advisor per 3-5 giorni. Dopo cinque giorni, i consigli non sono disponibili in Trusted Advisor. Per visualizzare i consigli, apri la console Amazon RDS, quindi scegli Consigli.
> Se elimini un'istanza o un cluster DB, i consigli associati a tali istanze o cluster non sono disponibili nella console di Trusted Advisor gestione Amazon RDS.

ID di controllo

`c1qf5bt027`

Criteri di avviso

Giallo: i gruppi di parametri DB hanno il parametro track_counts disattivato.

Operazione consigliata

Imposta il parametro track_counts su 1

Risorse aggiuntive

Quando il parametro track_counts è disattivato, disabilita la raccolta di statistiche sulle attività del database. Il demone autovacuum richiede le statistiche raccolte per identificare le tabelle per autovacuum e autoanalyze.

Per ulteriori informazioni, consulta Runtime Statistics for PostgreSQL sul sito Web della documentazione di PostgreSQL.

Colonne del report

- Stato
- Regione
- Risorsa
- Valore del parametro
- Valore consigliato
- Ora ultimo aggiornamento

Registrazione dei log di controllo del cluster di Amazon Redshift

Descrizione

Controlla se la registrazione dei log di controllo del database è attivata per i cluster di Amazon Redshift. Amazon Redshift registra informazioni su connessioni e attività degli utenti nel database.

Puoi specificare il nome del bucket Amazon S3 di registrazione desiderato in modo che corrisponda nel parametro bucketNames delle tue regole. AWS Config

Per ulteriori informazioni, consulta Registrazione dei log di controllo del database.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz134`

Origine

`AWS Config Managed Rule: redshift-audit-logging-enabled`

Criteri di avviso

Giallo: la registrazione dei log di controllo del database di un cluster di Amazon Redshift è disabilitata

Operazione consigliata

Attiva la registrazione dei log e il monitoraggio dei cluster di Amazon Redshift.

Per ulteriori informazioni, consulta Configurazione della verifica tramite la console.

Risorse aggiuntive

Registrazione dei log e monitoraggio su Amazon Redshift

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Per Amazon S3 non sono abilitate le Notifiche di eventi

Descrizione

Controlla se le Notifiche di eventi di Amazon S3 sono abilitate o se sono configurate correttamente con la destinazione o i tipi desiderati.

La funzionalità di Notifiche di eventi di Amazon S3 invia notifiche quando si verificano determinati eventi nel bucket di Amazon S3. Amazon S3 può inviare messaggi di notifica alle code di Amazon SQS, agli argomenti e alle funzioni di Amazon SNS. AWS Lambda

Puoi specificare la destinazione e i tipi di evento desiderati utilizzando i parametri destinationARN ed eventTypes delle tue regole. AWS Config

Per ulteriori informazioni, consulta Notifiche degli eventi di Amazon S3.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz163`

Origine

`AWS Config Managed Rule: s3-event-notifications-enabled`

Criteri di avviso

Giallo: per Amazon S3 le Notifiche degli eventi non sono abilitate o configurate con la destinazione o i tipi desiderati.

Operazione consigliata

Configura le Notifiche di eventi di Amazon S3 per gli eventi relativi a oggetti e bucket.

Per ulteriori informazioni, consulta Attivazione e configurazione delle Notifiche di eventi tramite la console di Amazon S3.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Gli argomenti di Amazon SNS non registrano i log dello stato di consegna dei messaggi

Descrizione

Controlla se per gli argomenti di Amazon SNS è attivata la registrazione dei log dello stato di consegna dei messaggi.

Configura gli argomenti di Amazon SNS per la registrazione dei log dello stato di consegna dei messaggi in modo da fornire maggiori approfondimenti operativi. Ad esempio, la registrazione dei log di consegna dei messaggi verifica se un messaggio è stato consegnato a un particolare endpoint di Amazon SNS. La registrazione dei log, inoltre, facilitano l'identificazione della risposta inviata dall'endpoint.

Per ulteriori informazioni, consulta Stato di consegna dei messaggi di Amazon SNS.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz121`

Origine

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

Criteri di avviso

Giallo: la registrazione dei log dello stato di consegna dei messaggi non è attivata per un argomento di Amazon SNS.

Operazione consigliata

Attiva la registrazione dei log dello stato di consegna dei messaggi per gli argomenti SNS.

Per ulteriori informazioni, consulta Configurazione della registrazione dei log dello stato di consegna con la Console di gestione AWS.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Amazon VPC senza log di flusso

Descrizione

Controlla se per un VPC sono stati creati i log di flusso di Amazon Virtual Private Cloud.

È possibile specificare il tipo di traffico utilizzando il parametro TrafficType nelle regole. AWS Config

Per ulteriori informazioni, consulta Registrazione dei log del traffico IP utilizzando i log di flusso VPC.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

```
c18d2gz122
```

Origine

```
AWS Config Managed Rule: vpc-flow-logs-enabled
```

Criteri di avviso

Giallo: i VPC non includono log di flusso di Amazon VPC.

Operazione consigliata

Crea log di flusso VPC per ogni VPC.

Per ulteriori informazioni, consulta Creazione di un log di flusso

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Application Load Balancer e Classic Load Balancer senza log di accesso abilitati

Descrizione

Controlla se in Application Load Balancer e Classic Load Balancer è abilitata la registrazione dei log di accesso.

Elastic Load Balancing fornisce log di accesso che acquisiscono informazioni dettagliate sulle richieste inviate al tuo load balancer. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server. Puoi utilizzare questi log per analizzare i modelli di traffico e risolvere i problemi che potresti incontrare.

I log di accesso sono una funzionalità facoltativa di Elastic Load Balancing che per impostazione predefinita è disabilitata. Dopo aver abilitato i log di accesso per il load balancer, Elastic Load Balancing acquisisce i log e li archivia nel bucket Amazon S3 specificato.

Puoi specificare il bucket Amazon S3 del log di accesso che desideri controllare utilizzando il BucketNames parametro s3 nelle tue regole. AWS Config

Per ulteriori informazioni, consulta Log di accesso per Application Load Balancer o Log di accesso per Classic Load Balancer.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz167`

Origine

`AWS Config Managed Rule: elb-logging-enabled`

Criteri di avviso

Giallo: la funzionalità dei log di accesso non è abilitata per Application Load Balancer o Classic Load Balancer.

Operazione consigliata

Abilita i log di accesso per Application Load Balancer e Classic Load Balancer.

Per ulteriori informazioni, consulta Abilitazione dei log di accesso per Application Load Balancer o Abilitazione dei log di accesso per Classic Load Balancer.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS CloudFormation Notifica Stack

Descrizione

Verifica se tutti i tuoi AWS CloudFormation stack utilizzano Amazon SNS per ricevere notifiche quando si verifica un evento.

Puoi configurare questo controllo per cercare ARN specifici per argomenti di Amazon SNS utilizzando i parametri delle tue regole. AWS Config

Per ulteriori informazioni, consulta Impostazione delle opzioni AWS CloudFormation dello stack.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz111`

Origine

`AWS Config Managed Rule: cloudformation-stack-notification-check`

Criteri di avviso

Giallo: le notifiche degli eventi di Amazon SNS per i tuoi AWS CloudFormation stack non sono attivate.

Operazione consigliata

Assicurati che i tuoi AWS CloudFormation stack utilizzino Amazon SNS per ricevere notifiche quando si verifica un evento.

Il monitoraggio degli eventi dello stack ti aiuta a rispondere rapidamente ad azioni non autorizzate che potrebbero alterare il tuo ambiente. AWS

Risorse aggiuntive

Come posso ricevere un avviso e-mail quando il mio CloudFormation stack AWS entra nello stato ROLLBACK_IN_PROGRESS?

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS CloudTrail registrazione degli eventi relativi ai dati per gli oggetti in un bucket S3

Descrizione

Verifica se almeno un AWS CloudTrail trail registra gli eventi relativi ai dati di Amazon S3 per tutti i bucket Amazon S3.

Per ulteriori informazioni, consulta Registrazione dei log sulle chiamate dell'API Amazon S3 utilizzando AWS CloudTrail.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

```
c18d2gz166
```

Origine

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

Criteri di avviso

Giallo: la registrazione AWS CloudTrail degli eventi per i bucket Amazon S3 non è configurata

Operazione consigliata

Abilita la registrazione CloudTrail degli eventi per i bucket e gli oggetti Amazon S3 per tenere traccia delle richieste di accesso ai bucket di destinazione.

Per ulteriori informazioni, consulta Abilitazione della registrazione CloudTrail degli eventi per i bucket e gli oggetti S3.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS CodeBuild Registrazione del progetto

Descrizione

Verifica se l'ambiente del AWS CodeBuild progetto utilizza la registrazione. Le opzioni di registrazione possono essere log in Amazon CloudWatch Logs, integrati in uno specifico bucket Amazon S3 o entrambi. L'abilitazione della registrazione in un CodeBuild progetto può offrire diversi vantaggi, come il debug e il controllo.

Puoi specificare il nome del bucket Amazon S3 o del gruppo CloudWatch Logs per l'archiviazione dei log, utilizzando il parametro s3 BucketNames o cloud WatchGroup Names nelle tue regole. AWS Config

Per ulteriori informazioni, consulta Monitoraggio di AWS CodeBuild.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz113`

Origine

`AWS Config Managed Rule: codebuild-project-logging-enabled`

Criteri di avviso

Giallo: la registrazione del AWS CodeBuild progetto non è abilitata.

Operazione consigliata

Assicurati che la registrazione sia attivata nel tuo AWS CodeBuild progetto. Questo controllo non può essere escluso dalla visualizzazione nella AWS Trusted Advisor console.

Per ulteriori informazioni, consulta Accesso e monitoraggio. AWS CodeBuild

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS CodeDeploy Rollback e monitoraggio automatici abilitati

Descrizione

Controlla se il gruppo di istanze implementate è configurato con il rollback automatico dell'implementazione e il monitoraggio dell'implementazione con allarmi collegati. In caso di problemi durante un'implementazione, questa viene ripristinata automaticamente e l'applicazione rimane in uno stato stabile

Per ulteriori informazioni, consulta Ridistribuire e ripristinare una distribuzione con. CodeDeploy

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz114`

Origine

`AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled`

Criteri di avviso

Giallo: il rollback AWS CodeDeploy automatico della distribuzione e il monitoraggio della distribuzione non sono abilitati.

Operazione consigliata

Configura un gruppo di istanze implementate o un'implementazione in modo che venga eseguito automaticamente il rollback quando un'implementazione non riesce o quando viene raggiunta una soglia di monitoraggio specificata.

Configura l'allarme per monitorare vari parametri, ad esempio l'utilizzo della CPU, l'utilizzo della memoria o il traffico di rete, durante il processo di implementazione. Se uno di questi parametri supera determinate soglie, si attivano gli allarmi e l'implementazione viene interrotta o ripristinata.

Per informazioni sull'impostazione dei rollback automatici e sulla configurazione degli allarmi per i gruppi di istanze implementate, consulta Configurazione delle opzioni avanzate per un gruppo di istanze implementate.

Risorse aggiuntive

Che cos'è CodeDeploy?

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS CodeDeploy Lambda utilizza all-at-once la configurazione di distribuzione

Descrizione

Verifica se il gruppo AWS CodeDeploy di distribuzione per la piattaforma di AWS Lambda elaborazione utilizza la configurazione di all-at-once distribuzione.

Per ridurre il rischio di errori di implementazione delle funzioni CodeDeploy Lambda, è consigliabile utilizzare la configurazione di distribuzione canaria o lineare anziché l'opzione predefinita in cui tutto il traffico viene spostato dalla funzione Lambda originale alla funzione aggiornata contemporaneamente.

Per ulteriori informazioni, consulta Versioni della funzione Lambda e Configurazione dell'implementazione.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz115`

Origine

`AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-disabled`

Criteri di avviso

Giallo: la distribuzione AWS CodeDeploy Lambda utilizza la configurazione di all-at-once distribuzione per spostare tutto il traffico verso le funzioni Lambda aggiornate contemporaneamente.

Operazione consigliata

Usa la configurazione di distribuzione Canary o Linear del gruppo di CodeDeploy distribuzione per la piattaforma di calcolo Lambda.

Risorse aggiuntive

Configurazione della distribuzione

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Elastic Beanstalk Enhanced Health Reporting non è configurato

Descrizione

Verifica se un AWS Elastic Beanstalk ambiente è configurato per una reportistica sanitaria avanzata.

I report avanzati sull'integrità di Elastic Beanstalk forniscono parametri dettagliati sulle prestazioni, ad esempio l'utilizzo della CPU, l'utilizzo della memoria, il traffico di rete e informazioni sullo stato dell'infrastruttura, ad es. il numero di istanze e lo stato del sistema di bilanciamento del carico.

Per ulteriori informazioni, consulta Monitoraggio e report avanzati sull'integrità.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

```
c18d2gz108
```

Origine

```
AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled
```

Criteri di avviso

Giallo: l'ambiente Elastic Beanstalk non è configurato per i report avanzati sull'integrità

Operazione consigliata

Assicurati che l'ambiente Elastic Beanstalk sia configurato per i report avanzati sull'integrità.

Per ulteriori informazioni, consulta Abilitazione di report avanzati sull'integrità utilizzando la console di Elastic Beanstalk.

Risorse aggiuntive

- Abilitazione di report avanzati sull'integrità di Elastic Beanstalk
- Monitoraggio e report avanzati sull'integrità

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Elastic Beanstalk con gli aggiornamenti gestiti della piattaforma disattivati

Descrizione

Controlla se gli aggiornamenti della piattaforma gestita negli ambienti Elastic Beanstalk e nei modelli di configurazione sono abilitati.

AWS Elastic Beanstalk rilascia regolarmente aggiornamenti della piattaforma per fornire correzioni, aggiornamenti software e nuove funzionalità. Con gli aggiornamenti della piattaforma gestita, Elastic Beanstalk può eseguire automaticamente gli aggiornamenti della piattaforma per nuove patch e versioni secondarie della piattaforma.

Puoi specificare il livello di aggiornamento desiderato nei UpdateLevelparametri delle tue AWS Config regole.

Per ulteriori informazioni, consulta Aggiornamento della versione della piattaforma dell'ambiente Elastic Beanstalk.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz177`

Origine

`AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled`

Criteri di avviso

Giallo: gli aggiornamenti AWS Elastic Beanstalk gestiti della piattaforma non sono configurati affatto, nemmeno a livello secondario o di patch.

Operazione consigliata

Abilita gli aggiornamenti della piattaforma gestita negli ambienti Elastic Beanstalk o configurali a un livello minore o di aggiornamento.

Per ulteriori informazioni, consulta Aggiornamenti della piattaforma gestita.

Risorse aggiuntive

- Abilitazione di report avanzati sull'integrità di Elastic Beanstalk
- Monitoraggio e report avanzati sull'integrità

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Fargate la versione della piattaforma non è la più recente

Descrizione

Controlla se Amazon ECS sta eseguendo la versione più recente della piattaforma AWS Fargate. Per la versione della piattaforma Fargate si intende un determinato ambiente di runtime per l'infrastruttura delle attività Fargate. È una combinazione delle versioni del kernel e del runtime del container. Le nuove versioni della piattaforma vengono rilasciate nel corso dell'evoluzione dell'ambiente di runtime. Ad esempio, se sono disponibili aggiornamenti del kernel o del sistema operativo, nuove funzionalità, correzioni di bug o aggiornamenti di sicurezza.

Per ulteriori informazioni, consulta Manutenzione delle attività Fargate.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz174`

Origine

`AWS Config Managed Rule: ecs-fargate-latest-platform-version`

Criteri di avviso

Giallo: Amazon ECS non è in esecuzione sulla versione più recente della piattaforma Fargate.

Operazione consigliata

Esegui l’aggiornamento alla versione della piattaforma Fargate più recente.

Per ulteriori informazioni, consulta Manutenzione delle attività Fargate.

Colonne del report

- Stato

- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Systems Manager State Manager Association in stato di non conformità

Descrizione

Verifica se lo stato di conformità dell' AWS Systems Manager associazione è CONFORME o NON_COMPLIANT dopo l'esecuzione dell'associazione sull'istanza.

State Manager, una funzionalità di AWS Systems Manager, è un servizio di gestione della configurazione sicuro e scalabile che automatizza il processo di mantenimento dei nodi gestiti e delle altre AWS risorse in uno stato definito dall'utente. Un'associazione State Manager è una configurazione che si assegna alle risorse. AWS La configurazione definisce lo stato che intendi mantenere sulle tue risorse, per facilitare la realizzazione dell'obiettivo, ad es. evitare variazioni di configurazione tra le tue istanze di Amazon EC2.

Per ulteriori informazioni, consulta State Manager AWS Systems Manager.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

```
c18d2gz147
```

Origine

```
AWS Config Managed Rule: ec2-managedinstance-association-compliance-
status-check
```

Criteri di avviso

Giallo: lo stato di conformità dell' AWS Systems Manager associazione è NON_COMPLIANT.

Operazione consigliata

Convalida lo stato delle associazioni di State Manager ed effettua le operazioni necessarie per il ripristino dello stato COMPLIANT.

Per ulteriori informazioni, consulta Informazioni su State Manager.

Risorse aggiuntive

AWS Systems Manager Responsabile dello stato

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

CloudTrail i trail non sono configurati con Amazon CloudWatch Logs

Descrizione

Verifica se i AWS CloudTrail trail sono configurati per inviare log a CloudWatch Logs.

Monitora i file di CloudTrail registro con CloudWatch Logs per attivare una risposta automatica quando vengono acquisiti eventi critici. AWS CloudTrail

Per ulteriori informazioni, vedere Monitoraggio dei file di CloudTrail registro con i CloudWatch registri.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore

prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz164`

Origine

`AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled`

Criteri di avviso

Giallo: non AWS CloudTrail è configurato con l'integrazione CloudWatch Logs.

Operazione consigliata

Configura i CloudTrail percorsi per inviare gli eventi di registro ai CloudWatch registri.

Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi per CloudTrail eventi: esempi.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Protezione dall’eliminazione Elastic Load Balancing non abilitata per i sistemi di bilanciamento del carico

Descrizione

Controlla se la protezione dall’eliminazione è attivata per i sistemi di bilanciamento del carico.

Elastic Load Balancing supporta la protezione dall’eliminazione per Application Load Balancer, Network Load Balancer e Gateway Load Balancer. Per evitare che il sistema di bilanciamento

del carico venga eliminato accidentalmente, abilita la protezione dall'eliminazione. La protezione dall'eliminazione è disattivata per impostazione predefinita quando crei un sistema di bilanciamento del carico. Se i tuoi sistemi di bilanciamento del carico fanno parte di un ambiente di produzione, valuta l'opportunità di attivare la protezione dall'eliminazione.

I log di accesso sono una funzionalità facoltativa di Elastic Load Balancing che per impostazione predefinita è disabilitata. Dopo aver abilitato i log di accesso per il load balancer, Elastic Load Balancing acquisisce i log e li archivia nel bucket Amazon S3 specificato.

Per ulteriori informazioni, consulta Protezione dall'eliminazione di Application Load Balancer, Protezione dall'eliminazione di Network Load Balancer o Protezione dall'eliminazione di Gateway Load Balancer.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz168`

Origine

`AWS Config Managed Rule: elb-deletion-protection-enabled`

Criteri di avviso

Giallo: la protezione dall'eliminazione non è abilitata per un sistema di bilanciamento del carico.

Operazione consigliata

Attiva la protezione dall'eliminazione per Application Load Balancer, Network Load Balancer e Gateway Load Balancer.

Per ulteriori informazioni, consulta Protezione dall'eliminazione di Application Load Balancer, Protezione dall'eliminazione di Network Load Balancer o Protezione dall'eliminazione di Gateway Load Balancer.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Controllo della protezione dall’eliminazione del cluster DB di RDS

Descrizione

Controlla se è abilitata la protezione dall’eliminazione nei cluster DB di Amazon RDS.

Quando è configurata la protezione dall’eliminazione in un cluster, il database non può essere eliminato da un utente.

La protezione da eliminazione è disponibile per Amazon Aurora e RDS per MySQL, RDS per MariaDB, RDS per Oracle, RDS per PostgreSQL e RDS per SQL Server in tutte le regioni. AWS

Per ulteriori informazioni, consulta Protezione dall’eliminazione per i cluster di Aurora.

ID di controllo

`c18d2gz160`

Origine

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

Criteri di avviso

Giallo: esistono cluster DB di Amazon RDS per cui non è abilitata la protezione dall’eliminazione.

Operazione consigliata

Attiva la protezione dall’eliminazione quando crei un cluster del database di Amazon RDS.

Puoi eliminare solo i cluster per cui non è abilitata la protezione dall'eliminazione. L'attivazione della protezione dall’eliminazione aggiunge un ulteriore livello di protezione ed evita la perdita di dati dovuta all'eliminazione accidentale o non accidentale di un'istanza del database. La

protezione dall'eliminazione contribuisce anche a soddisfare i requisiti di conformità normativa e a garantire la continuità aziendale.

Per ulteriori informazioni, consulta Protezione dall'eliminazione per i cluster di Aurora.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

Risorse aggiuntive

Protezione dall'eliminazione per i cluster di Aurora

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Controllo automatico dell'aggiornamento delle versioni secondarie di istanze DB di RDS

Descrizione

Controlla se per le istanze DB di Amazon RDS sono configurati aggiornamenti automatici delle versioni secondarie.

Attiva gli aggiornamenti automatici delle versioni secondarie di un'istanza di Amazon RDS per assicurarti che sul database sia sempre in esecuzione la versione più recente, sicura e stabile. Gli aggiornamenti secondari forniscono aggiornamenti di sicurezza, correzioni di bug, miglioramenti delle prestazioni e mantengono la compatibilità con le applicazioni esistenti.

Per ulteriori informazioni, consulta Aggiornamento di una versione del motore delle istanze DB.

> **Note**
>
> I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Al momento, non è possibile escludere le risorse da questo controllo.

ID di controllo

`c18d2gz155`

Origine

`AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled`

Criteri di avviso

Giallo: per l'istanza DB di RDS non sono attivati gli aggiornamenti automatici delle versioni secondarie.

Operazione consigliata

Attiva gli aggiornamenti automatici delle versioni secondarie quando crei un'istanza DB di Amazon RDS.

Quando attivi l'aggiornamento della versione secondaria, la versione del database viene aggiornata automaticamente se esegue una versione secondaria del motore DB inferiore alla versione del motore aggiornata manualmente.

Colonne del report

- Stato
- Regione
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

Registro delle modifiche per AWS Trusted Advisor

Vedi il seguente argomento per le modifiche recenti ai Trusted Advisor controlli.

> **Note**
>
> Se utilizzi la Trusted Advisor console o l' AWS Support API, i controlli che sono stati rimossi non verranno visualizzati nei risultati dei controlli. Se utilizzi uno dei controlli rimossi, ad esempio specificando l'ID di controllo in un'operazione AWS Support API o il tuo codice, devi rimuovere questi controlli per evitare errori nelle chiamate API.

Per ulteriori informazioni sulle operazioni API disponibili, consulta la sezione AWS Trusted Advisor verifica riferimento.

Sono stati rimossi 5 controlli e aggiunto 1 controllo

Trusted Advisor sono stati deprecati 3 controlli di tolleranza agli errori, 1 controllo delle prestazioni e 1 controllo di sicurezza il 15 maggio 2024:

- Uso della IAM
- Bilanciamento del carico tra Zone ELB
- Volumi magnetici Amazon EBS sovrautilizzati
- Numero elevato di regole del gruppo di sicurezza EC2 applicate a un'istanza
- Numero elevato di regole in un gruppo di sicurezza EC2

Trusted Advisor aggiunto 1 nuovo controllo di sicurezza il 15 maggio 2024:

- Registri di accesso al server Amazon S3 abilitati

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Controlli di tolleranza agli errori rimossi

Trusted Advisor deprecato controllo 3 Fault Tolerance il 25 aprile 2024:

- AWS Direct Connect Ridondanza di connessione

- AWS Direct Connect Ridondanza di ubicazione
- AWS Direct Connect Ridondanza dell'interfaccia virtuale

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovi controlli di tolleranza agli errori

Trusted Advisor aggiunto 1 controllo di tolleranza agli errori il 29 febbraio 2024:

- NLB: risorsa rivolta a Internet in sottorete privata

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Tolleranza agli errori e controlli di sicurezza aggiornati

Trusted Advisor ha aggiunto 1 nuovo controllo di tolleranza agli errori e modificato 1 controllo di tolleranza agli errori e 1 controllo di sicurezza esistenti il 28 marzo 2024:

- Aggiunto il controllo dei componenti AWS Resilience Hub dell'applicazione
- Funzioni aggiornate AWS Lambda abilitate per VPC senza ridondanza Multi-AZ
- Funzioni aggiornate AWS Lambda utilizzando runtime obsoleti

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovi controlli di tolleranza agli errori

Trusted Advisor aggiunto 1 controllo di tolleranza agli errori il 31 gennaio 2024:

- AWS Direct Connect Resilienza della posizione

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Controllo aggiornato della tolleranza agli errori

Trusted Advisor 1 controllo di tolleranza ai guasti modificato l'8 gennaio 2024:

- Il parametro innodb_flush_log_at_trx_commit di Amazon RDS non è 1

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Controllo di sicurezza aggiornato

Trusted Advisor 1 controllo di sicurezza modificato il 21 dicembre 2023:

- AWS Lambda Funzioni che utilizzano runtime obsoleti

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovi controlli di sicurezza e prestazioni

Trusted Advisor ha aggiunto 2 nuovi controlli di sicurezza e 2 nuovi controlli delle prestazioni il 20 dicembre 2023:

- I client Amazon EFS non utilizzano data-in-transit la crittografia
- Cluster Amazon Aurora DB con un provisioning insufficiente per il carico di lavoro di lettura
- Istanza Amazon RDS con capacità di sistema insufficiente
- Fine del supporto standard per le istanze Amazon EC2 con Ubuntu LTS

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovo controllo di sicurezza

Trusted Advisor aggiunto 1 nuovo controllo di sicurezza il 15 dicembre 2023:

- Record CNAME di Amazon Route 53 non corrispondenti che puntano direttamente ai bucket S3

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovi controlli di tolleranza agli errori e ottimizzazione dei costi

Trusted Advisor ha aggiunto 2 nuovi controlli di tolleranza agli errori e 1 nuovo controllo di ottimizzazione dei costi il 07 dicembre 2023:

- Cluster Amazon DocumentDB Single-AZ
- Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3

- Driver Amazon ECS AWS Logs in modalità di blocco

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovi controlli di tolleranza ai guasti

Trusted Advisor ha aggiunto 3 nuovi controlli di tolleranza agli errori il 17 novembre 2023:

- ALB Multi-AZ
- NLB Multi-AZ
- Interfaccia VPC: interfacce di rete endpoint in più AZ

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuovi controlli per Amazon RDS

Trusted Advisor ha aggiunto 37 nuovi controlli per Amazon RDS il 15 novembre 2023.

Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Nuova API AWS Trusted Advisor

AWS Trusted Advisor introduce nuove API per consentire l'accesso programmatico ai controlli delle best practice, ai consigli e ai consigli con priorità di Trusted Advisor. Trusted Advisor Le API consentono l'integrazione programmatica Trusted Advisor con lo strumento operativo preferito per automatizzare e ottimizzare i carichi di lavoro su larga scala. Disponibili per i clienti Business, Enterprise On-Ramp o Enterprise Support, le nuove API forniscono l'accesso ai Trusted Advisor consigli per il tuo account o per tutti gli account collegati all'interno di un account di pagamento. I clienti di Enterprise Support con accesso agli account di gestione o amministratori delegati possono inoltre recuperare in modo programmatico consigli prioritari all'interno della propria organizzazione.

Le nuove Trusted Advisor API sostituiranno le 3 funzionalità precedentemente offerte tramite AWS Support API (SAPI). SAPI continuerà a offrire casi e altre informazioni di supporto.

Trusted Advisor Le API sono generalmente disponibili nelle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Asia Pacifico (Seoul), Asia Pacifico (Sydney) ed Europa (Irlanda).

Per saperne di più, visita la pagina delle API.AWS Trusted Advisor

Trusted Advisor controlla la rimozione

Trusted Advisor ha rimosso i seguenti controlli il 9 novembre 2023.

Nome di controllo	Categoria di controllo	ID di controllo
I volumi EBS devono essere collegati alle istanze EC2	Sicurezza	`Hs4Ma3G119`
I bucket S3 devono avere la crittografia lato server abilitata	Sicurezza	`Hs4Ma3G167`
CloudFront le distribuzioni devono avere l'identità di accesso all'origine abilitata	Sicurezza	`Hs4Ma3G195`

Integrazione dei AWS Config controlli in Trusted Advisor

Trusted Advisor aggiunti 64 nuovi controlli introdotti entro AWS Config il 30 ottobre 2023.

Per ulteriori informazioni, consulta Visualizzazione dei controlli AWS Trusted Advisor forniti da AWS Config.

Nuovi controlli di tolleranza ai guasti

Trusted Advisor ha aggiunto i seguenti controlli il 12 ottobre 2023.

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver Ridondanza della zona di disponibilità degli endpoint
- Dimensionamento automatico degli IP disponibili nelle sottoreti
- Broker Amazon MSK che ospitano un numero eccessivo di partizioni

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Nuova verifica dei limiti del servizio

Trusted Advisor ha aggiunto il seguente controllo il 17 agosto 2023.

- Utilizzo dell'archiviazione di codice Lambda

Per ulteriori informazioni, consulta la categoria Limiti del servizio.

Nuovi controlli di tolleranza agli errori

Trusted Advisor ha aggiunto il seguente controllo il 3 agosto 2023.

- AWS Lambda On Failure Event Destinations

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Nuovi controlli di prestazioni e di tolleranza agli errori

Trusted Advisor ha aggiunto i seguenti controlli il 1° giugno 2023.

- Amazon EFS senza ridondanza della destinazione di montaggio
- Ottimizzazione della modalità di velocità di trasmissione effettiva di Amazon EFS
- Ridondanza della zona di disponibilità ActiveMQ
- Ridondanza della zona di disponibilità RabbitMQ

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti e la categoria Prestazioni.

Nuovi controlli di tolleranza ai guasti

Trusted Advisor ha aggiunto i seguenti controlli il 16 maggio 2023.

- Indipendenza AZ del Gateway NAT
- Controllo dell'applicazione in una singola AZ

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Nuovi controlli di tolleranza ai guasti

Trusted Advisor ha aggiunto i seguenti controlli il 27 aprile 2023.

- Numero di Regioni AWS in un set di repliche di Incident Manager
- AWS Resilience Hub età di valutazione

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Espansione regionale dei controlli di tolleranza agli errori di Amazon ECS

Trusted Advisor il 27 aprile 2023 ha esteso i seguenti controlli ad altre regioni. Trusted Advisor i controlli per Amazon ECS sono ora disponibili in tutte le regioni in cui Amazon ECS è generalmente disponibile.

- Servizio di Amazon ECS con un'unica AZ
- Strategia di collocazione Multi-AZ di Amazon ECS

Queste Regioni sono Africa (Città del Capo), Asia Pacifico (Hong Kong), Asia Pacifico (Hyderabad), Asia Pacifico (Giacarta), Asia Pacifico (Melbourne), Europa (Milano), Europa (Spagna), Europa (Zurigo), Medio Oriente (Bahrein) e Medio Oriente (Emirati Arabi Uniti).

Nuovi controlli di tolleranza ai guasti

Trusted Advisor ha aggiunto i seguenti controlli il 30 marzo 2023.

- Servizio di Amazon ECS con un'unica AZ
- Strategia di collocazione Multi-AZ di Amazon ECS

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Nuovi controlli di tolleranza ai guasti

Trusted Advisor ha aggiunto i seguenti controlli il 15 dicembre 2022.

- AWS CloudHSM cluster che eseguono istanze HSM in un'unica AZ
- Cluster Amazon ElastiCache Multi-AZ

- Cluster Multi-AZ Amazon MemoryDB

Per ricevere risultati per i tuoi cluster e Trusted Advisor per AWS CloudHSM quelli ElastiCache di MemoryDB, devi disporre di cluster nelle tue zone di disponibilità. Per ulteriori informazioni, consulta la seguente documentazione :

- AWS CloudHSM Guida per l'utente
- Guida per lo sviluppatore di Amazon MemoryDB per Redis
- Guida ElastiCache per l'utente di Amazon for Redis

Trusted Advisor ha aggiornato le seguenti informazioni di controllo il 15 dicembre 2022.

- AWS Resilience Hub politica violata: il nome dell'app è stato aggiornato al nome dell'applicazione
- AWS Resilience Hub punteggi di resilienza: App Name e App Resilience Score sono stati aggiornati in Application Name e Application Resilience Score

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Aggiornamenti all'integrazione con Trusted AdvisorAWS Security Hub

Trusted Advisor ha effettuato il seguente aggiornamento il 17 novembre 2022.

Se disabiliti Security Hub o AWS Config per un altro Regione AWS, Trusted Advisor now rimuove i risultati del controllo in merito Regione AWS entro 7-9 giorni. In precedenza, il periodo di tempo per rimuovere i dati del Security Hub Trusted Advisor era di 90 giorni.

Per ulteriori informazioni, consulta le sezioni seguenti nell'argomento Risoluzione dei problemi:

- Ho disattivato Security Hub o AWS Config in una regione
- Il mio controllo è archiviato in Security Hub ma visualizzo ancora i risultati in Trusted Advisor

Nuovi controlli di tolleranza ai guasti per AWS Resilience Hub

Trusted Advisor ha aggiunto i seguenti controlli il 17 novembre 2022.

- AWS Resilience Hub politica violata

- AWS Resilience Hub punteggi di resilienza

Puoi utilizzare questi controlli per visualizzare lo stato della policy di resilienza e il punteggio di resilienza più recenti per le tue applicazioni. Resilience Hub ti consente di definire, tracciare e gestire la resilienza e la disponibilità delle tue applicazioni da un'unica posizione.

Per ricevere risultati Trusted Advisor per le applicazioni Resilience Hub, è necessario distribuire un' AWS applicazione e utilizzare Resilience Hub per monitorare il livello di resilienza dell'applicazione. Per ulteriori informazioni, consulta la Guida per l'utente AWS Resilience Hub.

Per ricevere risultati Trusted Advisor per i tuoi cluster ElastiCache e MemoryDB, devi disporre di cluster nelle tue zone di disponibilità. Per ulteriori informazioni, consulta la seguente documentazione :

- Guida per lo sviluppatore di Amazon MemoryDB per Redis
- Guida ElastiCache per l'utente di Amazon for Redis

Per ulteriori informazioni, consulta la categoria Tolleranza ai guasti.

Aggiornamento alla console Trusted Advisor

Trusted Advisor ha aggiunto la seguente modifica il 16 novembre 2022.

La Trusted Advisor dashboard nella console è ora Trusted Advisor denominata Consigli. La pagina Consigli per Trusted Advisor mostra ancora i risultati dei controlli e i controlli disponibili per ogni categoria per il tuo Account AWS.

Questa modifica del nome aggiorna solo la Trusted Advisor console. Puoi continuare a utilizzare la Trusted Advisor console e le Trusted Advisor operazioni nell' AWS Support API come al solito.

Per ulteriori informazioni, consulta Come iniziare con Consigli per Trusted Advisor.

Nuovi controlli per Amazon EC2

Trusted Advisor ha aggiunto il seguente controllo il 1° settembre 2022.

- Fine del supporto per le istanze Amazon EC2 con Microsoft Windows Server

Per ulteriori informazioni, consulta la categoria Sicurezza.

Aggiunti controlli Security Hub a Trusted Advisor

A partire dal 23 giugno 2022, supporta Trusted Advisor solo i controlli del Security Hub disponibili fino al 7 aprile 2022. Questa versione supporta tutti i controlli dello standard di sicurezza AWS Foundational Security Best Practices ad eccezione dei controlli nella categoria: Recover > Resilience. Per ulteriori informazioni, consulta Visualizzazione controlli AWS Security Hub in AWS Trusted Advisor.

Per un elenco dei controlli supportati, consulta Controlli AWS Foundational Security Best Practices nella Guida per l'utente di AWS Security Hub .

Sono stati aggiunti controlli da AWS Compute Optimizer

Trusted Advisor ha aggiunto i seguenti controlli il 4 maggio 2022.

Nome di controllo	Categoria di controllo	ID di controllo
Volumi Amazon EBS con provisioning eccessivo	Ottimizzazione dei costi	`COr6dfpM03`
Volumi Amazon EBS con provisioning insufficiente	Prestazioni	`COr6dfpM04`
AWS Lambda funzioni sovrafornite per le dimensioni della memoria	Ottimizzazione dei costi	`COr6dfpM05`
AWS Lambda funzioni con dotazione insufficiente per le dimensioni della memoria	Prestazioni	`COr6dfpM06`

Devi attivare Compute Optimizer in modo che questi controlli possano ricevere dati dalle tue risorse Lambda e Amazon EBS. Account AWS Per ulteriori informazioni, consulta Attiva AWS Compute Optimizer i Trusted Advisor controlli.

Aggiornamenti al controllo Exposed Access Keys

Trusted Advisor ha aggiornato il seguente controllo il 25 aprile 2022.

Nome di controllo	Categoria di controllo	ID di controllo
Exposed Access Keys	Sicurezza	`12Fnkpl8Y5`

Trusted Advisor ora aggiorna automaticamente questo controllo. Questo controllo non può essere aggiornato manualmente dalla Trusted Advisor console o dall' AWS Support API. Se l'applicazione o il codice aggiorna questo controllo per conto tuo Account AWS, ti consigliamo di aggiornarlo per non aggiornare più questo controllo. In caso contrario, verrà ricevuto l'errore `InvalidParameterValue`.

Tutte le chiavi di accesso escluse prima di questo aggiornamento non saranno più escluse e appariranno come risorse interessate. Non è possibile escludere le chiavi di accesso dai risultati del controllo. Per ulteriori informazioni, consulta Exposed Access Keys.

> **Note**
>
> Se hai creato il tuo Account AWS dopo il 25 aprile 2022, i risultati del controllo per le chiavi di accesso esposte mostrano inizialmente l'icona grigia ( ) anche per le chiavi di accesso non esposte. Ciò significa che Trusted Advisor non ha identificato alcuna modifica al controllo.
> Se Trusted Advisor identifica una risorsa a rischio, lo stato passa all'icona dell'azione consigliata ( ). Dopo aver corretto o eliminato la risorsa, il risultato del controllo mostra l'icona del segno di spunta ( ).

Controlli aggiornati per AWS Direct Connect

Trusted Advisor ha aggiornato i seguenti controlli il 29 marzo 2022.

Nome di controllo	Categoria di controllo	ID di controllo
AWS Direct Connect Ridondanza di connessione	Tolleranza ai guasti	`0t121N1Ty3`

Nome di controllo	Categoria di controllo	ID di controllo
AWS Direct Connect Ridondanza di ubicazione	Tolleranza ai guasti	`8M012Ph3U5`
AWS Direct Connect Ridondanza dell'interfaccia virtuale	Tolleranza ai guasti	`4g3Nt5M1Th`

- Il valore per la colonna Regione ora mostra il codice Regione AWS anziché il nome completo. Ad esempio, le risorse negli Stati Uniti orientali (Virginia settentrionale) avranno ora il valore `us-east-1`.
- Il valore per la colonna marca temporale ora appare nel formato RFC 3339, come `2022-03-30T01:02:27.000Z`.
- Le risorse che non presentano problemi verranno ora visualizzate nella tabella di controllo. Queste risorse avranno un'icona con un segno di spunta ( ) accanto.

  In precedenza, nella tabella comparivano solo le risorse che Trusted Advisor consigliavano di esaminare. Queste risorse hanno un'icona di avviso ( ) accanto.

AWS Security Hub controlli aggiunti alla AWS Trusted Advisor console

AWS Trusted Advisor ha aggiunto 111 controlli Security Hub alla categoria Sicurezza il 18 gennaio 2022.

Puoi visualizzare i risultati relativi ai controlli di Security Hub dallo standard di sicurezza AWS Foundational Security Best Practices. Questa integrazione non include i controlli che hanno Categoria: Ripristino > Resilienza.

Per ulteriori informazioni sull'utilizzo di questa caratteristica, consulta Visualizzazione controlli AWS Security Hub in AWS Trusted Advisor.

Nuovi controlli per Amazon EC2 e AWS Well-Architected

Trusted Advisor ha aggiunto i seguenti controlli il 20 dicembre 2021.

- Consolidamento di istanze Amazon EC2 per Microsoft SQL Server
- Istanze Amazon EC2 con provisioning eccessivo per Microsoft SQL Server
- Fine del supporto per le istanze Amazon EC2 con Microsoft SQL Server
- Problemi ad alto rischio di AWS Well-Architected per l'ottimizzazione dei costi
- Problemi ad alto rischio di AWS Well-Architected per le prestazioni
- Problemi ad alto rischio di AWS Well-Architected per la sicurezza
- Problemi ad alto rischio di AWS Well-Architected per l'affidabilità

Per ulteriori informazioni, consulta il riferimento dei controlli AWS Trusted Advisor.

Nome di controllo aggiornato per Amazon OpenSearch Service

Trusted Advisor ha aggiornato il nome dell'Amazon OpenSearch Service Reserved Instance Optimizationassegno l'8 settembre 2021.

I suggerimenti di controllo, la categoria e l'ID sono gli stessi.

Nome di controllo	Categoria di controllo	ID di controllo
Ottimizzazione delle istanze riservate di Amazon OpenSearch Service	Ottimizzazione dei costi	`7ujm6yhn5t`

> **Note**
>
> Se utilizzi Trusted Advisor per i CloudWatch parametri Amazon, viene aggiornato anche il nome della metrica per questo controllo. Per ulteriori informazioni, consulta Creazione di allarmi Amazon CloudWatch per monitorare i parametri AWS Trusted Advisor.

Sono stati aggiunti controlli per l’archiviazione del volume Amazon Elastic Block Store

Trusted Advisor ha aggiunto i seguenti controlli l'8 giugno 2021.

Nome di controllo	Categoria di controllo	ID di controllo
Archiviazione di volumi SSD (gp3) a scopo generico EBS	Limiti del servizio	`dH7RR0l6J3`
Archiviazione di volumi SSD (io2) IOPS con provisioning EBS	Limiti del servizio	`gI7MM0l7J2`

Sono stati aggiunti controlli per AWS Lambda

Trusted Advisor ha aggiunto i seguenti controlli l'8 marzo 2021.

Nome di controllo	Categoria di controllo	ID di controllo
AWS Lambda Funzioni con timeout eccessivi	Ottimizzazione dei costi	`L4dfs2Q3C3`
AWS Lambda Funzioni con tassi di errore elevati	Ottimizzazione dei costi	`L4dfs2Q3C2`
AWS Lambda Funzioni che utilizzano runtime obsoleti	Sicurezza	`L4dfs2Q4C5`
AWS Lambda Funzioni abilitate per VPC senza ridondanza Multi-AZ	Tolleranza ai guasti	`L4dfs2Q4C6`

Per ulteriori informazioni su come utilizzare questi controlli con Lambda, consulta Example AWS Trusted Advisor workflow per visualizzare i consigli nella AWS Lambda Developer Guide.

Trusted Advisor controlla la rimozione

Trusted Advisor ha rimosso il seguente assegno AWS GovCloud (US) Region relativo all'8 marzo 2021.

Nome di controllo	Categoria di controllo	ID di controllo
Indirizzi IP elastici EC2	Limiti del servizio	aW9HH0l8J6

Controlli aggiornati per Amazon Elastic Block Store

Trusted Advisor il 5 marzo 2021 ha aggiornato l'unità del volume Amazon EBS da gibibyte (GiB) a tebibyte (TiB) per i seguenti controlli.

> **Note**
>
> Se utilizzi Trusted Advisor per i CloudWatch parametri Amazon, vengono aggiornati anche i nomi delle metriche per questi cinque controlli. Per ulteriori informazioni, consulta Creazione di allarmi Amazon CloudWatch per monitorare i parametri AWS Trusted Advisor.

Nome di controllo	Categoria di controllo	ID di controllo	Metrica aggiornata a CloudWatch per ServiceLimit
Archiviazione di volumi HDD Cold (sc1) EBS	Limiti del servizio	gH5CC0e3J9	Archiviazione di volumi HDD Cold (sc1) (TiB)
Archiviazione di volumi SSD (gp2) a scopo generico EBS	Limiti del servizio	dH7RR0l6J9	Archiviazione di volumi SSD (gp2) a scopo generico (TiB)
Archiviazioni di volumi magnetici (standard) EBS	Limiti del servizio	cG7HH0l7J9	Archiviazione di volumi magnetici (standard) (TiB)

Nome di controllo	Categoria di controllo	ID di controllo	Metrica aggiornata a CloudWatch per ServiceLimit
Archiviazione di volumi SSD (io1) IOPS con provisioning EBS	Limiti del servizio	`gI7MM0l7J9`	Archiviazione (SSD) IOPS con provisioning (TiB)
Archiviazione di volumi HDD ottimizzati per la velocità effettiva (st1) EBS	Limiti del servizio	`wH7DD0l3J9`	Archiviazione di volumi HDD ottimizzati per la velocità effettiva (st1) (TiB)

Trusted Advisor controlla la rimozione

> **Note**
>
> Trusted Advisor ha rimosso i seguenti controlli il 18 novembre 2020.

Controlli rimossi il 18 novembre 2020	Categoria di controllo	ID di controllo
Servizio EC2Config per istanze di Windows EC2	Tolleranza ai guasti	`V77iOLlBqz`
Versione del driver ENA per istanze di Windows EC2	Tolleranza ai guasti	`TyfdMXG69d`
Versione del driver NVMe per istanze di Windows EC2	Tolleranza ai guasti	`yHAGQJV9K5`
Versione del Driver PV per istanze di Windows EC2	Tolleranza ai guasti	`Wnwm9Il5bG`
Volumi EBS attivi	Limiti del servizio	`fH7LL0l7J9`

Amazon Elastic Block Store non è più caratterizzato da un limite per quanto riguarda il numero di volumi su cui è possibile effettuare il provisioning.

Puoi monitorare le istanze Amazon EC2 e verificare che siano aggiornate utilizzando il AWS Systems Manager Distributor, altri strumenti di terze parti o scrivere script personalizzati per restituire informazioni sui driver per Windows Management Instrumentation, (WMI).

Trusted Advisor verifica la rimozione

Trusted Advisor ha rimosso il seguente controllo il 18 febbraio 2020.

Nome di controllo	Categoria di controllo	ID di controllo
Restrizioni dei servizi	Prestazioni	eW7HH0l7J9

AWS Support App in Slack

Puoi utilizzare l' AWS Support App per gestire i tuoi casi di AWS assistenza in Slack. Invita i membri del tuo team a utilizzare i canali di chat, rispondi agli aggiornamenti dei casi e chatta direttamente con gli agenti dell'assistenza. Usa l' AWS Support app per gestire rapidamente i casi di assistenza in Slack.

Usa l' AWS Support app per effettuare le seguenti operazioni:

- Creazione, aggiornamento, ricerca e risoluzione dei casi di supporto nei canali Slack
- Allegare file ai casi di supporto
- Richiesta di aumenti delle quote da Service Quotas
- Condividi i dettagli del caso di supporto con il tuo team senza uscire dal canale Slack
- Inizia una sessione di live chat con gli agenti dell'assistenza

Quando crei, aggiorni o risolvi un caso di assistenza nell' AWS Support App, il caso viene aggiornato anche in AWS Support Center Console. Non è necessario accedere alla console del Centro assistenza per gestire i casi di supporto separatamente.

> **Note**
>
> - I tempi di risposta per i casi di supporto sono gli stessi, indipendentemente dal fatto che tu abbia creato il caso da Slack o dalla console del Centro assistenza.
> - Puoi creare un caso di supporto in relazione all'account e alla fatturazione, all'aumento della quota di servizio e al supporto tecnico.

Argomenti

- Ricerca di casi di supporto in Slack
- Risoluzione di un caso di supporto in Slack
- Riapertura di un caso di supporto in Slack
- Richiesta di aumenti della quota di servizio
- Eliminazione di una configurazione di canale Slack dall'app AWS Support
- Eliminazione di una configurazione del workspace Slack dall'app AWS Support
- App AWS Support nei comandi Slack
- Visualizzazione delle corrispondenze dell'app AWS Support nella AWS Support Center Console
- Creazione dell'app AWS Support nelle risorse Slack con AWS CloudFormation

Prerequisiti

Per utilizzare l'app AWS Support in Slack è necessario soddisfare i seguenti requisiti:

- Disponi di un piano di supporto Business, Enterprise On-Ramp o Enterprise. Puoi trovare il tuo piano di supporto dalla AWS Support Center Console o dalla pagina Piani di supporto. Per ulteriori informazioni, consulta Confronta piani AWS Support.
- Hai un canale e un workspace Slack per la tua organizzazione. Per aggiungere app a tale workspace è necessario essere un amministratore del workspace Slack o disporre dell'autorizzazione. Per ulteriori informazioni, consulta il Centro assistenza di Slack.
- Accedi all'Account AWS come ruolo o utente AWS Identity and Access Management (IAM) con le autorizzazioni richieste. Per ulteriori informazioni, consulta Gestione degli accessi al widget dell'app AWS Support.
- Dovrai creare un ruolo IAM con le autorizzazioni necessarie per eseguire operazioni al posto tuo. L'app AWS Support utilizza questo ruolo per effettuare chiamate API a servizi diversi. Per ulteriori informazioni, consulta Gestione degli accessi all'app AWS Support.

Argomenti

- Gestione degli accessi al widget dell'app AWS Support
- Gestione degli accessi all'app AWS Support

Gestione degli accessi al widget dell'app AWS Support

Puoi collegare una policy AWS Identity and Access Management (IAM) per concedere a un utente IAM l'autorizzazione necessaria a configurare il widget dell'app AWS Support nella AWS Support Center Console.

Per ulteriori informazioni su come aggiungere una policy a un'entità IAM, consulta la sezione Aggiunta di autorizzazioni alle identità IAM (console) nella Guida per l'utente di IAM.

> **Note**
>
> Puoi anche accedere come utente root dal tuo Account AWS, ma sconsigliamo di eseguire questa operazione. Per ulteriori informazioni sull'accesso degli utenti root, consulta Proteggi le tue credenziali utente root e non usarle per le attività quotidiane nella Guida per l'utente di IAM.

Policy IAM di esempio

È possibile collegare la policy seguente a un'entità, ad esempio un utente o un gruppo IAM. Questa policy consente a un utente di autorizzare un workspace Slack e di configurare i canali Slack nella console del Centro assistenza.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
```

```
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni necessarie per connettere l’App a Slack AWS Support

L’App AWS Support include operazioni di sola autorizzazione che non corrispondono direttamente a un'operazione API. Queste operazioni sono indicate nella Guida di riferimento per l'autorizzazione al servizio con [solo autorizzazione].

L'App AWS Support utilizza le seguenti azioni API per connettersi a Slack e quindi elenca i canali Slack pubblici in AWS Support Center Console:

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

Queste operazioni API non devono essere chiamate dal codice. Di conseguenza, queste operazioni API non sono incluse nella AWS CLI e nei kit SDK di AWS.

Gestione degli accessi all'app AWS Support

Dopo avere ottenuto le autorizzazioni per il widget dell'app AWS Support, è necessario creare anche un ruolo AWS Identity and Access Management (IAM). Questo ruolo esegue operazioni da altri Servizi AWS per tuo conto, come l'API AWS Support e Service Quotas.

Quindi colleghi una policy IAM a questo ruolo in modo che il ruolo disponga delle autorizzazioni necessarie per completare queste operazioni. Scegli questo ruolo quando crei la configurazione del tuo canale Slack nella console del Centro assistenza.

Gli utenti del tuo canale Slack dispongono delle stesse autorizzazioni che concedi al ruolo IAM. Ad esempio, se specifichi l'accesso in sola lettura ai tuoi casi di supporto, gli utenti del tuo canale Slack possono visualizzare i casi ma non possono aggiornarli.

> **Important**
>
> Quando chiedi una chat dal vivo con un agente dell'assistenza e scegli un nuovo canale privato come canale di chat dal vivo, l'app AWS Support crea un canale Slack separato. Questo canale Slack dispone delle stesse autorizzazioni del canale in cui hai creato il caso o avviato la chat.
> Se modifichi il ruolo IAM o la policy IAM, le modifiche si applicano al canale Slack che hai configurato e a qualsiasi nuovo canale Slack di live chat che l'app AWS Support crea per te.

Segui queste procedure per creare il ruolo e la policy IAM.

Argomenti

- Usa una policy gestita da AWS o crea una policy gestita dal cliente
- Creazione di un ruolo IAM
- Risoluzione dei problemi

Usa una policy gestita da AWS o crea una policy gestita dal cliente

Per concedere le autorizzazioni relative al ruolo, puoi utilizzare una policy gestita da AWS o una policy gestita dal cliente.

> **Tip**
>
> Se non desideri creare una policy manualmente, ti consigliamo di utilizzare una policy gestita da AWS e saltare questa procedura. Le policy gestite dispongono automaticamente delle autorizzazioni necessarie per l'app AWS Support. Non è necessario aggiornare le policy manualmente. Per ulteriori informazioni, consulta AWS politiche gestite per AWS Support App in Slack.

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

Come creare una policy gestita dal cliente per l'app AWS Support

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

2. Nel pannello di navigazione, seleziona Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Scegliere la scheda JSON.
5. Inserisci il tuo JSON, quindi sostituisci il JSON predefinito nell'editor. Puoi utilizzare la policy di esempio.
6. Scegli Successivo: Tag.
7. (Facoltativo) Puoi aggiungere metadati alla policy collegando i tag come coppie chiave-valore.
8. Seleziona Next: Revisione.
9. Nella pagina Review policy (Rivedi policy), immetti un Name (Nome), ad esempio *AWSSupportAppRolePolicy*, e una Description (Descrizione) facoltativa.
10. Rivedi la pagina Summary (Riepilogo) per controllare le autorizzazioni concesse dalla policy, quindi seleziona Create policy (Crea policy).

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.

Policy IAM di esempio

Puoi collegare al tuo ruolo IAM la seguente policy di esempio. Questa policy concede al ruolo autorizzazioni complete per tutte le operazioni richieste per l'app AWS Support. Dopo aver configurato un canale Slack con il ruolo, qualsiasi utente del tuo canale dispone delle stesse autorizzazioni.

> **Note**
>
> Per un elenco delle policy gestite da AWS, consulta la pagina AWS politiche gestite per AWS Support App in Slack.

Puoi aggiornare la policy per rimuovere un'autorizzazione dall'app AWS Support.

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

```
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Per le descrizioni di ciascuna operazione, consulta i seguenti argomenti nella documentazione di riferimento sulle autorizzazioni dei servizi:

- Operazioni, risorse e chiavi di condizione per AWS Support
- Operazioni, risorse e chiavi di condizione per Service Quotas
- Operazioni, risorse e chiavi di condizione per AWS Identity and Access Management

Creazione di un ruolo IAM

Dopo avere creato la policy, devi creare un ruolo IAM e collegare la policy a tale ruolo. Scegli questo ruolo quando crei una configurazione del canale Slack nella console del Centro assistenza.

Come creare un ruolo per l'app AWS Support

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. In Select trusted entity (Seleziona entità attendibile), scegli Servizio AWS.
4. Seleziona l'app AWS Support.
5. Scegliere Successivo: Autorizzazioni.
6. Inserisci il nome della policy. Puoi scegliere la policy gestita da AWS o una policy gestita dal cliente che hai creato, ad esempio *AWSSupportAppRolePolicy*. Dopodiché, seleziona la casella di controllo accanto alla policy.
7. Scegli Successivo: Tag.
8. (Facoltativo) Puoi aggiungere metadati al ruolo collegando i tag come coppie chiave-valore.
9. Seleziona Next: Revisione.
10. In Role name (Nome ruolo), digita un nome, come *AWSSupportAppRole*.
11. (Facoltativo) In Role description (Descrizione ruolo), immettere una descrizione per il nuovo ruolo.
12. Rivedere il ruolo e scegliere Crea ruolo. Ora puoi scegliere questo ruolo quando configuri un canale Slack nella console del Centro assistenza. Per informazioni, consultare Configurazione di un canale Slack.

Per ulteriori informazioni, consulta la pagina Creazione di un ruolo per un servizio AWS nella Guida per l'utente di IAM.

Risoluzione dei problemi

Consulta i seguenti argomenti per gestire l'accesso all'app AWS Support.

Indice

Desidero limitare determinate operazioni a utenti specifici del mio canale Slack

Per impostazione predefinita, gli utenti del tuo canale Slack dispongono delle stesse autorizzazioni specificate nella policy IAM che colleghi al ruolo IAM che crei. Ciò significa che chiunque si trovi nel canale dispone dell'accesso in lettura o in scrittura ai tuoi casi di supporto, indipendentemente dal fatto che abbia o meno un Account AWS o sia un utente IAM.

È preferibile seguire le best practice seguenti:

- Configurare i canali Slack come privati con l'app AWS Support
- Invitare al canale solo gli utenti che hanno effettivo bisogno di accedere ai casi di supporto
- Utilizzare una policy IAM con le autorizzazioni minime richieste per l'app AWS Support. Per informazioni, consultare AWS politiche gestite per AWS Support App in Slack.

Quando configuro un canale Slack, non vedo il ruolo IAM che ho creato

Se il tuo ruolo IAM non compare nell'elenco dei ruoli IAM per l'app AWS Support, significa che il ruolo non ha impostato l'app AWS Support come entità attendibile o che il ruolo è stato eliminato. Puoi aggiornare il ruolo esistente oppure crearne un altro. Per informazioni, consultare Creazione di un ruolo IAM.

Al mio ruolo IAM manca un'autorizzazione

Il ruolo IAM che crei per il tuo canale Slack deve disporre delle autorizzazioni per eseguire le operazioni che ti interessano. Ad esempio, se desideri che i tuoi utenti in Slack creino casi di supporto, il ruolo deve disporre dell'autorizzazione `support:CreateCase`. L'app AWS Support assume questo ruolo per eseguire queste operazioni per tuo conto.

Se viene visualizzato un errore relativo a un'autorizzazione mancante dall'app AWS Support, verifica che la policy collegata al tuo ruolo disponga dell'autorizzazione richiesta.

Consulta la Policy IAM di esempio precedente.

Un errore di Slack segnala che il mio ruolo IAM non è valido

Verifica di avere scelto il ruolo corretto per la configurazione del canale.

Come verificare il ruolo

1. Accedi a AWS Support Center Console alla pagina https://console.aws.amazon.com/support/app#/config.

2. Scegli il canale che hai configurato con l'app AWS Support.
3. Nella sezione Permissions (Autorizzazioni), trova il nome del ruolo IAM che hai scelto.
   - Per cambiare il ruolo, scegli Edit (Modifica), seleziona un altro ruolo e scegli Save (Salva).
   - Per aggiornare il ruolo o la policy collegata al ruolo, accedi alla Console IAM.

L'app AWS Support segnala l'assenza di un ruolo IAM per Service Quotas

È necessario che l'account disponga del ruolo `AWSServiceRoleForServiceQuotas` per richiedere aumenti delle quote da Service Quotas. Se ricevi un errore relativo a una risorsa mancante, completa uno dei seguenti passaggi:

- Per richiedere l'aumento di una quota, è possibile utilizzare la console Service Quotas. Quando inoltri correttamente una richiesta, Service Quotas crea automaticamente questo ruolo. Dopodiché, puoi utilizzare l'app AWS Support per richiedere aumenti delle quote in Slack. Per ulteriori informazioni, consulta la sezione Richiesta di un aumento di quota.
- Aggiorna la policy IAM collegata al tuo ruolo. In questo modo, al ruolo viene concessa l'autorizzazione per accedere a Service Quotas. La sezione seguente (Policy IAM di esempio) autorizza l'app AWS Support a creare il ruolo Service Quotas per l'utente.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

Se elimini il ruolo IAM che configuri per il tuo canale, devi creare manualmente il ruolo o aggiornare la policy IAM per autorizzare l'app AWS Support a crearne uno per te.

Autorizzazione di un workspace Slack

Dopo avere autorizzato il tuo workspace e avere fornito all'app AWS Support l'autorizzazione per accedervi, hai bisogno di un ruolo AWS Identity and Access Management (IAM) per il tuo Account AWS. L'app AWS Support utilizza questo ruolo per chiamare le operazioni API da AWS Support

e Service Quotas per tuo conto. Ad esempio, l'app AWS Support utilizza il ruolo per chiamare l'operazione `CreateCase` per creare un caso di supporto per tuo conto in Slack.

> **Note**
>
> - Il canale Slack eredita le autorizzazioni dal ruolo IAM. Ciò significa che qualsiasi utente nel canale Slack dispone delle stesse autorizzazioni specificate nella policy IAM collegata al ruolo.
>
> Ad esempio, se la tua policy IAM concede al ruolo autorizzazioni complete di lettura e scrittura per i tuoi casi di supporto, chiunque si trovi nel tuo canale Slack può creare, aggiornare e risolvere i tuoi casi di supporto. Se la tua policy IAM concede al ruolo autorizzazioni di sola lettura, gli utenti del tuo canale Slack dispongono soltanto delle autorizzazioni di lettura per i tuoi casi di supporto.
> - Ti consigliamo di aggiungere i workspace e i canali Slack necessari per gestire le operazioni di supporto. Ti consigliamo di configurare i canali come privati e di invitare solo gli utenti necessari.

È necessario autorizzare ogni workspace Slack che desideri utilizzare per il tuo Account AWS. Se gli Account AWS sono molteplici, è necessario accedere a ciascun account e ripetere la procedura seguente per autorizzare il workspace. Se il tuo account appartiene a un'organizzazione in AWS Organizations e desideri autorizzare più account, vai a Autorizzazione di più account.

Come autorizzare il workspace Slack per il tuo Account AWS

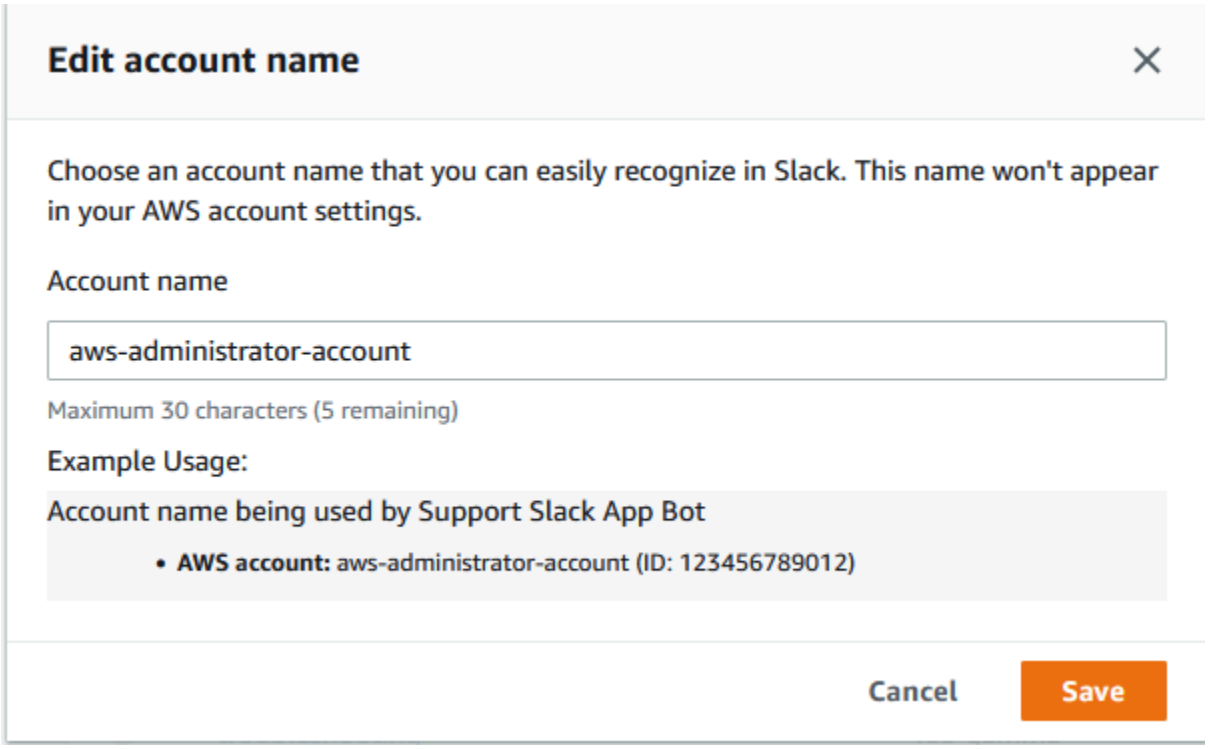
1. Accedi alla AWS Support Center Console e scegli Slack configuration (Configurazione di Slack).
2. Nella pagina Getting started (Nozioni di base), scegli Authorize workspace (Autorizza Workspace).
3. Se non hai ancora effettuato l'accesso a Slack, nella pagina Sign in to your workspace (Accedi al tuo workspace), inserisci il nome del workspace e seleziona Continue (Continua).
4. Nella pagina AWS Support is requesting permission to access the your-workspace-name Slack (richiede l'autorizzazione per accedere al tuo workspace Slack), scegli Allow. (Consenti).

> **Note**
>
> Se non riesci ad autorizzare Slack ad accedere al tuo workspace, assicurati di possedere le autorizzazioni fornite dall'amministratore Slack per aggiungere l'app AWS Support al workspace. Per informazioni, consultare Prerequisiti.

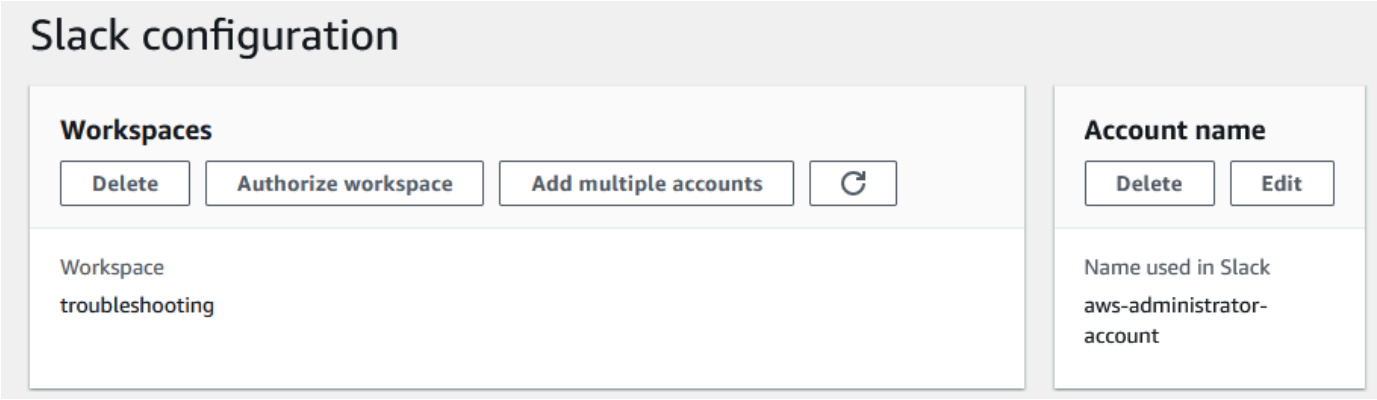
Nella pagina Slack configuration (Configurazione di Slack), il nome del tuo workspace appare nella sezione Workspaces (Workspace).

5. (Facoltativo) Per aggiungere altri workspace, scegli Authorize workspace (Autorizza Workspace) e ripeti i passaggi da 3 a 4. Puoi aggiungere fino a cinque workspace al tuo account.
6. (Facoltativo) Per impostazione predefinita, il numero ID del tuo Account AWS viene visualizzato come nome dell'account nel tuo canale Slack. Per modificare questo valore, alla voce Account name (Nome dell'account), scegli Edit (Modifica), immetti il nome dell'account e scegli Save (Salva).

> **Tip**
>
> Usa un nome che tu e il tuo team possiate riconoscere facilmente. L'app AWS Support utilizza questo nome per identificare il tuo account nel canale Slack. Puoi aggiornare questo nome in qualsiasi momento.



Il nome del workspace e dell'account vengono visualizzati nella pagina Slack configuration (Configurazione di Slack).



Autorizzazione di più account

Per autorizzare più Account AWS a utilizzare workspace di Slack, puoi usare AWS CloudFormation o Terraform e creare le tue risorse dell'app AWS Support.

Configurazione di un canale Slack

Dopo aver autorizzato il tuo workspace Slack, puoi configurare i tuoi canali Slack affinché utilizzino l'app AWS Support.

Il canale in cui inviti e aggiungi l'app AWS Support è dove puoi creare e cercare casi e ricevere notifiche sui casi. Questo canale mostra gli aggiornamenti dei casi (come i casi appena creati o risolti), le corrispondenze aggiunte e i dettagli dei casi condivisi.

Il canale Slack eredita le autorizzazioni dal ruolo IAM. Ciò significa che qualsiasi utente nel canale Slack dispone delle stesse autorizzazioni specificate nella policy IAM collegata al ruolo.

Ad esempio, se la tua policy IAM concede al ruolo autorizzazioni complete di lettura e scrittura per i tuoi casi di supporto, chiunque si trovi nel tuo canale Slack può creare, aggiornare e risolvere i tuoi casi di supporto. Se la tua policy IAM concede al ruolo autorizzazioni di sola lettura, gli utenti del tuo canale Slack dispongono soltanto delle autorizzazioni di lettura per i tuoi casi di supporto.

Puoi aggiungere fino a 20 canali per un account. Un canale Slack può avere fino a 100 Account AWS. Ciò significa che solo 100 account possono aggiungere lo stesso canale Slack all'app AWS Support. Ti consigliamo di aggiungere solo gli account necessari per gestire i casi di supporto per la tua organizzazione. Questo può ridurre il numero di notifiche che ricevi nel canale, e di conseguenza le distrazioni per te e il tuo team.

Ciascun Account AWS deve configurare separatamente un canale Slack nell'app AWS Support. In questo modo, l'app AWS Support può accedere ai casi di supporto in tale Account AWS. Se un altro Account AWS nella tua organizzazione ha già invitato l'app AWS Support in quel canale Slack, salta al passaggio 3.

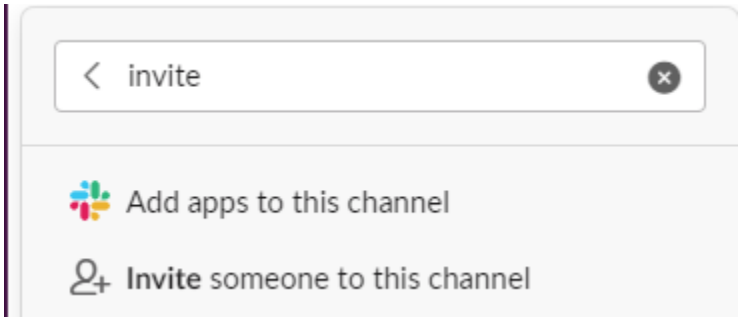
> **Note**
>
> Puoi configurare i canali che fanno parte di Slack Connect e i canali condivisi con più workspace. Tuttavia, solo il primo workspace che ha configurato il canale condiviso per un Account AWS può utilizzare l'app AWS Support. L'app AWS Support restituisce un messaggio di errore se provi a configurare lo stesso canale Slack per un altro workspace.

Come configurare un canale Slack

1. Dalla tua applicazione Slack, scegli il canale Slack che desideri utilizzare con l'app AWS Support.

2. Completa i seguenti passaggi per invitare l'app AWS Support al tuo canale:

   a. Scegli l'icona + e inserisci `invite`, poi, quando richiesto, seleziona Add apps to this channel (Aggiungi app a questo canale).

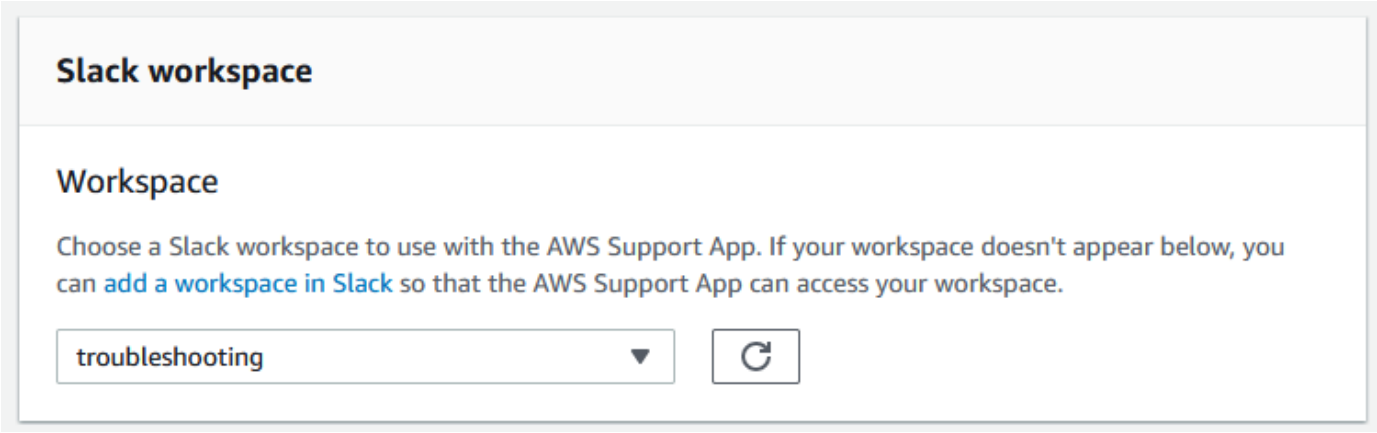
   

   b. Per cercare l'app, in Add apps to channelName (Aggiungi le app a channelName) inserisci App AWS Support.

   c. Scegli Add (Aggiungi) accanto ad AWS Support App.

3. Accedi alla console del Centro assistenza e scegli Slack configuration (Configurazione di Slack).
4. Scegli Add channel (Aggiungi canale).
5. Nella pagina Add channel (Aggiungi canale), in Workspace, scegli il nome del workspace precedentemente autorizzato. Se il nome del workspace non viene visualizzato nell'elenco, puoi scegliere l'icona di aggiornamento.

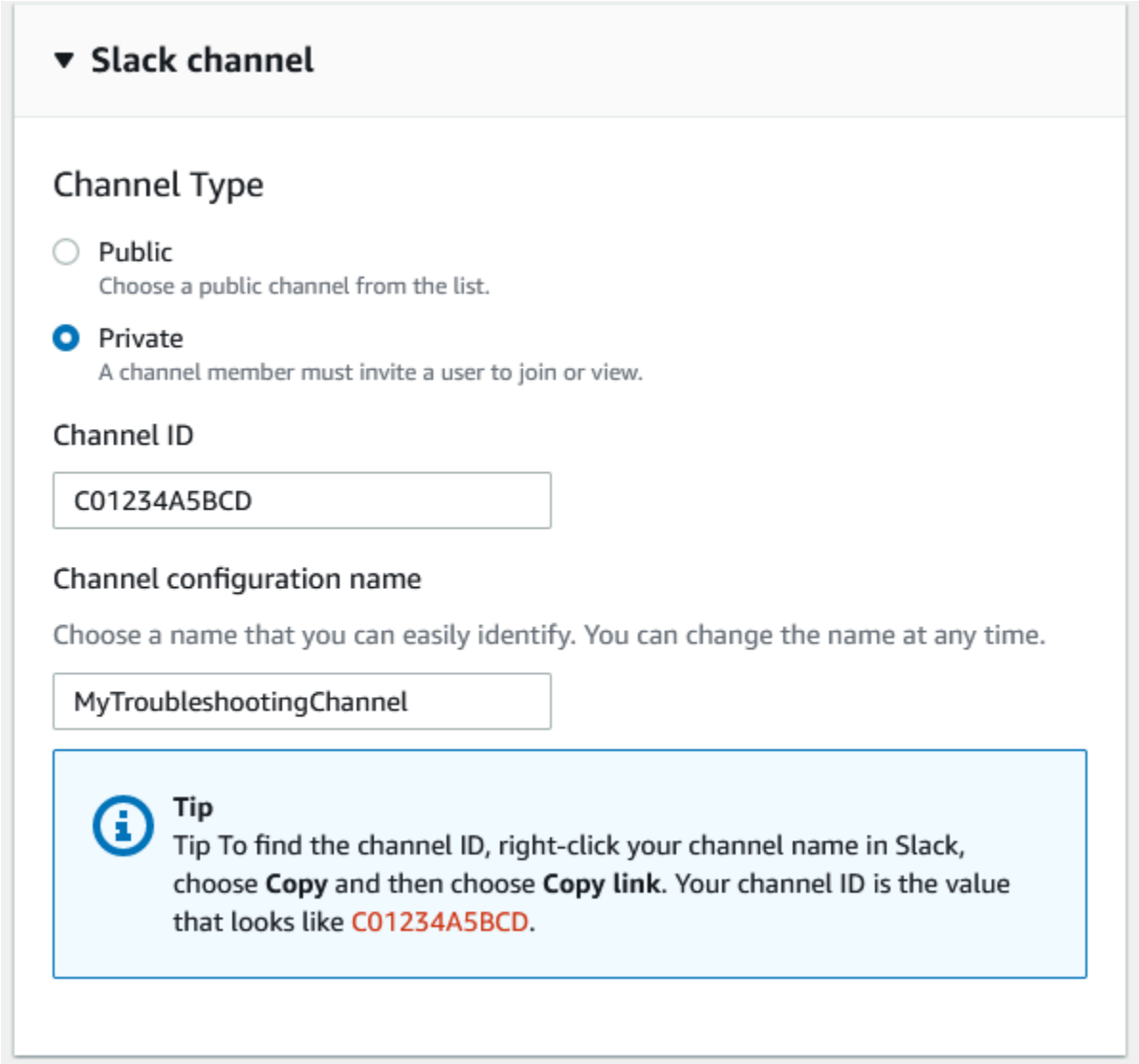
6. In Slack channel (Canale Slack), per Channel type (Tipo di canale) scegli una delle seguenti opzioni:

- Public (Pubblico): in Public channel (Canale pubblico), scegli il canale Slack al quale hai invitato l'app AWS Support (passaggio 2). Se il tuo canale non compare nell'elenco, scegli l'icona di aggiornamento e riprova.
- Private (Privato): in Channel ID (ID canale), inserisci l'ID o l'URL del canale Slack al quale hai invitato l'app AWS Support.

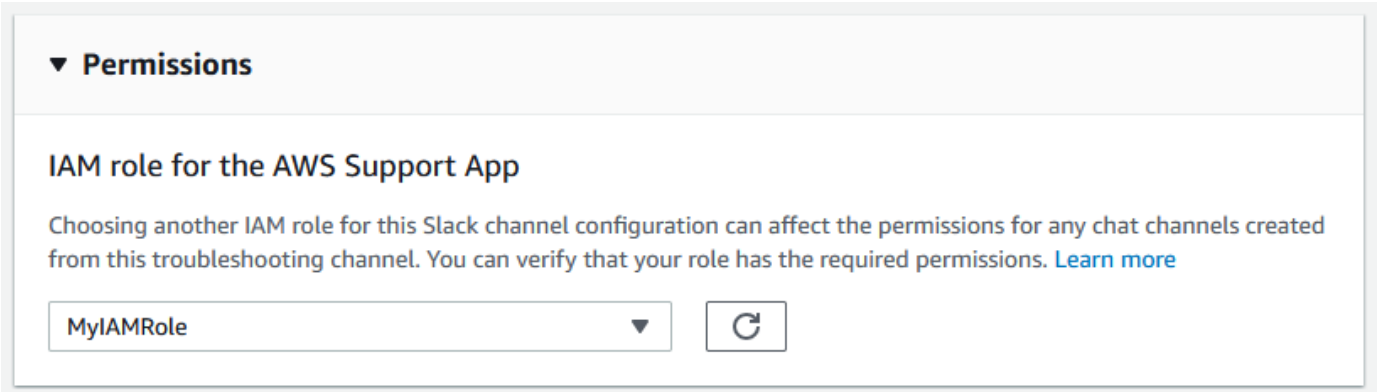
> **Tip**
>
> Per trovare l'ID del canale, apri il menu contestuale (facendo clic con il pulsante destro del mouse) del nome del canale in Slack, quindi scegli Copy (Copia) e Copy link (Copia collegamento). L'ID del canale è un valore del tipo *C01234A5BCD*.

7. In Channel configuration name (Nome della configurazione del canale), inserisci un nome che identifichi facilmente la configurazione del tuo canale Slack per l'app AWS Support. Questo nome appare solo nel tuo Account AWS e non viene visualizzato in Slack. Puoi rinominare la configurazione del canale in un secondo momento.

   Il tipo di canale Slack potrebbe essere simile al seguente esempio.



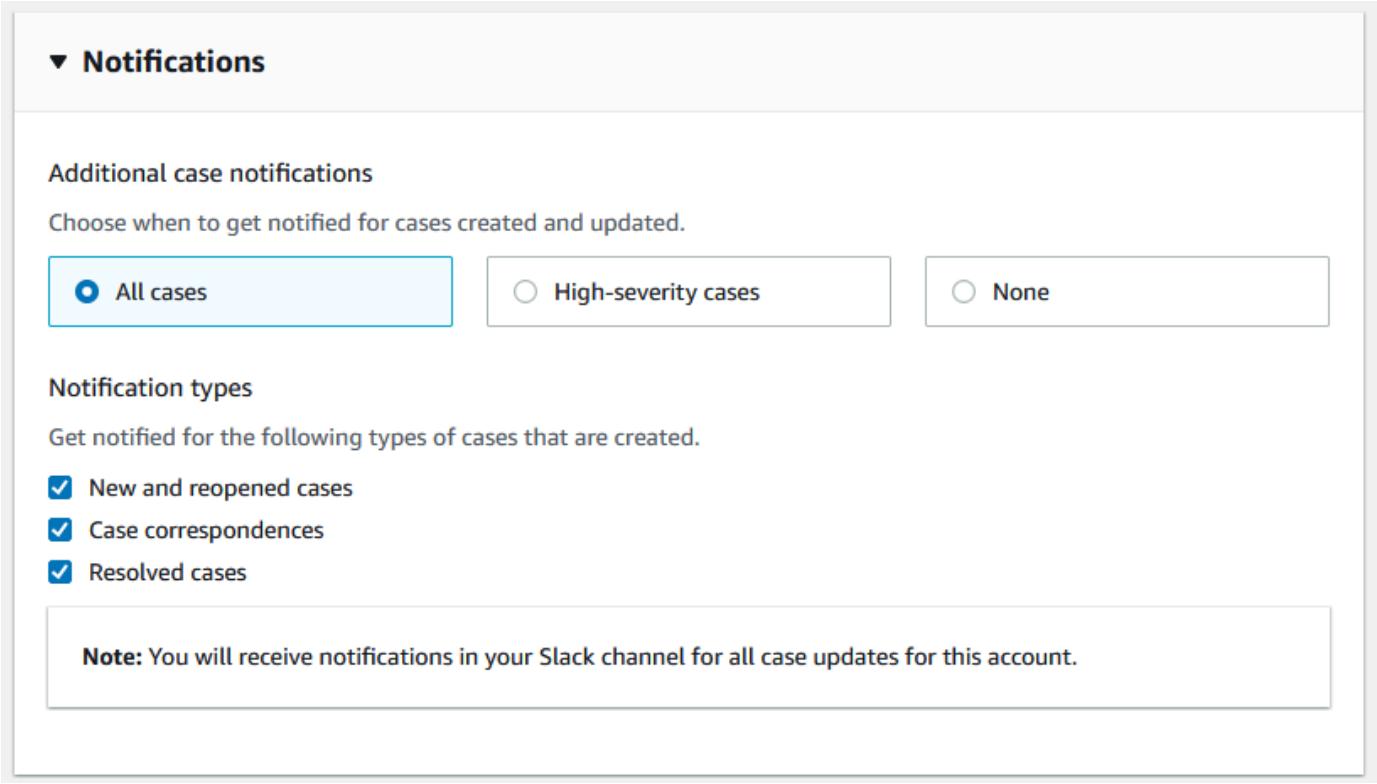
8. In Autorizzazioni, per Ruolo IAM per l'app AWS Support in Slack, scegli un ruolo che hai creato per l'app AWS Support. Solo i ruoli che dispongono dell'app AWS Support come entità attendibile appaiono nell'elenco.



> **Note**
>
> Se non hai creato un ruolo o non lo vedi nell'elenco, consulta la pagina Gestione degli accessi all'app AWS Support.

9. In Notifications (Notifiche), specifica come ricevere una notifica per i casi.
   - All cases (Tutti i casi): ricevi una notifica per tutti gli aggiornamenti dei casi.
   - High-severity cases (Casi di elevata gravità): ricevi una notifica solo per i casi che riguardano un sistema di produzione o superiore. Per ulteriori informazioni, consulta la pagina Scelta del livello di gravità.
   - None (Nessuna): non riceverai notifiche per gli aggiornamenti dei casi.
10. (Facoltativo) Se scegli All cases (Tutti i casi) o High-severity cases (Casi di elevata gravità), è necessario selezionare almeno una delle seguenti opzioni:
    - New and reopened cases (Casi nuovi e riaperti)
    - Case correspondences (Corrispondenze di casi)
    - Resolved cases (Casi risolti)

    Il seguente canale riceve notifiche di casi per tutti gli aggiornamenti dei casi in Slack.



11. Controlla la tua configurazione e scegli Add channel (Aggiungi canale). Il tuo canale viene visualizzato nella pagina Slack configuration (Configurazione Slack).

Aggiorna la configurazione del tuo canale Slack

Dopo avere configurato il canale Slack, puoi aggiornarlo in un secondo momento per modificare il ruolo IAM o le notifiche sui casi.

Come aggiornare la configurazione del tuo canale Slack

1. Accedi alla console del Centro assistenza e scegli Slack configuration (Configurazione di Slack).
2. In Channels (Canali), scegli la configurazione del canale che desideri.
3. Nella pagina ***channelName***, puoi eseguire le seguenti operazioni:
   - Scegli Rename (Rinomina) per aggiornare il nome della configurazione del canale. Questo nome appare solo nel tuo Account AWS e non in Slack.
   - Scegli Delete (Elimina) per eliminare la configurazione del canale dall'app AWS Support. Consulta Eliminazione di una configurazione di canale Slack dall'app AWS Support.
   - Scegli Open in Slack (Apri in Slack) per aprire il canale Slack nel tuo browser.
   - Scegli Edit (Modifica) per modificare il ruolo IAM o le notifiche.

Creazione di casi di supporto in un canale Slack

Dopo avere autorizzato il tuo workspace Slack e aggiunto il tuo canale Slack, puoi creare un caso di supporto nel tuo canale Slack.

Come creare un caso di supporto in Slack

1. Nel tuo canale Slack, inserisci il comando seguente:

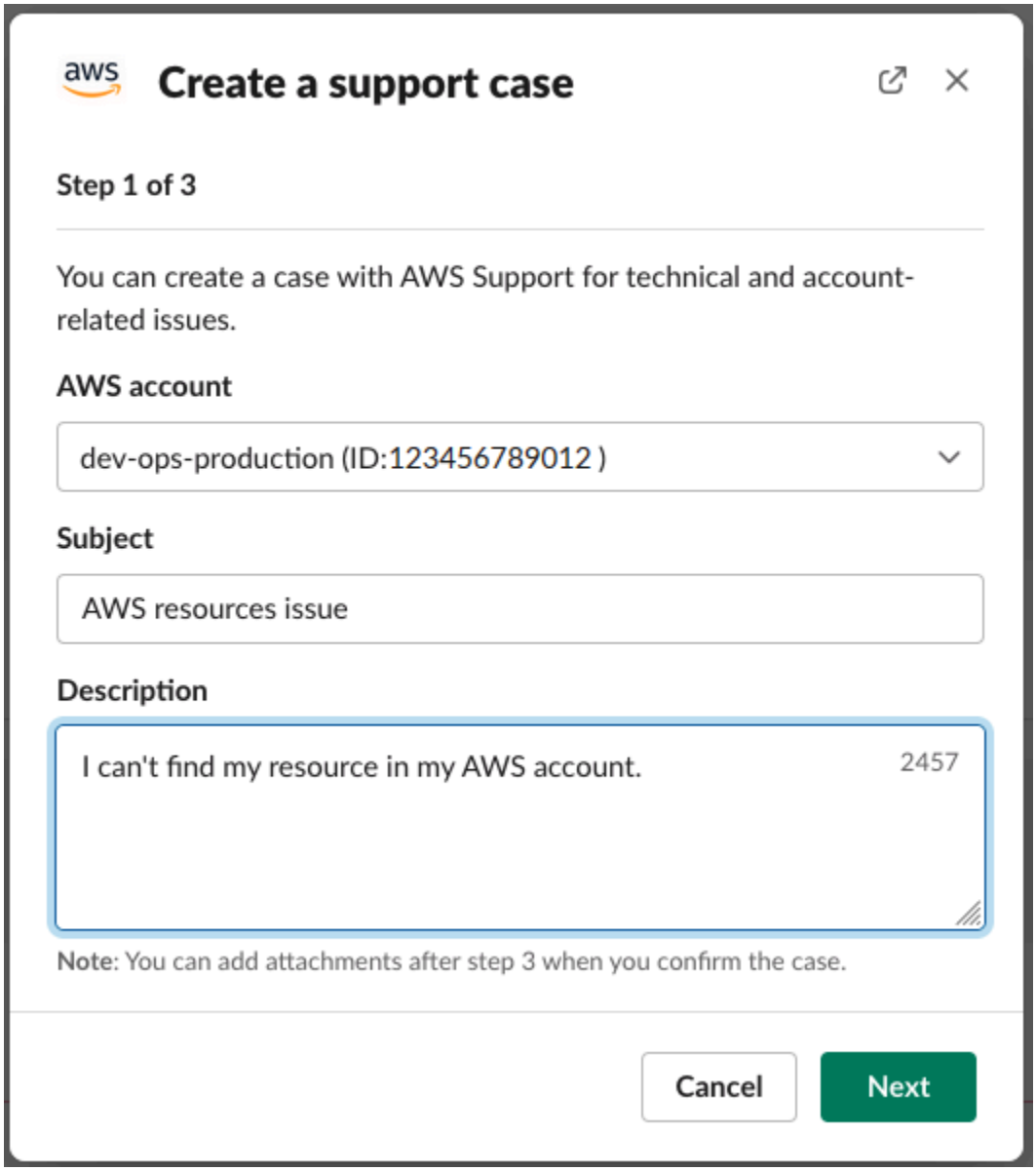
   ```
   /awssupport create
   ```

2. Nella finestra di dialogo Create a support case (Crea un caso di supporto), segui questi passaggi:

   a. Se hai configurato più di un account per questo canale Slack, in Account AWS scegli l'ID dell'account. Se hai creato un nome account, questo valore viene visualizzato accanto all'ID dell'account. Per ulteriori informazioni, consulta Autorizzazione di un workspace Slack.

   b. In Subject (Oggetto), inserisci un titolo per il caso di supporto.

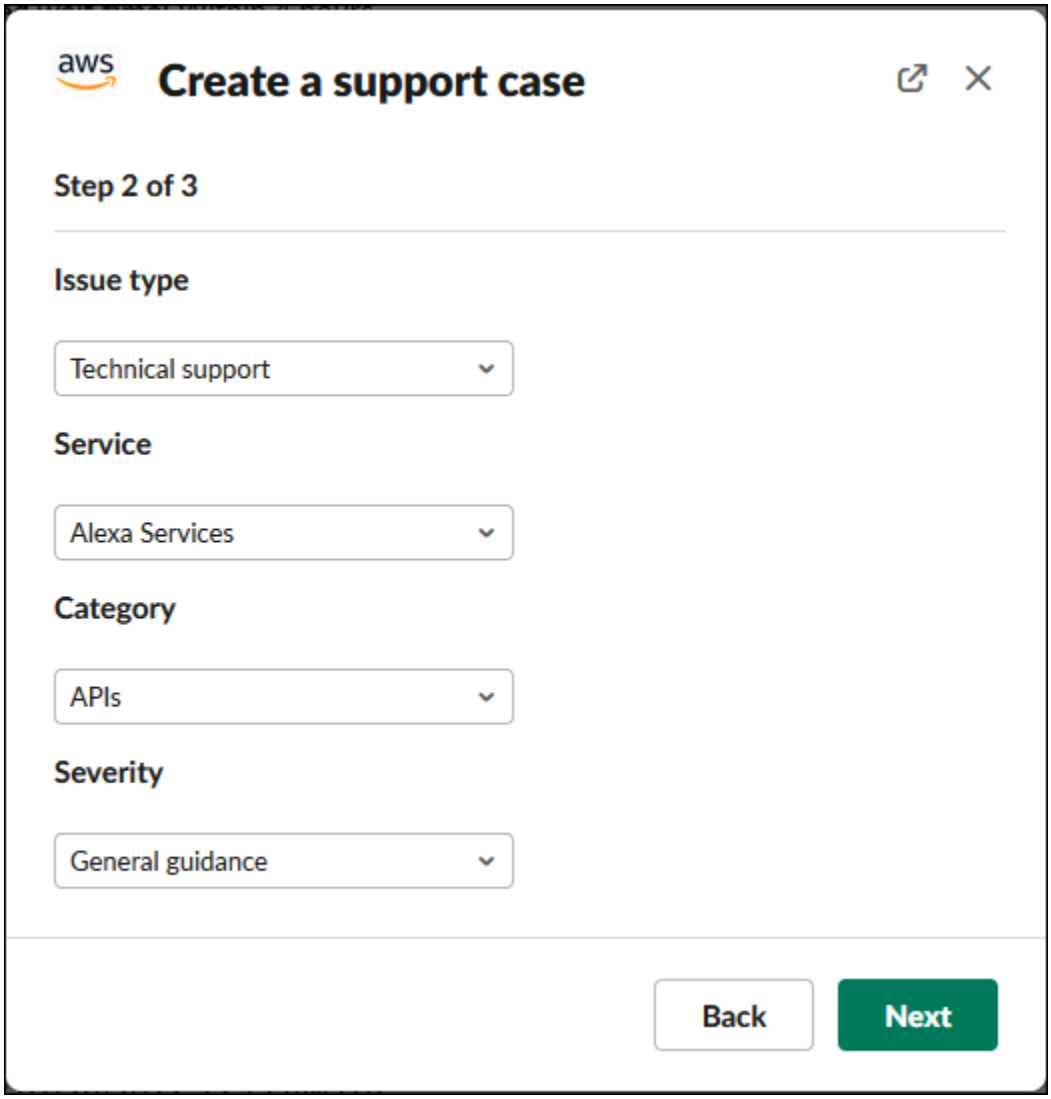
   c. In Case description (Descrizione del caso), descrivi il caso di supporto. Fornisci dettagli sull'utilizzo di Servizio AWS e su quali procedure di risoluzione dei problemi hai effettuato.



3. Seleziona Successivo.
4. Nella finestra di dialogo Create a support case (Crea un caso di supporto), specifica le opzioni seguenti:

   a. Scegli un valore per Issue type (Tipo di problema).
   b. Scegli un valore per Service (Servizio).
   c. Scegli un valore per Category (Categoria).
   d. Scegli un valore per Severity (Gravità).
   e. Rivedi i dettagli del caso e seleziona Next (Avanti).

   L'esempio seguente mostra un caso di supporto tecnico per i servizi Alexa.

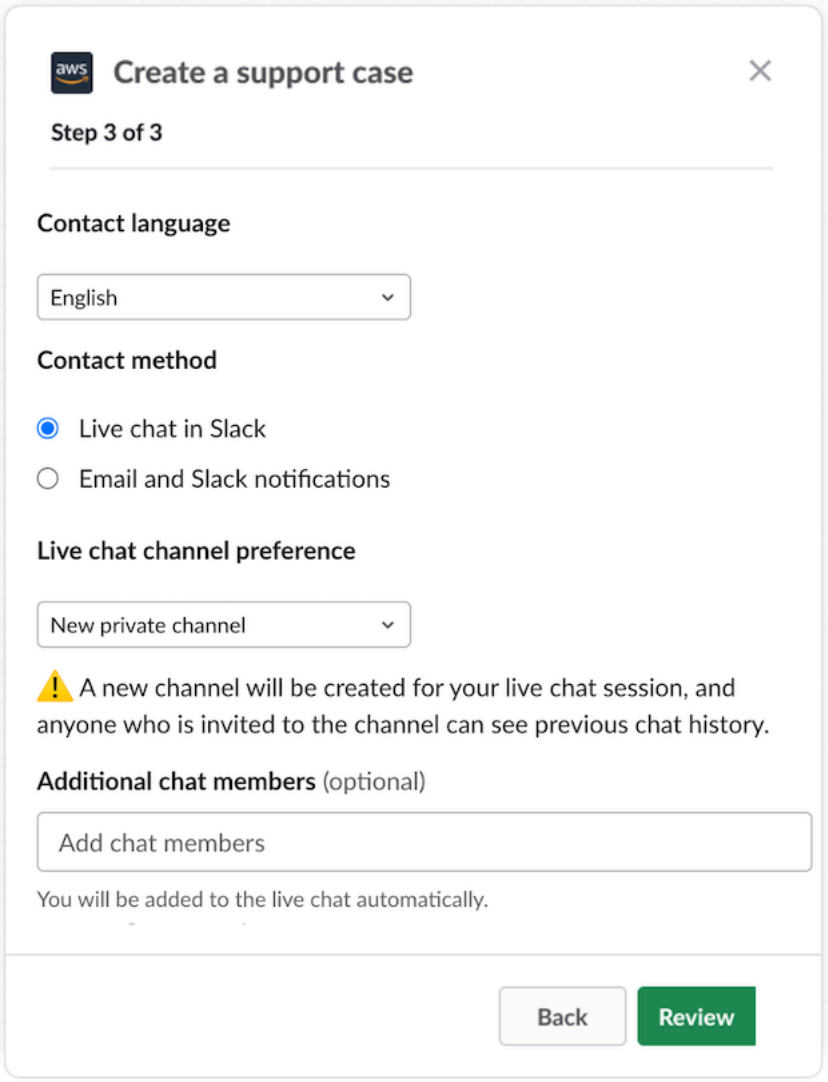


5. Per Contact language (Lingua di contatto) scegli la lingua preferita per il caso di supporto.

> **Note**
>
> Il supporto in lingua giapponese non è disponibile per la chat dal vivo in Slack per i casi relativi ad account e fatturazione.

6. Come Contact method (Metodo di contatto), scegli Email and Slack notifications (Notifiche via e-mail e Slack) o Live chat in Slack.

   L'esempio seguente mostra come scegliere una chat dal vivo in Slack.



a. Se scegli Chat dal vivo in Slack, seleziona Nuovo canale privato o Canale attuale come Preferenza di canale per chat dal vivo. Il Nuovo canale privato creerà un canale privato separato per chattare con l'agente AWS Support, mentre il Canale attuale utilizzerà un thread nel canale attuale per consentirti di chattare con l'agente AWS Support.

b. (Facoltativo) Se scegli Live chat in Slack, puoi inserire i nomi degli altri membri di Slack. Per Nuovo canale privato, l'app AWS Support aggiungerà automaticamente te e i membri selezionati al nuovo canale. Per il Canale attual, l'app AWS Support taggherà automaticamente te e i membri selezionati nel thread della chat quando l'agente AWS Support si unisce.

> **Important**
>
> - È preferibile aggiungere solo i membri della chat che devono accedere ai dettagli del tuo caso di supporto e alla cronologia della chat.
> - Se avvii una nuova sessione di chat dal vivo per un caso di supporto esistente, l'app AWS Support utilizza lo stesso canale o thread di chat utilizzato per una precedente chat dal vivo. L'app AWS Support utilizza anche la stessa preferenza di canale di chat dal vivo utilizzata in precedenza.
> - L'opzione Canale attuale è disponibile solo se la chat viene richiesta da un canale privato. È preferibile utilizzare questa opzione solo se tutti i membri di un canale devono accedere alla tua chat.

7. (Facoltativo) Per Additional contacts to notify (Altri contatti da informare), inserisci gli indirizzi e-mail per ricevere anche gli aggiornamenti su questo caso di supporto. Puoi aggiungere fino a 10 indirizzi e-mail.
8. Scegliere Review (Rivedi).
9. Nel canale Slack puoi esaminare i dettagli del caso. Puoi eseguire le operazioni indicate di seguito:
   - Scegli Edit (Modifica) per modificare i dettagli del caso.
   - Aggiungi un file al tuo caso. A tale scopo, procedi nel seguente modo:
     a. Scegli Attach file (Allega file), seleziona l'icona + in Slack e scegli Your computer (Il tuo computer).
     b. Individua e scegli il tuo file.
     c. Nella finestra di dialogo Upload a file (Carica un file), inserisci `@awssupport` e seleziona l'icona

        per l'invio del messaggio.

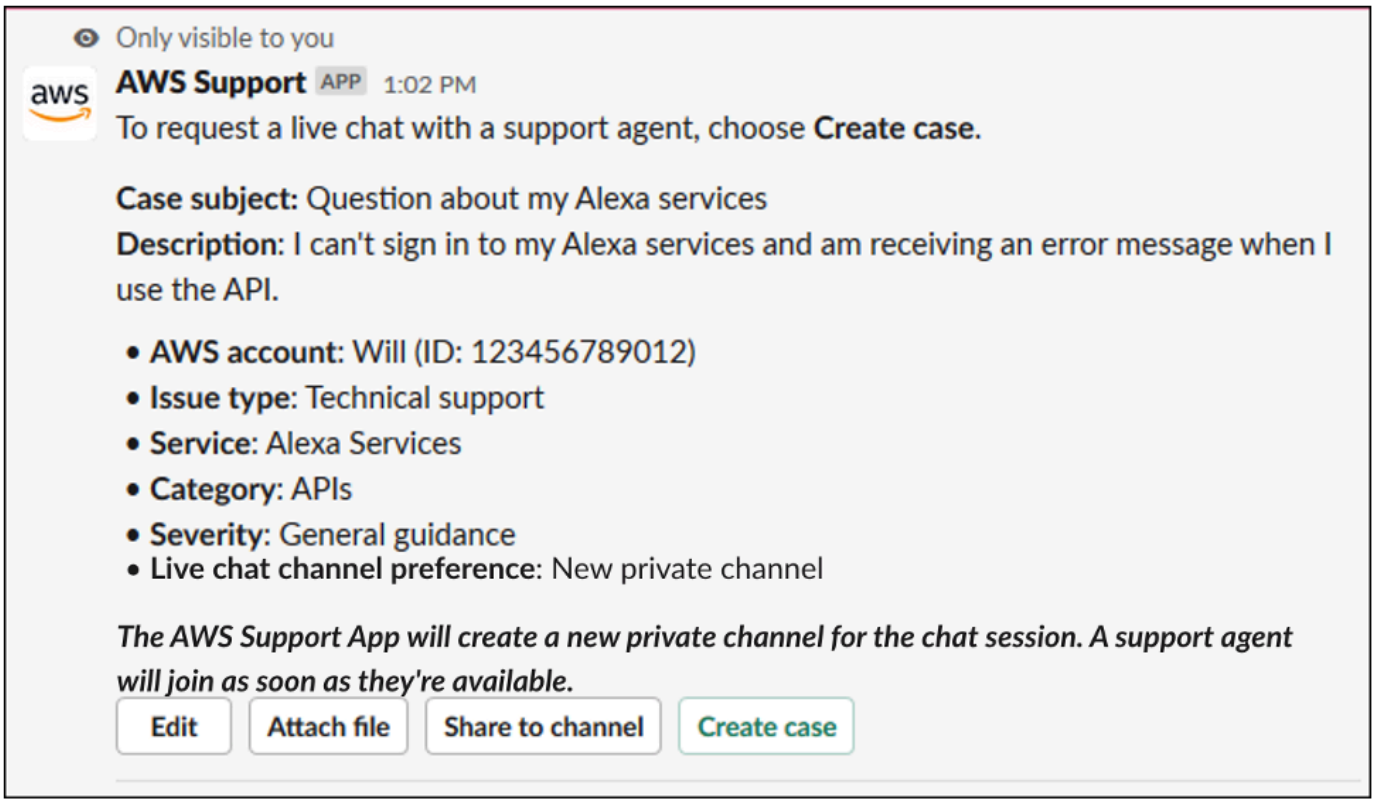
> **Note**
>
> - Puoi allegare fino a tre file. Ogni file può essere fino a 5 MB.

- Se si allega un file al caso di supporto, è necessario inviare il caso entro 1 ora. In caso contrario, è necessario aggiungere nuovamente i file.

- Scegli Share to channel (Condividi con canale) per condividere i dettagli del caso con altri utenti del canale Slack. Puoi utilizzare questa opzione per condividere i dettagli del caso con il tuo team prima di creare il caso.

10. Esamina i dettagli del caso e scegli Create case (Crea caso).

    L'esempio seguente mostra un caso di supporto tecnico per i servizi Alexa.



    Dopo aver creato un caso di supporto, potrebbero essere necessari alcuni minuti prima che i dettagli del caso diventino visibili.

11. Quando il caso di supporto viene aggiornato, puoi selezionare See details (Vedi i dettagli) per visualizzare le informazioni sul caso. A questo punto puoi effettuare le seguenti operazioni:

    - Scegli Share to channel (Condividi con canale) per condividere i dettagli del caso con altri utenti del canale Slack.
    - Scegli Reply (Rispondi) per aggiungere una corrispondenza.
    - Seleziona Risolvi caso.

> **Note**
>
> Se non hai scelto di ricevere aggiornamenti automatici sul caso in Slack, puoi cercare il caso di supporto per consultare l'opzione See details (Vedi i dettagli).

Risposta ai casi di supporto in Slack

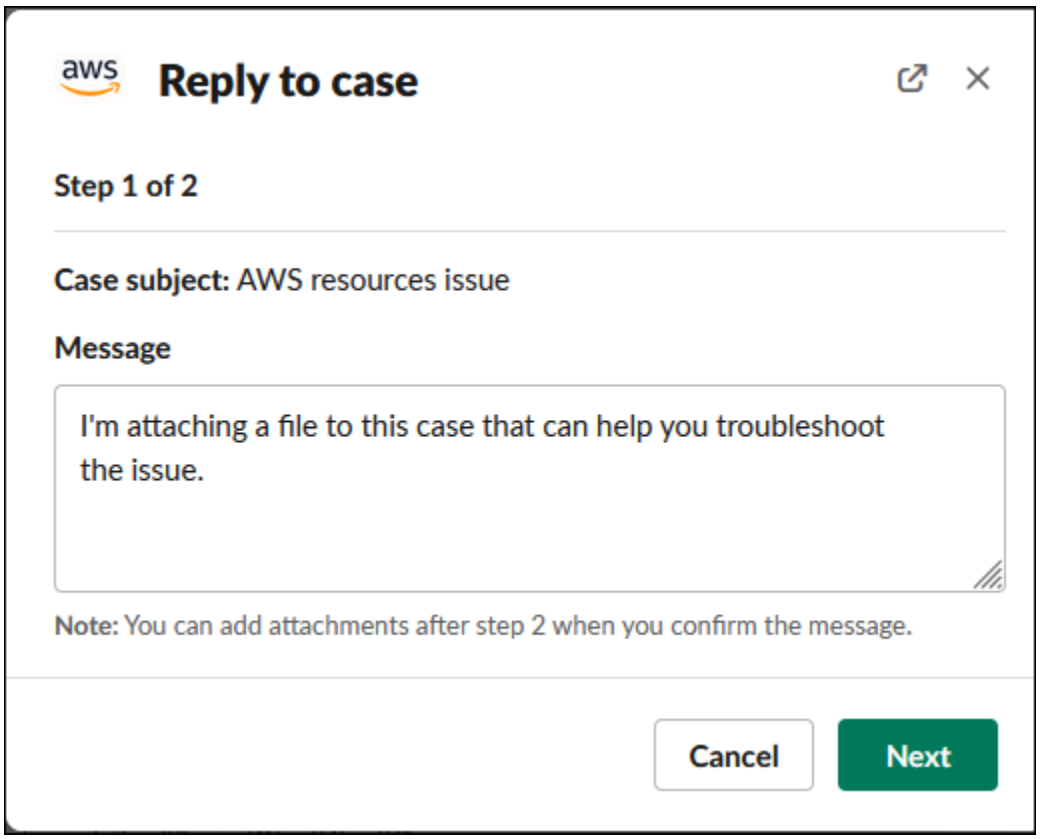
Puoi aggiungere aggiornamenti al tuo caso, ad esempio dettagli e collegamenti del caso, e rispondere alle risposte dell'agente di supporto.

> **Note**
>
> - Puoi anche utilizzare la AWS Support Center Console per rispondere agli agenti di supporto. Per ulteriori informazioni, consulta Aggiornamento, risoluzione e riapertura del caso.
> - Non puoi aggiungere corrispondenze ai casi dai canali di chat creati dall'app AWS Support. I canali di live chat inviano messaggi agli agenti solo durante la live chat.

Come rispondere a un caso di supporto in Slack

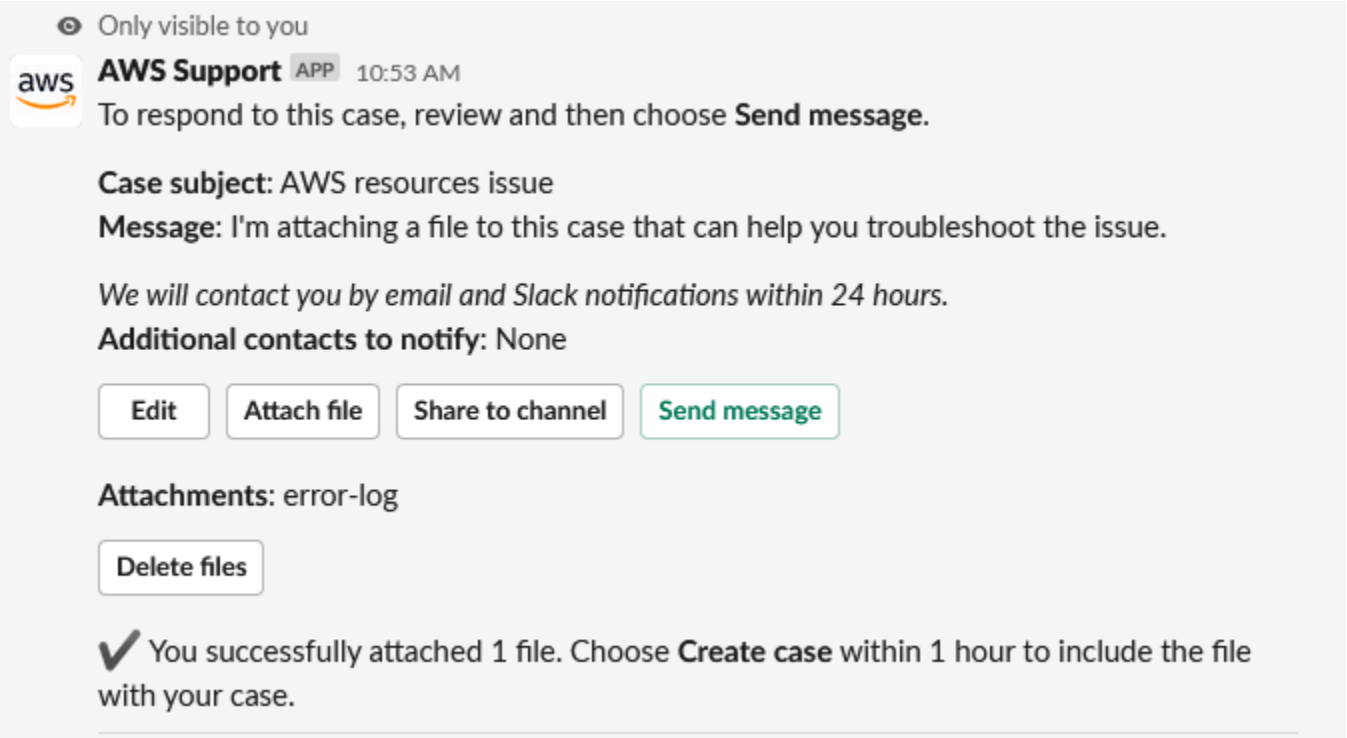
1. Nel tuo canale Slack, scegli il caso al quale desideri rispondere. Puoi inserire `/awssupport search` per trovare il caso di supporto.
2. Scegli See details (Vedi i dettagli) accanto al caso che ti interessa.
3. Nella parte inferiore dei dettagli del caso, scegli Reply (Rispondi).

4. Nella finestra di dialogo Reply to case (Rispondi al caso), inserisci una breve descrizione del problema nel campo Message (Messaggio). Quindi scegli Next (Successivo).



5. Scegli il tuo metodo di contatto. I metodi di contatto disponibili dipendono dal tipo di caso e dal piano di supporto.
6. (Facoltativo) Per Additional contacts to notify (Contatti aggiuntivi da notificare), inserisci altri indirizzi e-mail per i quali desideri ricevere aggiornamenti su questo caso di supporto. Puoi aggiungere fino a 10 indirizzi e-mail.
7. Scegliere Review (Rivedi). Quindi, puoi scegliere se modificare la risposta, allegare file o condividerli con il canale.
8. Quando sei pronto a rispondere, scegli Send message (Invia messaggio).
9. (Facoltativo) Per visualizzare la corrispondenza precedente relativa al tuo caso, scegli Previous correspondence (Corrispondenza precedente). Per visualizzare i messaggi abbreviati, scegli Show full message (Mostra messaggio completo).

Example : risposta a un caso in Slack



Partecipa a una sessione di chat dal vivo con AWS Support

Quando richiedi una chat dal vivo per il tuo caso, scegli di utilizzare un nuovo canale di chat o un thread nel canale corrente per te e l' AWS Support agente. Utilizza questo canale o thread di chat per comunicare con l'agente dell'assistenza e tutti coloro che hai invitato alla chat dal vivo.

Important

Chiunque si unisca al tuo canale con una chat dal vivo può visualizzare i dettagli su questo specifico caso di supporto e la cronologia della chat. È consigliabile aggiungere solo gli utenti che richiedono l'accesso ai casi di supporto. Qualsiasi membro di un canale o thread di chat può partecipare anche a una chat attiva.

Note

I canali e i thread di chat dal vivo ricevono inoltre notifiche quando viene aggiunta una corrispondenza al caso al di fuori della sessione di chat dal vivo. Ciò si verifica prima, durante e dopo una sessione di chat, quindi puoi utilizzare un canale o un thread di chat

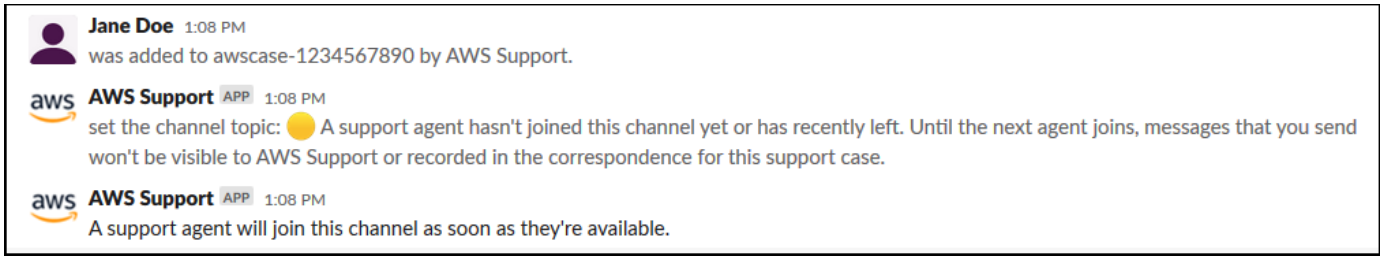
per monitorare tutti gli aggiornamenti relativi a un caso. Se hai scelto di utilizzare un nuovo canale di chat, utilizza il canale di configurazione a cui hai invitato l' AWS Support App per rispondere a queste corrispondenze.

Per partecipare a una sessione di chat dal vivo AWS Support in un nuovo canale

1. Nell'applicazione Slack, vai al canale che l' AWS Support App crea per te. Il nome del canale include l'ID del caso di supporto, ad esempio *awscase-1234567890*.

   > **Note**
   >
   > L' AWS Support app aggiunge un messaggio in evidenza al canale di live chat che contiene dettagli sulla tua richiesta di assistenza. Dal messaggio appuntato, puoi terminare la chat o risolvere il caso. Puoi trovare tutti i messaggi appuntati in questo canale sotto il nome del canale.

2. Quando l'agente dell'assistenza si unisce al canale, puoi parlare del tuo caso di supporto. Fino a quando un agente dell'assistenza non si unisce al canale, l'agente non vedrà i messaggi in quella chat e i messaggi non compaiono nella corrispondenza del caso.

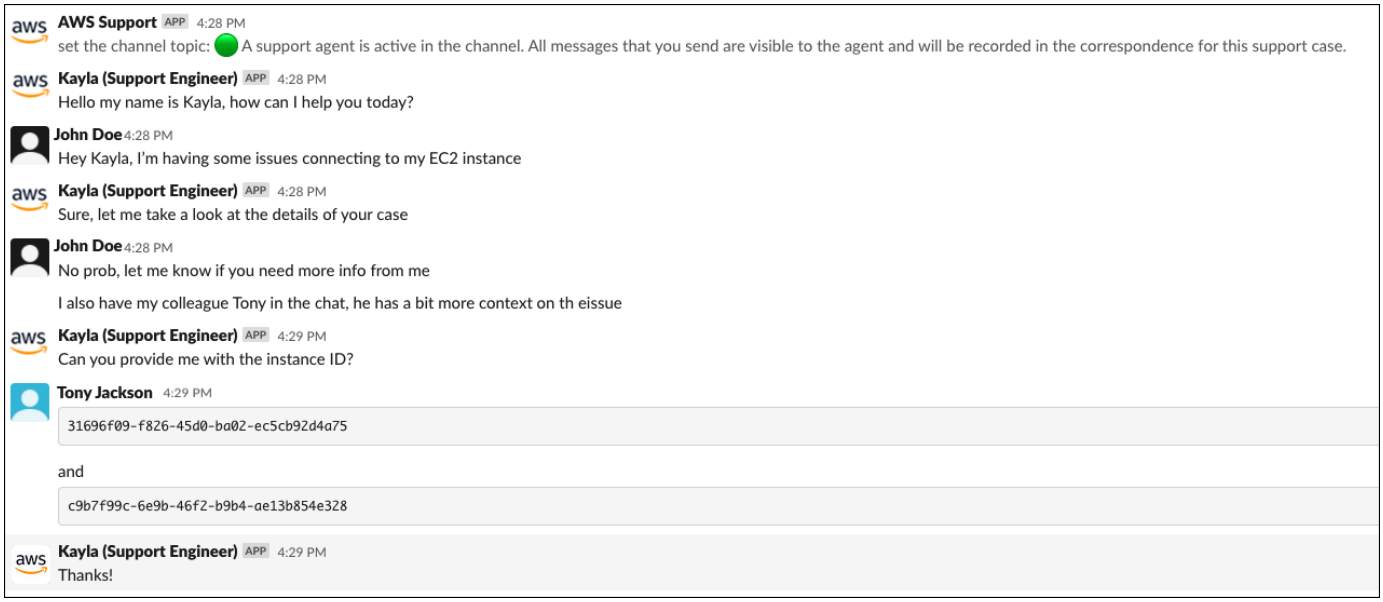
3. (Facoltativo) Aggiungi altri membri al canale della chat. Per impostazione predefinita, i canali della chat sono privati.
4. Una volta che l'agente di assistenza entra nella chat, il canale di chat è attivo e l'app AWS Support registra la chat.

   Puoi parlare in chat con l'agente in merito al tuo caso di supporto e caricare eventuali file allegati sul canale. L' AWS Support app salva automaticamente i file e il registro della chat nella corrispondenza relativa al caso.

> **Note**
>
> Quando chatti con un agente dell'assistenza, tieni presente le seguenti differenze in Slack per l' AWS Support app:
>
> - Gli agenti dell'assistenza non possono visualizzare messaggi o thread condivisi. Per condividere il testo di un messaggio o di un thread, inserisci il testo come nuovo messaggio.
> - Se modifichi o elimini un messaggio, l'agente continua a visualizzare il messaggio originale. È necessario inserire nuovamente il nuovo messaggio per mostrare la revisione.

Example : sessione di live chat

Di seguito è riportato un esempio di live chat con un agente dell'assistenza per la risoluzione di un problema di connettività per due istanze Amazon Elastic Compute Cloud (Amazon EC2).

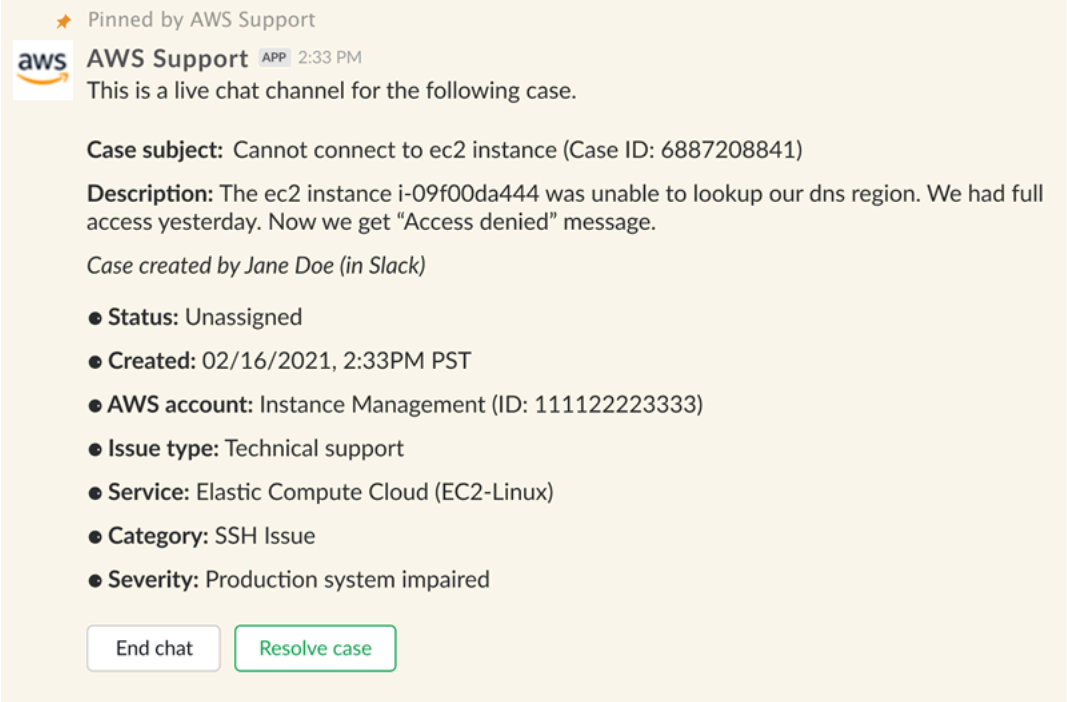


5. (Facoltativo) Per interrompere la live chat, scegli End chat (Termina la chat). L'agente dell'assistenza lascia il canale e l' AWS Support App interrompe la registrazione della chat dal vivo. Puoi trovare la cronologia della chat in allegato alla corrispondenza del caso relativo a questo caso di supporto.

6. Se il problema è stato risolto, puoi scegliere Resolve case (Risolvi il caso) dal messaggio appuntato o digitare `/awssupport resolve`.

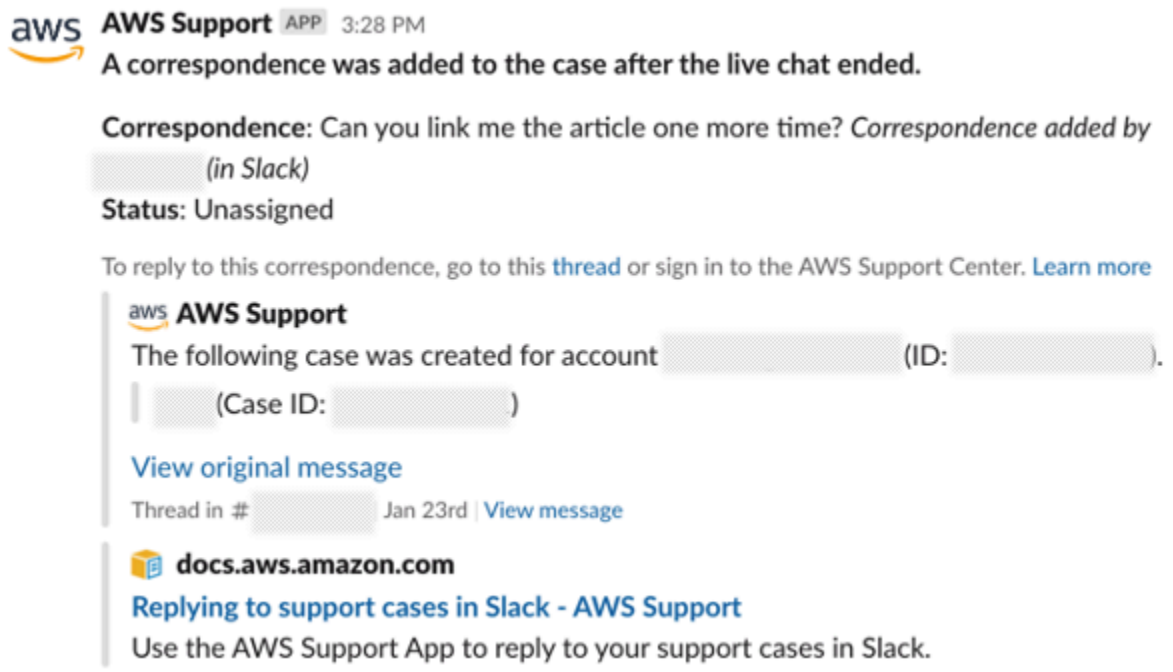
   Example : chiusura di una live chat

   Il seguente messaggio appuntato mostra i dettagli del caso relativo a un'istanza Amazon EC2. Puoi trovare i messaggi appuntati sotto il nome del canale Slack.



   Example : notifica della corrispondenza nel canale di chat

   Di seguito è riportato un esempio di un canale di live chat che riceve una notifica quando un altro collaboratore aggiunge un aggiornamento al termine della chat.

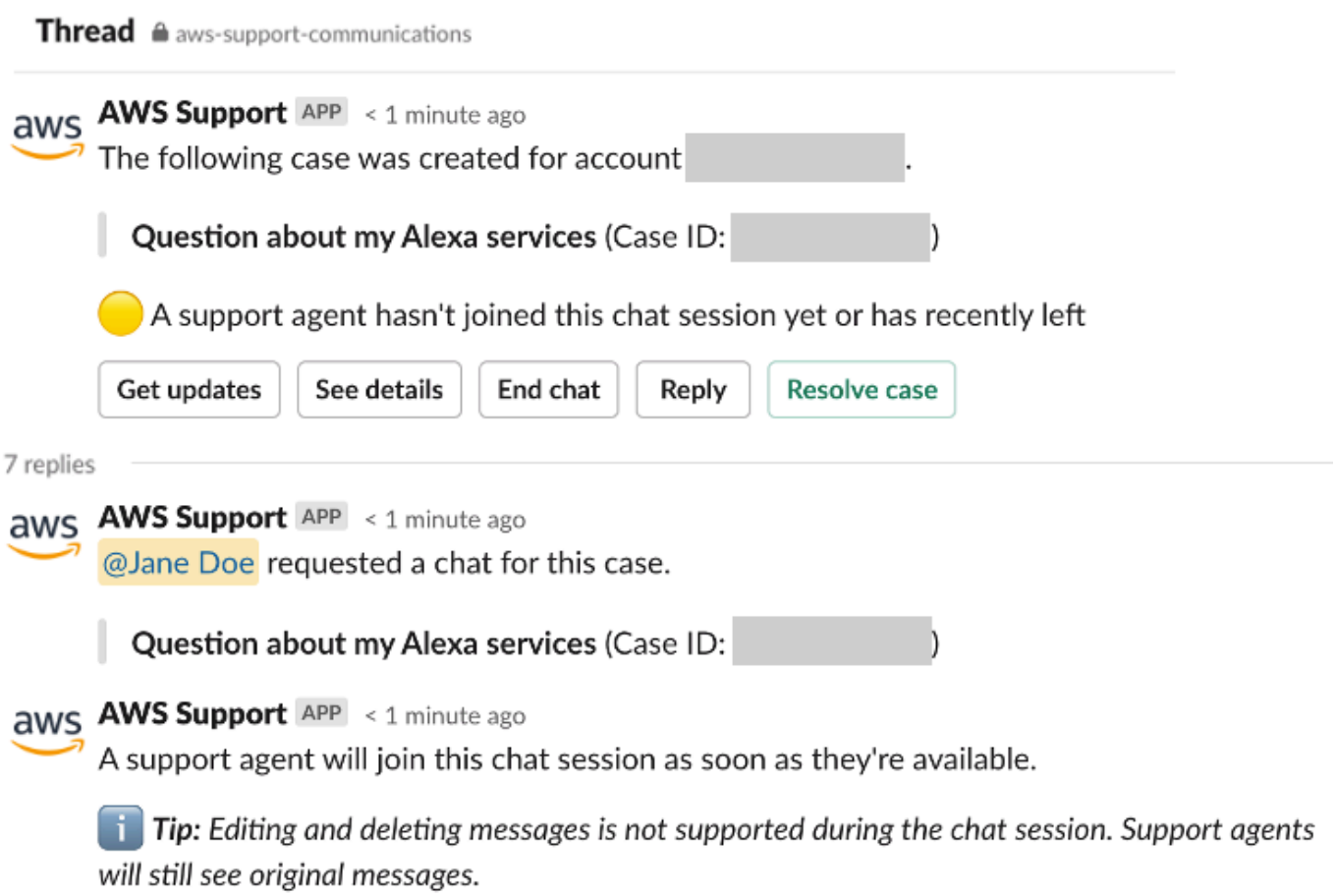


La notifica indicherà lo stato della chat (richiesta, in corso o terminata) e se la corrispondenza è stata aggiunta da un agente o da un altro collaboratore. L'app di supporto tenterà anche di ricollegarsi al thread o al canale Slack originale in cui è stata richiesta questa chat. Puoi rispondere a questo caso da tale canale o da qualsiasi altro canale con accesso a questo caso.

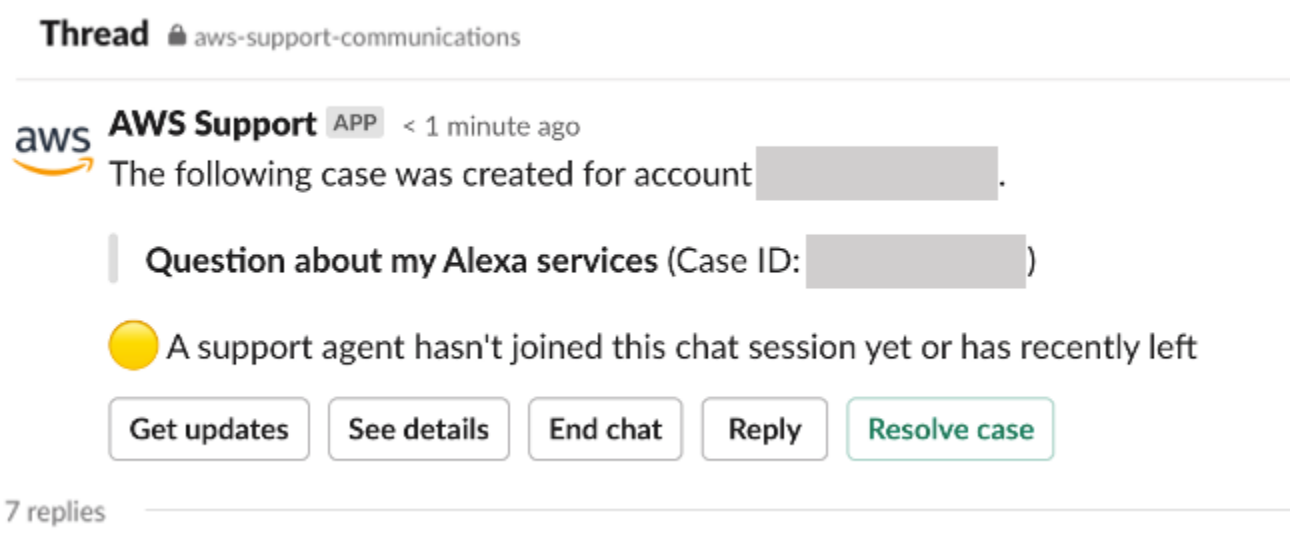
Per partecipare a una sessione di chat dal vivo AWS Support utilizzando il canale corrente

1. Nell'applicazione Slack, vai al thread nel canale corrente che l' AWS Support App utilizza per la chat. Nella maggior parte dei casi, corrisponderà al thread avviato quando il caso è stato creato per la prima volta.
2. Quando l'agente dell'assistenza si unisce al thread, puoi chattare riguardo al tuo caso di supporto. Fino a quando un agente dell'assistenza non si unisce al thread, non vedrà i messaggi in tale thread e i messaggi non compariranno nella corrispondenza del tuo caso quando la chat viene terminata.

> **Note**
>
> I messaggi inviati a questo canale al di fuori del thread della chat non vengono mai visti da AWS Support, anche quando una chat è attiva.



3. (Facoltativo) Tagga gli altri membri del canale per avvisarli nel thread della chat.
4. Dopo che l'agente dell'assistenza si è unito alla chat, il thread della chat è attivo e l' AWS Support App registra la chat. Come per l'opzione del nuovo canale di chat, puoi chattare con l'agente in merito al tuo caso di supporto e caricare eventuali file allegati al thread. L' AWS Support app salva automaticamente i file e il registro della chat nella corrispondenza del caso.
5. (Facoltativo) Per interrompere la chat dal vivo, seleziona Termina chat dal messaggio iniziale di tale thread. L'agente dell'assistenza lascia il thread e l' AWS Support App interrompe la registrazione della chat dal vivo. Puoi trovare la cronologia della chat in allegato alla corrispondenza del caso relativo a questo caso di supporto.
6. Se il problema è stato risolto, puoi scegliere Risolvi il caso a partire dal messaggio iniziale di tale thread.



Ricerca di casi di supporto in Slack

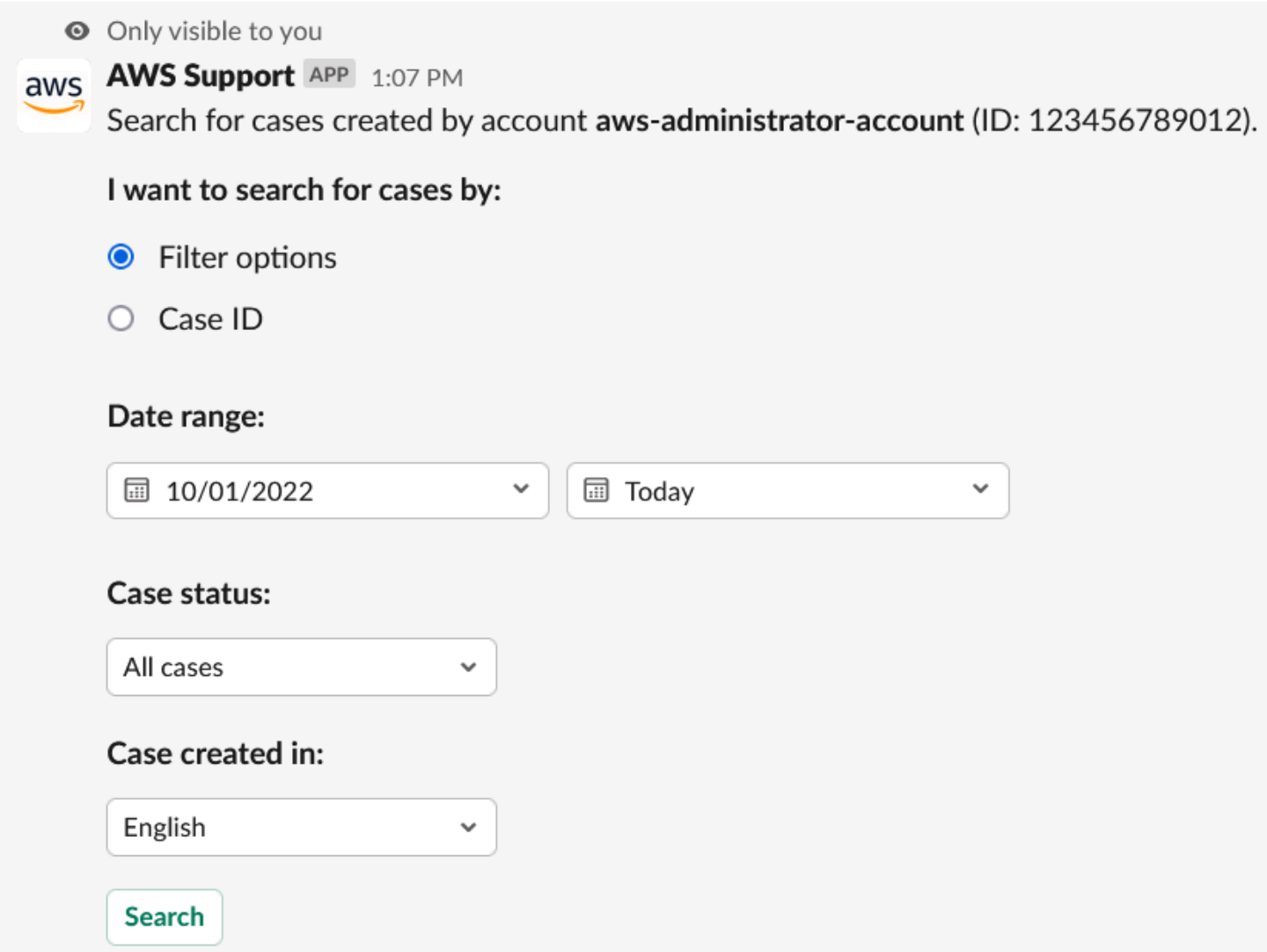
Dal tuo canale Slack, puoi cercare i casi di supporto dal tuo Account AWS e da altri account che hanno configurato lo stesso canale e lo stesso workspace. Ad esempio, se il tuo account (123456789012) e l'account del tuo collega (111122223333) hanno configurato lo stesso workspace e gli stessi canali nella AWS Support Center Console, puoi utilizzare il comando dell'app AWS Support per cercare e aggiornare casi di supporto reciproci.

Per filtrare i risultati della ricerca, puoi utilizzare le opzioni seguenti:

- ID account
- ID del caso
- Stato del caso
- Lingua di contatto
- Intervallo di date

Example : ricerca i casi in Slack

L'esempio seguente mostra come cercare un singolo account in base alle opzioni di filtro, specificando l'intervallo di date, lo stato del caso e la lingua di contatto.



Per cercare un caso di supporto in Slack

1. Nel canale Slack, immetti il seguente comando:

   ```
   /awssupport search
   ```

2. Per I want to search for cases by: (Voglio effettuare la ricerca dei casi in base a:), scegli una delle opzioni seguenti:

   A. Filter options (Opzioni di filtro): puoi filtrare i casi in base alle opzioni seguenti:

   - Account AWS: questo elenco appare solo se disponi di più account in questo canale.
   - Date range (Intervallo di date): la data di creazione del caso.
   - Case status (Stato del caso): lo stato del caso corrente, ad esempio All open cases (Tutti i casi aperti) o Resolved (Risolti).

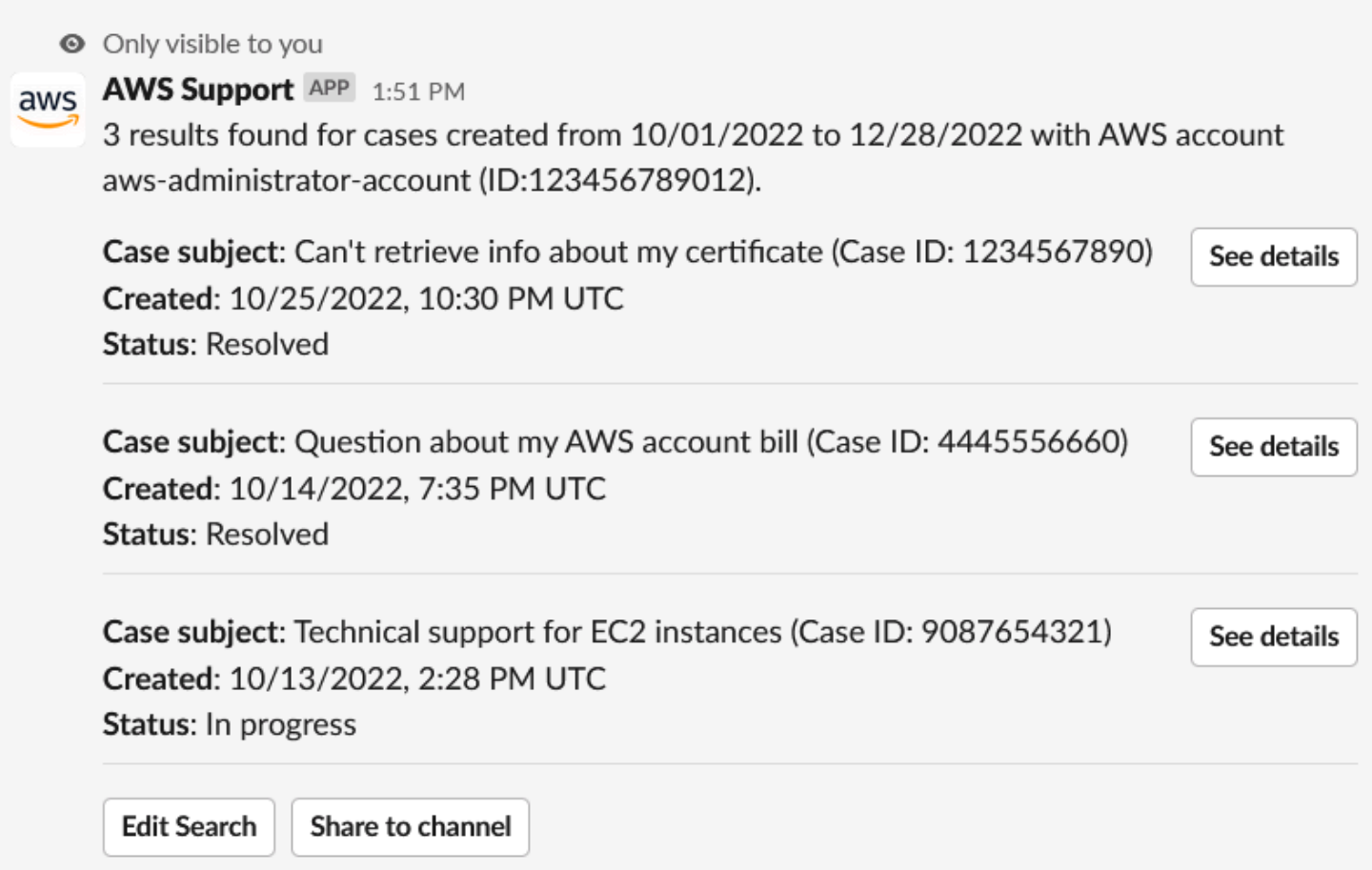
- Case created in (Caso creato in): la lingua di contatto per il caso.

B. Case ID (ID caso): inserisci l'ID del caso. Puoi inserire un solo ID caso alla volta. Se nel canale sono presenti più account, scegli l'Account AWS per effettuare una ricerca del caso.

3. Selezionare Search (Cerca). I risultati della ricerca vengono visualizzati in Slack.

Utilizzo dei risultati della ricerca

L'esempio seguente restituisce tre casi di supporto da un Account AWS.



Dopo aver ricevuto i risultati della ricerca, puoi eseguire le operazioni seguenti:

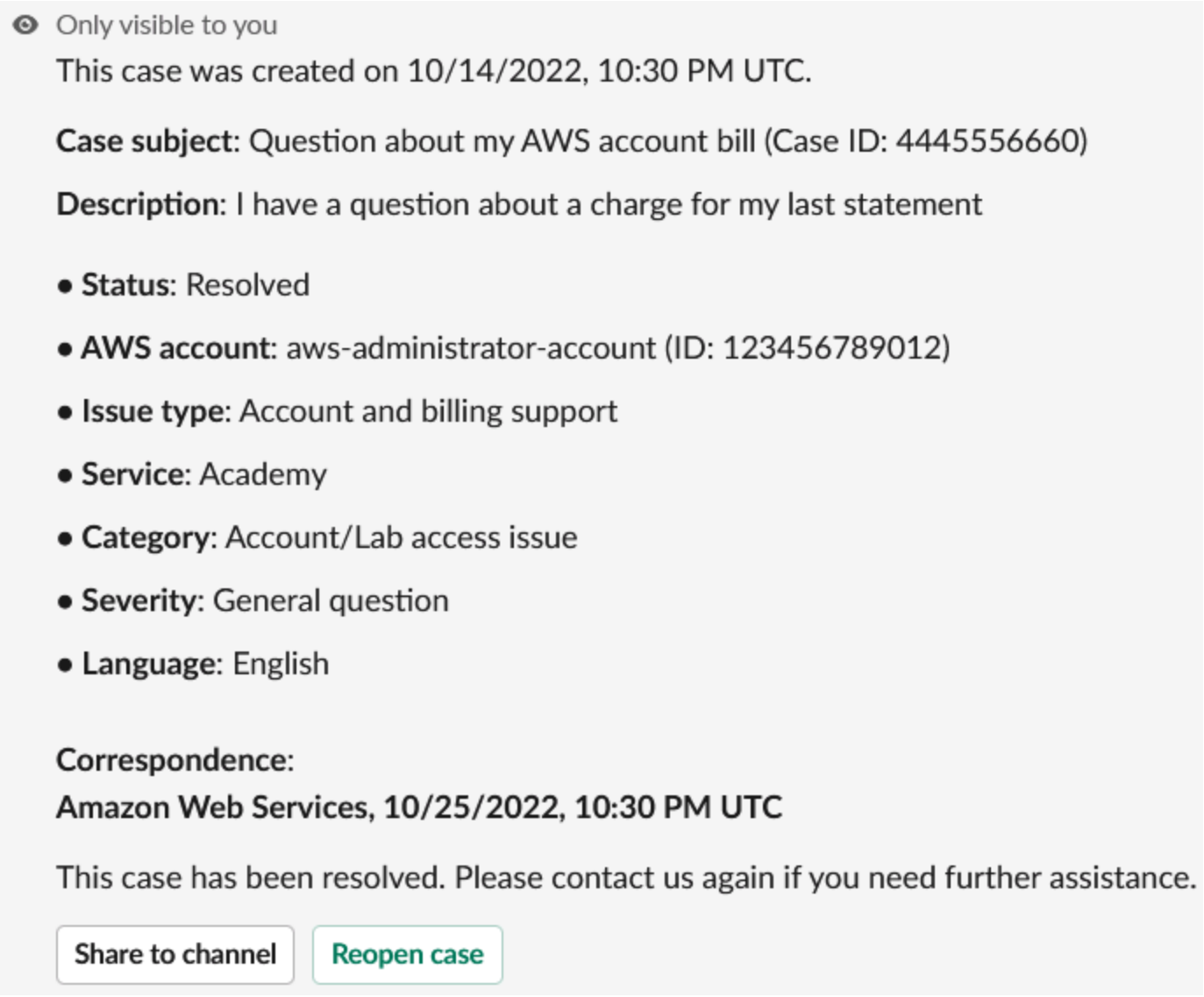
Per utilizzare i risultati della ricerca

1. Scegli Edit Search (Modifica ricerca) per modificare le opzioni di filtro precedenti o l'ID del caso.
2. Scegli Share to channel (Condividi con canale) per condividere i risultati della ricerca con il canale.

3. Scegli See details (Vedi i dettagli) per ulteriori informazioni su un caso. È possibile scegliere Show full message (Mostra messaggio completo) per visualizzare il resto della corrispondenza più recente.
4. Se hai eseguito la ricerca tramite Filter options (Opzioni di filtro), i risultati della ricerca possono restituire più casi. Scegli Prossimi 5 risultati (5 risultati successivi) o Previous 5 results (5 risultati precedenti) per visualizzare i 5 casi successivi o precedenti.

Example : caso di supporto risolto

L'esempio seguente mostra un caso di supporto risolto relativo a un problema di account e fatturazione dopo aver selezionato l'opzione See details (Vedi i dettagli).

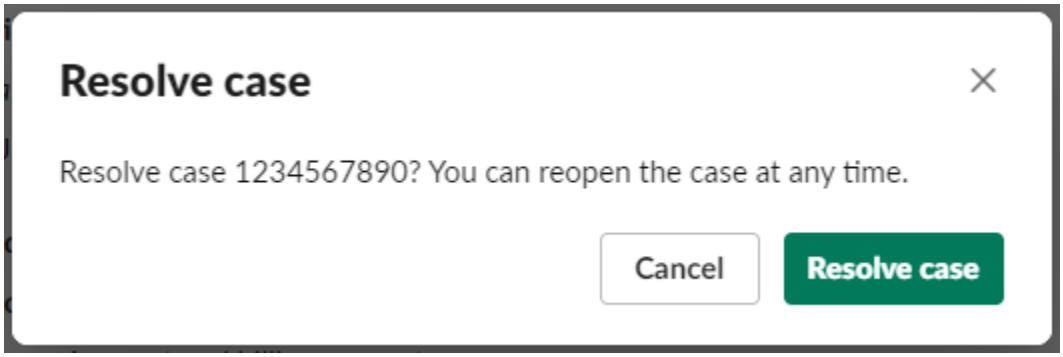


Risoluzione di un caso di supporto in Slack

Se non hai più bisogno di un caso di supporto o hai risolto il problema, puoi risolvere il caso direttamente in Slack. In questo modo il caso viene risolto anche nella AWS Support Center Console. Dopo avere risolto un caso, puoi riaprirlo in un secondo momento.

Come risolvere un caso di supporto in Slack

1. Nel tuo canale Slack, accedi al caso di supporto. Per informazioni, consultare Ricerca di casi di supporto in Slack.
2. Scegli See details (Vedi i dettagli) per il caso.
3. Seleziona Risolvi caso.
4. Nella finestra di dialogo Resolve case (Risolvi il caso), scegli Resolve case (Risolvi il caso). Puoi riaprire un caso nel canale Slack o dalla console del Centro assistenza.

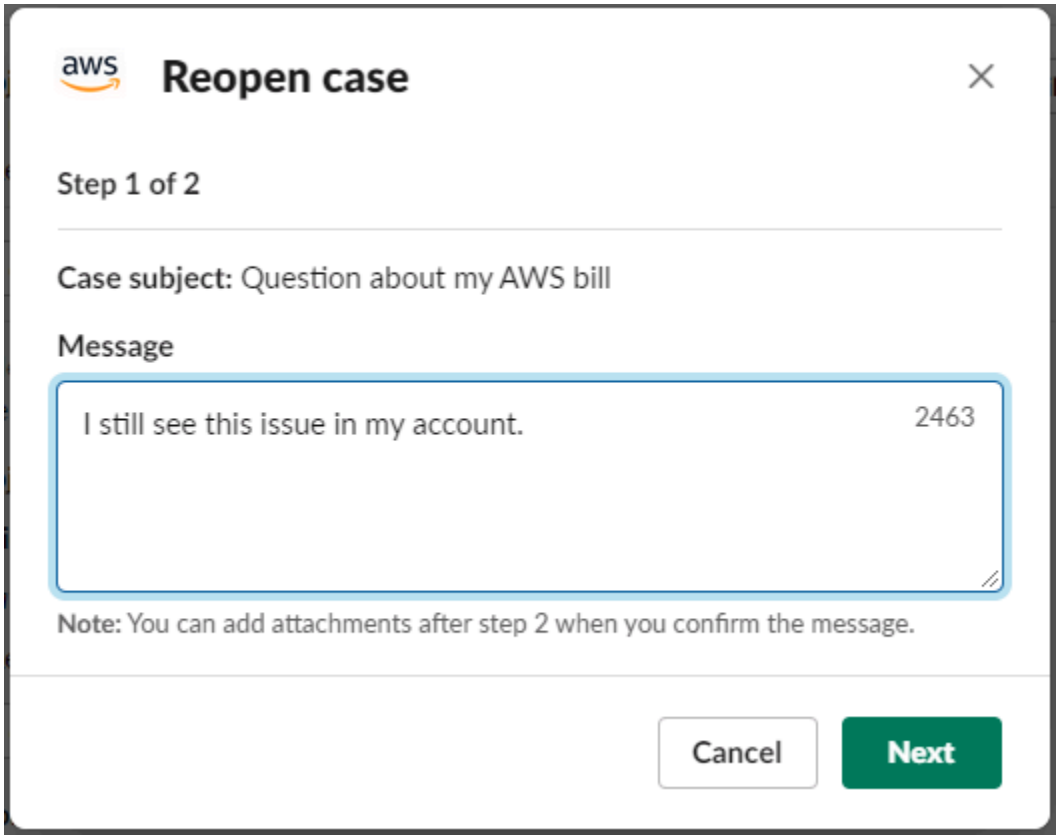


Riapertura di un caso di supporto in Slack

Dopo avere risolto un caso di supporto, puoi riaprirlo da Slack.

Come riaprire un caso di supporto in Slack

1. Trova il caso di supporto da riaprire in Slack. Per informazioni, consultare Ricerca di casi di supporto in Slack.
2. Scegli See details (Vedi i dettagli).
3. Seleziona Riapri il caso.
4. Nella finestra di dialogo Reopen case (Riapri il caso), inserisci una breve descrizione del problema nel campo Message (Messaggio).
5. Seleziona Successivo.



6. (Facoltativo) Inserisci contatti aggiuntivi.
7. Scegliere Review (Rivedi).
8. Rivedi i dettagli del caso, quindi scegli Send message (Invia messaggio). Il tuo caso si riapre. Se hai chiesto una nuova chat dal vivo con un agente dell'assistenza, Slack utilizza lo stesso canale o thread di chat utilizzato precedentemente per una chat dal vivo. Se hai chiesto una chat dal vivo in un nuovo canale e non ne hai ancora ottenuta una, viene aperto un nuovo canale di chat. Se hai richiesto una chat dal vivo nel canale attuale e non ne hai ancora ottenuta una, viene utilizzato un thread nel canale attuale.

Richiesta di aumenti della quota di servizio

Puoi richiedere aumenti della quota di servizio per il tuo account dal tuo canale Slack.

Come richiedere aumenti delle quote di servizio

1. Nel canale Slack, immetti il seguente comando:

   ```
   /awssupport quota
   ```

2. Nella finestra di dialogo Increase service quota (Aumenta la quota di servizio), inserisci le informazioni riportate di seguito:

    a. Seleziona Account AWS.

    b. Seleziona Regione AWS.

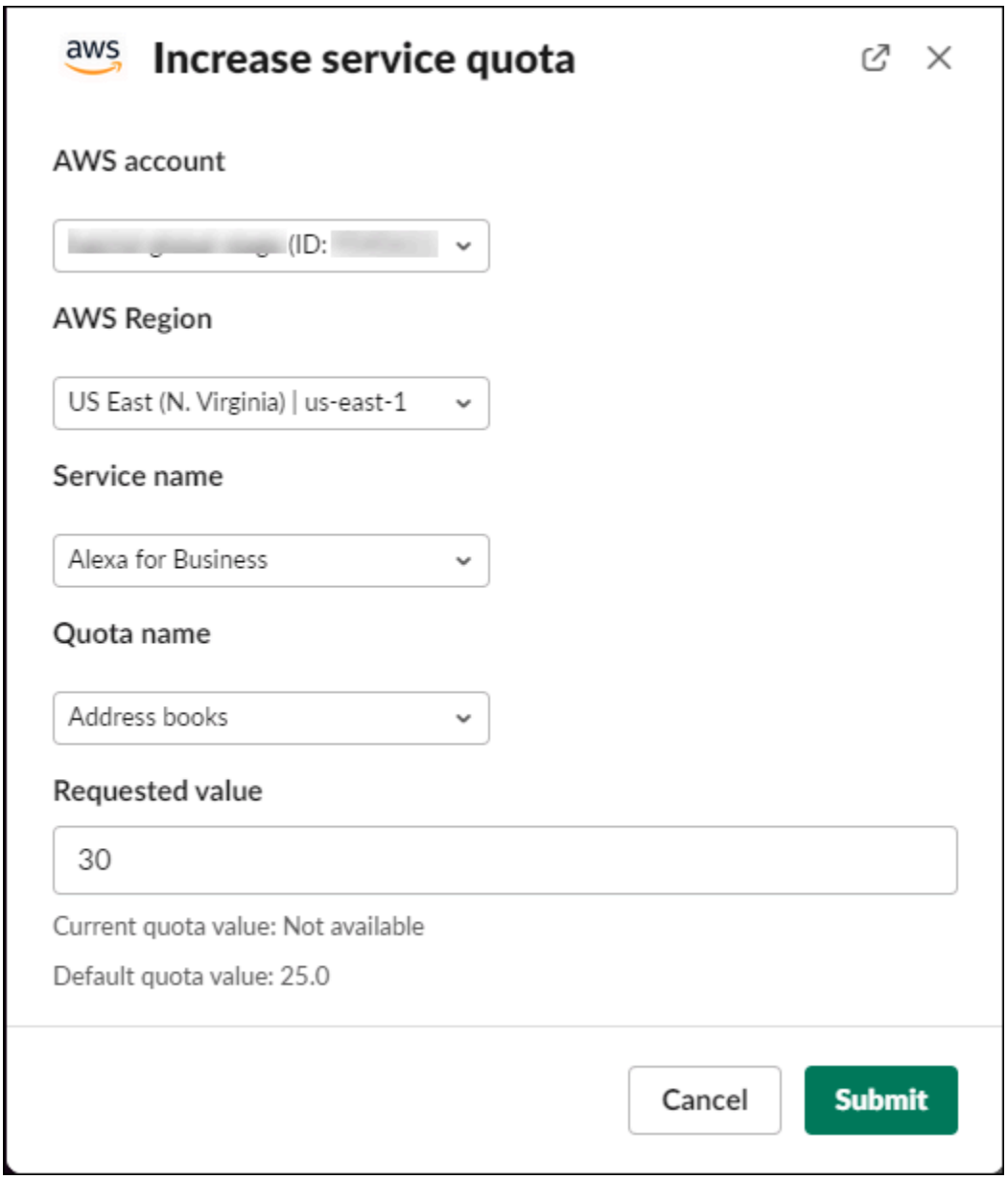
    c. Scegli Service name (Nome del servizio).

    d. Scegli Quota name (Nome della quota).

    e. Specifica il campo Requested value (Valore richiesto) per l'aumento della quota. È necessario immettere un valore superiore alla quota predefinita.

3. Scegli Submit (Invia).

Example : aumento della quota di Alexa per le aziende



Inoltre, è possibile visualizzare le richieste dalla console Service Quotas. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente per Service Quotas.

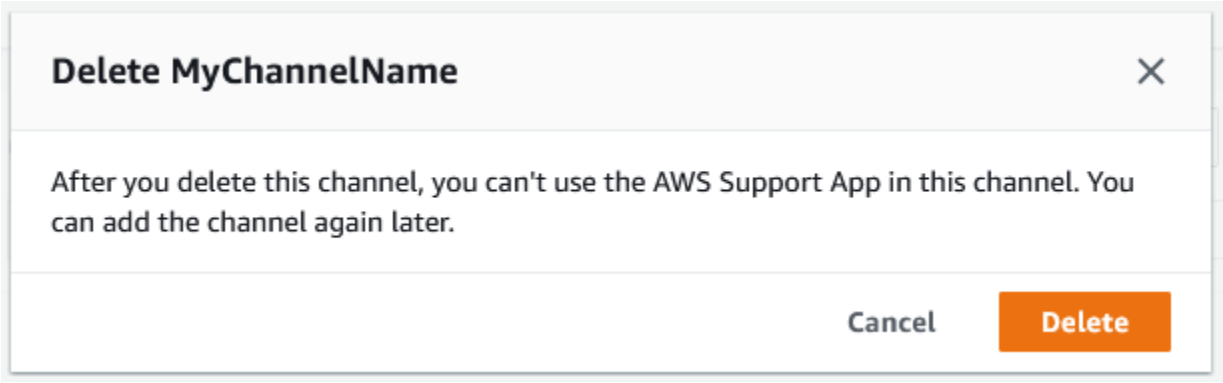
Eliminazione di una configurazione di canale Slack dall'app AWS Support

Se non ti occorre una configurazione di canale dall'app AWS Support, puoi eliminarla. Questa operazione rimuove solo il canale dall'app AWS Support e dalla AWS Support Center Console. Il tuo canale non è stato eliminato da Slack.

Puoi aggiungere fino a 20 canali per l'Account AWS. Se hai già raggiunto questa quota, devi eliminare un canale prima di poterne aggiungere un altro.

Come eliminare una configurazione di canale Slack

1. Accedi alla console del Centro assistenza e scegli Slack configuration (Configurazione di Slack).
2. Nella pagina Slack configuration (Configurazione di Slack), in Channels (Canali), scegli il nome del canale e quindi seleziona Delete (Elimina).
3. Nella finestra di dialogo Delete channel name (Elimina il nome del canale), scegli Delete (Elimina). Potrai aggiungere nuovamente questo canale all'app AWS Support in un secondo momento.



Eliminazione di una configurazione del workspace Slack dall'app AWS Support

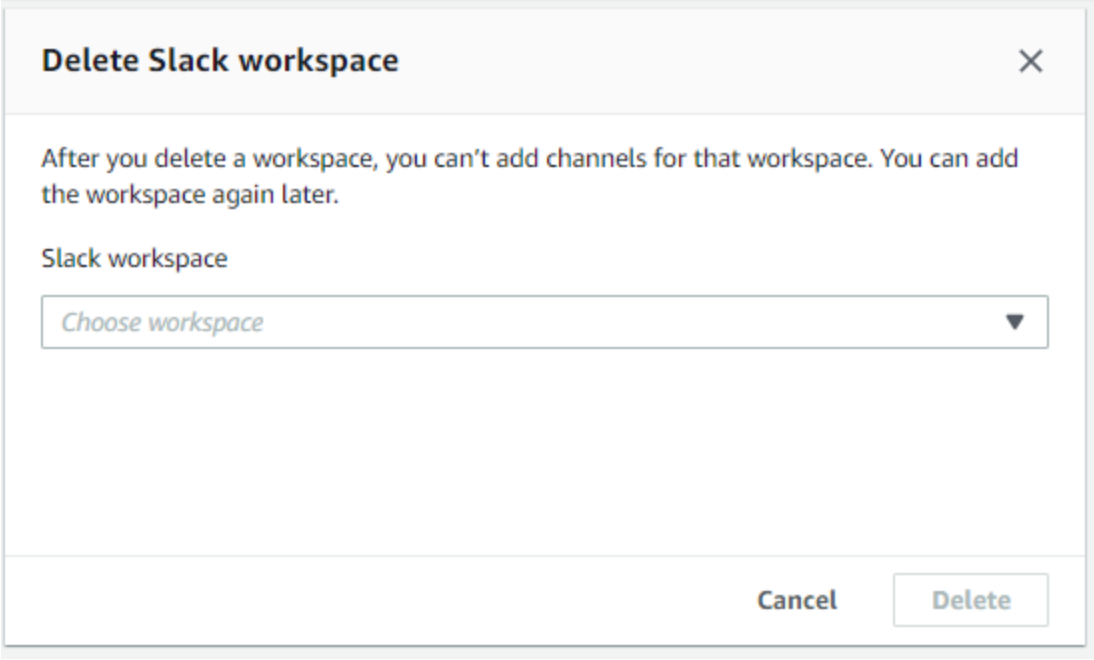
Puoi eliminare una configurazione del workspace dall'app AWS Support se non ti occorre. Questa operazione rimuove il workspace solo dall'app AWS Support e dalla AWS Support Center Console. Il tuo workspace non è stato eliminato da Slack.

Puoi aggiungere fino a 5 workspace per il tuo Account AWS. Se hai già raggiunto questa quota, devi eliminare un workspace Slack prima di poterne aggiungere un altro.

> **Note**
>
> Se hai aggiunto canali da questo workspace all'app AWS Support, prima di eliminare il workspace devi innanzitutto eliminare tali canali. Per informazioni, consultare Eliminazione di una configurazione di canale Slack dall'app AWS Support.

Come eliminare una configurazione di workspace Slack

1. Accedi alla AWS Support Center Console e scegli Slack configuration (Configurazione di Slack).
2. Nella pagina Slack configuration (Configurazione di Slack), alla voce Slack workspaces (Workspace Slack) scegli Delete a workspace (Elimina un workspace).
3. Nella finestra di dialogo Delete Slack workspace (Elimina un workspace Slack), seleziona il nome del workspace Slack, quindi seleziona Delete (Elimina). Puoi aggiungere nuovamente il workspace al tuo Account AWS in un secondo momento.



App AWS Support nei comandi Slack

Comandi del canale Slack

Puoi inserire i seguenti comandi nel canale Slack al quale hai invitato l'app AWS Support. Il nome di questo canale Slack viene visualizzato anche come canale configurato nella AWS Support Center Console.

`/awssupport create` o `/awssupport create-case`

Crea un caso di supporto.

`/awssupport search` o `/awssupport search-case`

Cerca i casi. Puoi cercare i casi di supporto per gli Account AWS che hanno configurato l'app AWS Support per lo stesso canale Slack.

`/awssupport quota` o `/awssupport service-quota-increase`

Richiedi un aumento della quota di servizio.

Comandi del canale della live chat

Puoi inserire i seguenti comandi nel canale della live chat. Questo è il canale che viene creato dall'app AWS Support per l'utente quando scegli un nuovo canale per la chat con AWS Support. I canali di chat includono l'ID del caso di supporto, ad esempio *`awscase-1234567890`*.

> **Note**
>
> I comandi seguenti non sono disponibili quando utilizzi un thread nel canale attuale per una chat dal vivo. Utilizza. invece. i pulsanti collegati al messaggio iniziale del thread per terminare una chat, invitare un nuovo agente o risolvere il caso.

`/awssupport endchat`

Rimuovi l'agente dell'assistenza e termina la sessione di live chat.

`/awssupport invite`

Invita un nuovo agente dell'assistenza su questo canale.

`/awssupport resolve`

Risolvi questo caso di supporto.

Visualizzazione delle corrispondenze dell'app AWS Support nella AWS Support Center Console

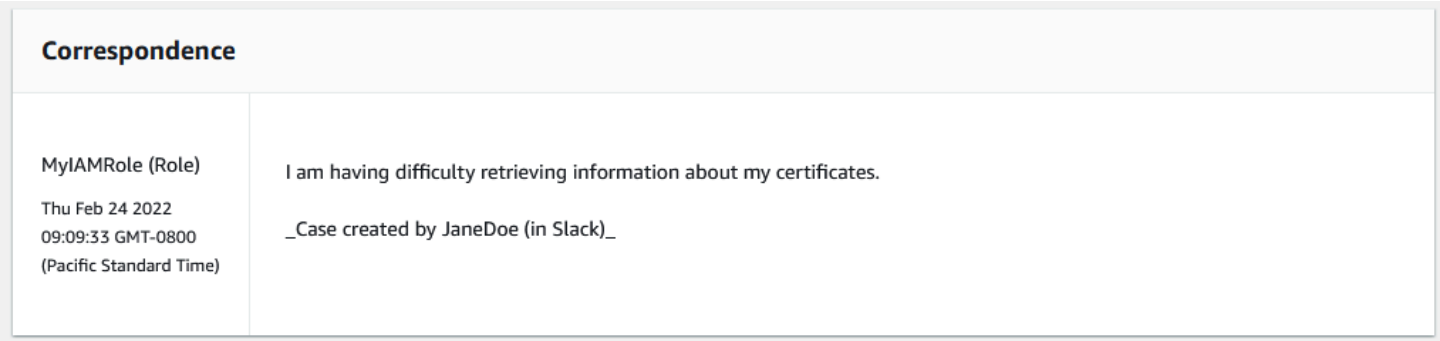
Quando crei, aggiorni o risolvi i casi di supporto per il tuo account nel canale Slack, puoi anche accedere alla console del Centro assistenza per visualizzare i tuoi casi. Puoi visualizzare le corrispondenze di caso per determinare se il caso è stato aggiornato nel canale Slack, visualizzare la cronologia delle chat con un agente dell'assistenza e trovare gli eventuali allegati caricati da Slack.

Come visualizzare le corrispondenze di caso da Slack

1. Accedi alla AWS Support Center Console per il tuo account.
2. Scegli il tuo caso di supporto.
3. In Correspondence (Corrispondenza), puoi vedere se il caso è stato creato e aggiornato dal canale Slack.

Example : caso di supporto

Nella schermata seguente, Jane Doe ha riaperto un caso di supporto in Slack. Questa corrispondenza viene visualizzata per il caso di supporto nella console del Centro assistenza.



Creazione dell'app AWS Support nelle risorse Slack con AWS CloudFormation

L'app AWS Support in Slack è integrata con AWS CloudFormation, un servizio che ti consente di modellare e configurare le tue risorse AWS in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Puoi creare un modello che descrive tutte le risorse AWS desiderate (come AccountAlias e SlackChannelConfiguration) e AWS CloudFormation si occuperà del provisioning e della configurazione di queste risorse per tuo conto.

Quando usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse dell'app AWS Support in modo coerente e continuo. Basta descrivere le risorse una volta sola, dopodiché si può effettuare il provisioning di tali risorse quante volte si vuole in più Account AWS e regioni.

App AWS Support e modelli AWS CloudFormation

Per eseguire il provisioning e la configurazione delle risorse per l'app AWS Support e i servizi correlati, devi conoscere i modelli AWS CloudFormation. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a utilizzare i modelli AWS CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation.

L'app AWS Support supporta la creazione di AccountAlias e SlackChannelConfiguration in AWS CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse AccountAlias e SlackChannelConfiguration, consulta la documentazione di riferimento sui tipi di risorse dell'app AWS Support nella Guida per l'utente di AWS CloudFormation.

Creazione di risorse di configurazione Slack per la tua organizzazione

Puoi utilizzare modelli CloudFormation per creare le risorse necessarie per l'app AWS Support. Se sei il titolare dell'account di gestione della tua organizzazione, puoi utilizzare i modelli per creare queste risorse per i tuoi account membri in AWS Organizations.

Ad esempio, potresti utilizzare un modello per creare la stessa configurazione del workspace di Slack per tutti gli account dell'organizzazione e in seguito utilizzare modelli separati per creare diverse configurazioni di canali Slack per Account AWS o unità organizzative (UO) specifiche. Puoi anche usare un modello per creare una configurazione del workspace di Slack in modo che gli account membri possano configurare i canali Slack desiderati per i propri Account AWS.

Puoi scegliere se utilizzare o meno modelli CloudFormation. Se scegli di non utilizzare modelli CloudFormation, puoi completare manualmente la procedura seguente:

- Crea le risorse dell'app AWS Support nella AWS Support Center Console.
- Crea un caso di supporto con AWS Support per autorizzare più account all'uso dell'app AWS Support.
- Effettua una chiamata all'operazione API RegisterSlackWorkspaceForOrganization per registrare un workspace di Slack per il tuo account. Lo stack CloudFormation invoca automaticamente questa azione dell'API.

Segui queste procedure per caricare il modello CloudFormation nella tua organizzazione. Puoi usare i modelli di esempio inclusi nella pagina Documentazione di riferimento sul tipo di risorsa dell'app AWS Support.

I modelli indicano a CloudFormation di creare le risorse seguenti:

- Una configurazione del canale Slack.
- Una configurazione del workspace di Slack.
- Un ruolo IAM denominato `AWSSupportSlackAppCFNRole`. La policy AWSSupportAppFullAccess gestita da AWS è collegata.

Indice

Aggiornamento dei modelli CloudFormation per Slack

Per iniziare, usa i modelli seguenti per creare il tuo stack. Sostituisci i modelli con valori validi per il workspace e il canale Slack.

> **Note**
>
> Non ti consigliamo di utilizzare il modello per creare una risorsa AccountAlias per la tua organizzazione. La risorsa AccountAlias identifica in maniera univoca un Account AWS nell'app AWS Support. I tuoi account membri possono immettere un nome account nella

console del Centro assistenza. Per ulteriori informazioni, consulta Autorizzazione di un workspace Slack.

Come aggiornare modelli CloudFormation per Slack

1. Se sei titolare dell'account di gestione per un'organizzazione, devi prima autorizzare manualmente un workspace Slack per il tuo account affinché gli account membri possano utilizzare CloudFormation per creare le risorse. Se non l'hai ancora fatto, consulta la sezione Autorizzazione di un workspace Slack.
2. Dalla pagina Documentazione di riferimento per il tipo di risorse dell'app AWS Support, copia il modello JSON o YAML per la risorsa desiderata.
3. In un editor di testo, incolla il modello in un nuovo file.
4. Specifica i parametri desiderati all'interno del modello. Sostituisci almeno i valori per i campi seguenti:
   - `TeamId` con il tuo ID del workspace di Slack
   - `ChannelId` con l'ID del canale Slack
   - `ChannelName` con un nome che identifica la configurazione del canale Slack

   > **Tip**
   >
   > Per trovare il workspace e gli ID dei canali, apri il tuo canale Slack in un browser. Nell'URL, l'ID del workspace è il primo identificatore e l'ID del canale è il secondo. Ad esempio, in https://app.slack.com/client/T012ABCDEFG/C01234A5BCD, T012ABCDEFG è l'ID del workspace e C01234A5BCD è l'ID del canale.
5. Salva il file come JSON o YAML.

Creazione di uno stack per l'account di gestione

Successivamente, devi creare uno stack per l'account di gestione nell'organizzazione. Questo passaggio effettua una chiamata all'operazione API RegisterSlackWorkspaceForOrganization per conto tuo e autorizza il workspace con Slack.

> **Note**
>
> È preferibile caricare il modello di configurazione del workspace Slack che hai aggiornato nella procedura precedente per l'account di gestione. Non è necessario caricare il modello di configurazione del canale Slack, a meno che tu non stia configurando anche l'account di gestione per l'uso dell'app AWS Support.

Come creare uno stack per l'account di gestione

1. Accedi alla AWS Management Console utilizzando l'account di gestione per la tua organizzazione.
2. Apri la console di AWS CloudFormation all'indirizzo https://console.aws.amazon.com/cloudformation.
3. Se non l'hai ancora fatto, nel selettore di regione, scegli una delle Regioni AWS seguenti:
   - Europa (Francoforte)
   - Europa (Irlanda)
   - Europa (Londra)
   - Stati Uniti orientali (Virginia settentrionale)
   - Stati Uniti orientali (Ohio)
   - Stati Uniti occidentali (Oregon)
   - Asia Pacifico (Singapore)
   - Asia Pacifico (Tokyo)
   - Canada (Centrale)
4. Segui la procedura per creare uno stack. Per ulteriori informazioni, consulta Creazione di uno stack sulla console AWS CloudFormation.

   Dopo aver creato correttamente lo stack con CloudFormation, puoi utilizzare lo stesso modello per creare un set di stack per la tua organizzazione.

Creazione di un set di stack per l'organizzazione

Usa quindi lo stesso modello della configurazione del workspace di Slack per creare un set di stack con autorizzazioni `service-managed`. Puoi utilizzare i set di stack per creare lo stack per l'intera

organizzazione o specificare le unità organizzative desiderate. Per ulteriori informazioni, consulta Creazione di un set di stack.

Questa procedura effettua inoltre una chiamata all'operazione API RegisterSlackWorkspaceForOrganization per conto tuo. Questa operazione API autorizza il workspace di Slack per gli account membri.

Per creare un set di stack per l'organizzazione

1. Accedi alla AWS Management Console utilizzando l'account di gestione per la tua organizzazione.
2. Apri la console di AWS CloudFormation all'indirizzo https://console.aws.amazon.com/cloudformation.
3. Se non l'hai ancora fatto, nel selettore di regione seleziona la stessa Regione AWS utilizzata nella procedura precedente.
4. Nel riquadro di navigazione scegli StackSets.
5. Scegli Create StackSet (Crea StackSet).
6. Nella pagina Choose a template (Seleziona un modello), mantieni le opzioni predefinite per le seguenti opzioni:
   - In Permissions (Autorizzazioni), mantieni l'opzione Service-managed permissions (Autorizzazioni gestite dal servizio).
   - In Prerequisite - Prepare template (Prerequisito - Prepara modello), mantieni Template is ready (Il modello è pronto).
7. In Specify template (Specifica modello), seleziona Upload a template file (Carica un file di modello) e infine Choose file (Scegli file).
8. Scegli il file e quindi seleziona Next (Avanti).
9. Nella pagina Specify StackSet details (Specifica dettagli di StackSet), inserisci un nome per lo stack (ad esempio **`support-app-slack-workspace`**), una descrizione e infine seleziona Next (Avanti).
10. Nella pagina Configure StackSet options (Configura opzioni StackSet), mantieni le opzioni predefinite e quindi scegli Next (Avanti).
11. Nella pagina Set deployment options (Imposta opzioni di implementazione), per Add stacks to stack set (Aggiungi stack a un set di stack), mantieni l'opzione predefinita Deploy new stacks (Implementa nuovi stack).

12. In Deployment targets (Destinazioni di implementazione), scegli se vuoi creare lo stack per l'intera organizzazione o per unità organizzative specifiche. Se scegli un'unità organizzativa, inserisci l'ID UO.
13. In Specify regions (Specifica regioni), inserisci solo una delle Regioni AWS seguenti:

    - Europa (Francoforte)
    - Europa (Irlanda)
    - Europa (Londra)
    - Stati Uniti orientali (Virginia settentrionale)
    - Stati Uniti orientali (Ohio)
    - Stati Uniti occidentali (Oregon)
    - Asia Pacifico (Singapore)
    - Asia Pacifico (Tokyo)
    - Canada (Centrale)

    > **Note:**
    >
    > - Per semplificare il flusso di lavoro, ti consigliamo di utilizzare la stessa Regione AWS scelta nella fase 3.
    > - La scelta di molteplici Regione AWS può causare conflitti durante la creazione dello stack.

14. In Deployment options (Opzioni di implementazione), per Failure tolerance - optional(Tolleranza di errore - facoltativo) inserisci il numero di account in cui gli stack possono non riuscire prima che CloudFormation interrompa l'operazione. Ti consigliamo di inserire il numero di account che desideri aggiungere, meno uno. Ad esempio, se l'unità organizzativa specificata ha 10 account membro, inserisci 9. In tal modo, anche se l'operazione di CloudFormation non riesce per 9 volte, l'esito di almeno un account sarà positivo.
15. Seleziona Successivo.
16. Nella pagina Review (Esamina), rivedi le opzioni e scegli Submit (Invia). Puoi controllare lo stato dello stack nella scheda Stack instances (Istanze stack).
17. (Facoltativo) Ripeti questa procedura per caricare un modello per la configurazione di un canale Slack. Il modello di esempio crea anche il ruolo IAM e collega una policy gestita da AWS. Questo

ruolo dispone delle autorizzazioni necessarie per accedere ad altri servizi per conto tuo. Per ulteriori informazioni, consulta Gestione degli accessi all'app AWS Support.

Se la creazione della configurazione del canale Slack avviene senza l'utilizzo di set di stack, gli account membri possono configurare manualmente il canale Slack. Per ulteriori informazioni, consulta Configurazione di un canale Slack.

Dopo la creazione degli stack con CloudFormation, ogni account membro può accedere alla console del Centro assistenza e trovare i propri canali e workspace Slack configurati. I membri, quindi, possono utilizzare l'app AWS Support per il loro Account AWS. Per informazioni, consultare Creazione di casi di supporto in un canale Slack.

> **Tip**
>
> Se devi caricare un nuovo modello, ti consigliamo di utilizzare la stessa Regione AWS specificata in precedenza.

Ulteriori informazioni su CloudFormation

Per ulteriori informazioni su CloudFormation, consulta le risorse seguenti:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Documentazione di riferimento dell'API AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Creazione di risorse dell'app AWS Support con Terraform

Puoi anche utilizzare Terraform per creare le risorse dell'app AWS Support per il tuo Account AWS. Terraform è uno strumento infrastructure-as-code che puoi utilizzare per le applicazioni cloud. Puoi usare Terraform per creare risorse dell'app AWS Support invece di implementare uno stack CloudFormation su un account.

Dopo aver installato Terraform, puoi specificare le risorse dell'app AWS Support desiderate. Terraform effettua una chiamata all'operazione API RegisterSlackWorkspaceForOrganization per

registrare uno workspace di Slack per conto tuo e crea le relative risorse. Puoi accedere, quindi, alla console del Centro assistenza e trovare i canali e workspace Slack configurati.

> **Note**
>
> - Se sei titolare dell'account di gestione di un'organizzazione, devi prima autorizzare manualmente un workspace Slack per il tuo account affinché gli account membri possano utilizzare Terraform per creare le risorse. Se non l'hai ancora fatto, consulta la sezione Autorizzazione di un workspace Slack.
> - A differenza dei set di stack CloudFormation, non puoi utilizzare Terraform per creare le risorse dell'app AWS Support per un'unità organizzativa nella tua organizzazione.
> - Puoi inoltre trovare la cronologia degli eventi per questi aggiornamenti da Terraform in AWS CloudTrail. Gli `eventSource` per questi eventi saranno `cloudcontrolapi.amazonaws.com` e `supportapp.amazonaws.com`. Per ulteriori informazioni, consulta Registrazione dell'app AWS Support nelle chiamate API Slack utilizzando AWS CloudTrail.

Ulteriori informazioni

Per ulteriori informazioni su Terraform, consulta i seguenti argomenti:

- Installazione di Terraform
- Tutorial di Terraform: creazione di un'infrastruttura per AWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

Sicurezza in AWS Support

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

La sicurezza è una responsabilità condivisa tra AWS te e te. 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. Per maggiori informazioni sui programmi di conformità applicabili AWS Support, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformità .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

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

Argomenti

Protezione dei dati in AWS Support

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

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

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

Sicurezza per i tuoi casi AWS Support

Quando crei una richiesta di supporto, sei il proprietario delle informazioni che includi nella richiesta di supporto. AWS non accede ai tuoi Account AWS dati senza la tua autorizzazione. AWS non condivide le tue informazioni con terze parti.

Quando crei un caso di supporto, è bene ricordare che:

- AWS Support utilizza le autorizzazioni definite nel ruolo `AWSServiceRoleForSupport` collegato al servizio per chiamare altre persone Servizi AWS che risolvono i problemi dei clienti per conto tuo. Per ulteriori informazioni, vedere Utilizzo di ruoli collegati ai servizi per e policy gestite:. AWS SupportAWS AWSSupportServiceRolePolicy
- Puoi visualizzare le chiamate API a quelle AWS Support avvenute nel tuo. Account AWS Ad esempio, puoi visualizzare le informazioni di log quando qualcuno nel tuo account crea o risolve un caso di supporto. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS Support API con AWS CloudTrail.
- Puoi usare l' AWS Support API per chiamarla. `DescribeCases` Questa API restituisce informazioni sui casi di supporto, come l'ID del caso, la data di creazione e risoluzione e le corrispondenze con l'agente dell'assistenza. È possibile visualizzare i dettagli del caso per un massimo di 12 mesi dopo la creazione dello stesso. Per ulteriori informazioni, DescribeCasesconsulta l'AWS Support API Reference.
- I casi di supporto seguono la Convalida della conformità per AWS Support.
- Quando crei una richiesta di assistenza, AWS non ottiene l'accesso al tuo account. Se necessario, gli agenti dell'assistenza utilizzano uno strumento di condivisione dello schermo per visualizzare lo schermo in remoto al fine di identificare e risolvere i problemi. Questo strumento è di sola visualizzazione. AWS Support non può agire per tuo conto durante la sessione di condivisione dello schermo. È necessario fornire il consenso per condividere lo schermo con un agente dell'assistenza. Per ulteriori informazioni, consulta le domande frequenti su AWS Support.
- Puoi modificare il tuo AWS Support piano per ottenere l'assistenza di cui hai bisogno per il tuo account. Per ulteriori informazioni, consulta Confronto AWS Support dei piani e Modifica del AWS Support piano.

Gestione delle identità e degli accessi per AWS Support

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori

IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Support IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

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

Utente del servizio: se utilizzi il AWS Support servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Support 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 Support, consulta Risoluzione dei problemi di AWS Support identità e accesso.

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

come la tua azienda può utilizzare IAM con AWS Support, consultaCome AWS Support funziona con IAM.

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

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

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

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

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

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

AWS account utente root

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

Utenti e gruppi IAM

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

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

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

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per

ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

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

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

  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

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

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore

IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

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

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le

policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

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

Come AWS Support funziona con IAM

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

Per informazioni su come gestire l'accesso per l' AWS Support utilizzo di IAM, consulta Manage access for AWS Support.

Argomenti

- Policy AWS Support basate su identità
- AWS Support Ruoli IAM

Policy AWS Support basate su identità

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

Azioni

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

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

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

Le azioni politiche AWS Support utilizzano il seguente prefisso prima dell'azione:`support:`. Ad esempio, per concedere a qualcuno l'autorizzazione per eseguire un'istanza Amazon EC2 con l'operazione API `RunInstances` Amazon EC2, è necessario includere l'operazione `ec2:RunInstances` nella policy. Le istruzioni delle policy devono includere un elemento `Action` o `NotAction`. AWS Support definisce un proprio set di operazioni che descrivono le attività che puoi eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "ec2:Describe*"
```

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

Esempi

Per visualizzare esempi di politiche AWS Support basate sull'identità, consulta. AWS Support esempi di politiche basate sull'identità

AWS Support Ruoli IAM

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

Utilizzo di credenziali temporanee con AWS Support

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

AWS Support supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

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

AWS Support supporta ruoli collegati ai servizi. Per informazioni dettagliate sulla creazione o la gestione di ruoli AWS Support collegati ai servizi, vedere. Utilizzo di ruoli collegati ai servizi per AWS Support

Ruoli dei servizi

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

AWS Support supporta i ruoli di servizio.

AWS Support esempi di politiche basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse AWS Support . Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o. AWS Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

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

Argomenti

Best practice delle policy

Le policy basate su identità sono molto efficaci. Determinano se qualcuno può creare, accedere o eliminare AWS Support risorse nel tuo account. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia a utilizzare le politiche AWS gestite: per iniziare a utilizzare AWS Support rapidamente, utilizza le politiche AWS gestite per concedere ai dipendenti le autorizzazioni di cui hanno bisogno. Queste policy sono già disponibili nell'account e sono gestite e aggiornate da AWS. Per ulteriori informazioni, consulta Introduzione all'utilizzo delle autorizzazioni con policy AWS gestite nella Guida per l'utente IAM.
- Assegnare il privilegio minimo: quando si creano policy personalizzate, concedere solo le autorizzazioni richieste per eseguire un'attività. Inizia con un set di autorizzazioni minimo e concedi autorizzazioni aggiuntive quando necessario. Questo è più sicuro che iniziare con autorizzazioni che siano troppo permissive e cercare di limitarle in un secondo momento. Per ulteriori informazioni, consulta Assegnare il privilegio minimo nella Guida per l'utente di IAM.
- Abilitare MFA per operazioni sensibili– Per una maggiore sicurezza, richiedere agli utenti IAM di utilizzare l'autenticazione a più fattori (MFA) per accedere a risorse sensibili o operazioni API. Per ulteriori informazioni, consulta Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.
- Utilizzare le condizioni della policy per ulteriore sicurezza – Per quanto possibile, definire le condizioni in cui le policy basate su identità consentono l'accesso a una risorsa. Ad esempio, è possibile scrivere condizioni per specificare un intervallo di indirizzi IP consentiti dai quali deve provenire una richiesta. È anche possibile scrivere condizioni per consentire solo le richieste all'interno di un intervallo di date o ore specificato oppure per richiedere l'utilizzo di SSL o MFA. Per ulteriori informazioni, consultare Elementi delle policy JSON di IAM: Condizioni nella Guida per l'utente di IAM.

Utilizzo della console di AWS Support

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

Per assicurarti che tali entità possano ancora utilizzare la AWS Support console, allega anche la seguente politica AWS gestita alle entità. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

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

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

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

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

Uso di ruoli collegati ai servizi

AWS Support e AWS Trusted Advisor usa ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un ruolo IAM unico collegato direttamente a e. AWS Support Trusted Advisor In ogni caso, il ruolo collegato ai servizi è un ruolo predefinito. Questo ruolo include tutte le autorizzazioni necessarie AWS Support o Trusted Advisor necessarie per chiamare altri AWS servizi per tuo conto. I seguenti argomenti spiegano cosa fanno i ruoli collegati ai servizi e come utilizzarli in and. AWS Support Trusted Advisor

Argomenti

- Utilizzo di ruoli collegati ai servizi per AWS Support
- Utilizzo di ruoli collegati ai servizi per Trusted Advisor

Utilizzo di ruoli collegati ai servizi per AWS Support

AWS Support gli strumenti raccolgono informazioni sulle AWS risorse dell'utente tramite chiamate API per fornire assistenza clienti e supporto tecnico. Per aumentare la trasparenza e la verificabilità delle attività di supporto, AWS Support utilizza un ruolo collegato ai servizi AWS Identity and Access Management (IAM).

Il ruolo `AWSServiceRoleForSupport` collegato al servizio è un ruolo IAM unico a cui è collegato direttamente. AWS Support Questo ruolo collegato al servizio è predefinito e include le autorizzazioni necessarie per chiamare altri servizi per AWS Support tuo conto. AWS

Ai fini dell'assunzione del ruolo `AWSServiceRoleForSupport`, il ruolo collegato ai servizi `support.amazonaws.com`considera attendibile il servizio.

Per fornire questi servizi, le autorizzazioni predefinite del ruolo danno AWS Support accesso ai metadati delle risorse, non ai dati dei clienti. Solo AWS Support gli strumenti possono assumere questo ruolo, che esiste all'interno del tuo account. AWS

Abbiamo redatto campi che potrebbero contenere i dati dei clienti. Ad esempio, i `Output` campi `Input` e della GetExecutioncronologia per la chiamata AWS Step Functions API non sono visibili AWS Support. Usiamo AWS KMS keys per crittografare i campi sensibili. Questi campi sono oscurati nella risposta dell'API e non sono visibili agli AWS Support agenti.

> **Note**
>
> AWS Trusted Advisor utilizza un ruolo separato collegato ai servizi IAM per accedere alle AWS risorse del tuo account e fornire consigli e verifiche sulle migliori pratiche. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Trusted Advisor.

Il ruolo `AWSServiceRoleForSupport` collegato al servizio consente a tutte le chiamate AWS Support API di essere visibili ai clienti tramite. AWS CloudTrail Questo aiuta a soddisfare i requisiti di monitoraggio e controllo, poiché fornisce un modo trasparente per comprendere le azioni che vengono eseguite per conto dell' AWS Support utente. Per informazioni in merito CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Autorizzazioni del ruolo collegato ai servizi per AWS Support

Questo ruolo utilizza la politica `AWSSupportServiceRolePolicy` AWS gestita. Questa policy gestita è attribuita al ruolo e dà l'autorizzazione al ruolo di completare operazioni per tuo conto.

Queste operazioni possono includere:

- Fatturazione, amministrazione, assistenza e altri servizi clienti: il servizio AWS clienti utilizza le autorizzazioni concesse dalla politica gestita per eseguire una serie di servizi come parte del piano di supporto. Ciò implica analizzare e rispondere a domande sull'account e sulla fatturazione, fornire supporto amministrativo per l'account, aumentare le quote dei servizi e offrire ulteriore supporto al cliente.
- Elaborazione degli attributi del servizio e dei dati di utilizzo per l' AWS account: AWS Support potrebbe utilizzare le autorizzazioni concesse dalla politica gestita per accedere agli attributi del servizio e ai dati di utilizzo per l'account. AWS Questa politica consente di AWS Support fornire supporto tecnico, amministrativo e di fatturazione per l'account. Gli attributi di servizio includono gli

identificatori delle risorse, i tag dei metadati, i ruoli e le autorizzazioni dell'account. I dati di utilizzo includono le policy di utilizzo, le statistiche sull'utilizzo e analisi.

- Mantenimento dello stato operativo dell'account e delle relative risorse: AWS Support utilizza strumenti automatizzati per eseguire azioni relative al supporto operativo e tecnico.

Per ulteriori informazioni sui servizi e le operazioni consentite, consulta la policy AWSSupportServiceRolePolicy nella console IAM.

> **Note**
>
> AWS Support aggiorna automaticamente la `AWSSupportServiceRolePolicy` politica una volta al mese per aggiungere autorizzazioni per nuovi AWS servizi e azioni.

Per ulteriori informazioni, consulta AWS politiche gestite per AWS Support.

Creazione di un ruolo collegato al servizio per AWS Support

Non devi creare manualmente il ruolo `AWSServiceRoleForSupport`. Quando crei un AWS account, questo ruolo viene creato e configurato automaticamente per te.

> **Important**
>
> Se lo utilizzavi AWS Support prima che iniziasse a supportare ruoli collegati ai servizi, allora hai AWS creato il `AWSServiceRoleForSupport` ruolo nel tuo account. Per ulteriori informazioni, consulta Comparsa di un nuovo ruolo nell'account IAM.

Modifica ed eliminazione di un ruolo collegato al servizio per AWS Support

È possibile utilizzare IAM per modificare la descrizione del ruolo collegato ai servizi `AWSServiceRoleForSupport`. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Il `AWSServiceRoleForSupport` ruolo è necessario per AWS Support fornire supporto amministrativo, operativo e tecnico per l'account. Di conseguenza, questo ruolo non può essere eliminato tramite la console IAM, l'API o AWS Command Line Interface (AWS CLI). In questo modo il tuo account AWS è protetto, perché non è possibile rimuovere inavvertitamente le autorizzazioni necessarie per amministrare i servizi di supporto.

Per ulteriori informazioni sul ruolo `AWSServiceRoleForSupport` o sui suoi utilizzi, contatta AWS Support.

Utilizzo di ruoli collegati ai servizi per Trusted Advisor

AWS Trusted Advisor utilizza il ruolo collegato al servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un ruolo IAM unico a cui è collegato direttamente. AWS Trusted Advisor I ruoli collegati ai servizi sono predefiniti da Trusted Advisor e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS Trusted Advisor utilizza questo ruolo per verificare l'utilizzo da parte dell'utente AWS e fornire consigli per migliorare l'ambiente. AWS Ad esempio, Trusted Advisor analizza l'utilizzo dell'istanza Amazon Elastic Compute Cloud (Amazon EC2) per aiutarti a ridurre i costi, aumentare le prestazioni, tollerare i guasti e migliorare la sicurezza.

> **Note**
>
> AWS Support utilizza un ruolo separato collegato ai servizi IAM per accedere alle risorse del tuo account e fornire servizi di fatturazione, amministrazione e supporto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Support.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS supportati da IAM. Cerca i servizi che hanno Sì nella colonna Ruolo collegato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Argomenti

- Autorizzazioni del ruolo collegato ai servizi per Trusted Advisor
- Gestione dei permessi per ruoli collegati ai servizi
- Creazione di un ruolo collegato ai servizi per Trusted Advisor
- Modifica di un ruolo collegato ai servizi per Trusted Advisor
- Eliminazione di un ruolo collegato ai servizi per Trusted Advisor

Autorizzazioni del ruolo collegato ai servizi per Trusted Advisor

Trusted Advisor utilizza due ruoli collegati ai servizi:

- AWSServiceRoleForTrustedAdvisor— Questo ruolo prevede che il Trusted Advisor servizio assuma il ruolo di accedere ai AWS servizi per conto dell'utente. La politica di autorizzazione dei ruoli consente l'accesso in Trusted Advisor sola lettura a tutte le risorse. AWS Questo ruolo semplifica le operazioni iniziali con l' AWS account, in quanto non è necessario aggiungere le autorizzazioni necessarie per. Trusted Advisor Quando apri un AWS account, Trusted Advisor crea questo ruolo per te. Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Le policy di autorizzazioni non possono essere attribuite a nessun'altra entità IAM.

  Per ulteriori informazioni sulla politica allegata, vedere AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting: Questo ruolo consente al servizio Trusted Advisor di assumere il ruolo per la funzionalità di visualizzazione dell'organizzazione. Questo ruolo Trusted Advisor funge da servizio affidabile all'interno AWS Organizations dell'organizzazione. Trusted Advisor crea questo ruolo per te quando abiliti la visualizzazione organizzativa.

  Per ulteriori informazioni sulla policy attribuita, consulta la sezione AWSTrustedAdvisorReportingServiceRolePolicy.

  È possibile utilizzare la visualizzazione organizzativa per creare report per Trusted Advisor controllare i risultati di tutti gli account dell'organizzazione. Per ulteriori informazioni sull'utilizzo di questa caratteristica, consulta Visualizzazione organizzativa per AWS Trusted Advisor.

Gestione dei permessi per ruoli collegati ai servizi

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Gli esempi seguenti utilizzano il ruolo collegato ai servizi `AWSServiceRoleForTrustedAdvisor`.

Example : Consentire a un'entità IAM di creare il ruolo collegato ai servizi **`AWSServiceRoleForTrustedAdvisor`**

Questo passaggio è necessario solo se l' Trusted Advisor account è disabilitato, il ruolo collegato al servizio viene eliminato e l'utente deve ricreare il ruolo per riattivarlo. Trusted Advisor

Puoi aggiungere la seguente istruzione alla policy delle autorizzazioni per permettere all'entità IAM di creare il ruolo collegato ai servizi.

```
{
    "Effect": "Allow",
    "Action": [
```

```
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Consentire a un'entità IAM di modificare la descrizione del ruolo collegato ai servizi **`AWSServiceRoleForTrustedAdvisor`**

Puoi modificare solo la descrizione per ruolo `AWSServiceRoleForTrustedAdvisor`. Puoi aggiungere la seguente istruzione alla policy delle autorizzazioni per permettere all'entità IAM di modificare la descrizione di un ruolo collegato ai servizi.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Consentire a un'entità IAM di eliminare il ruolo collegato ai servizi **`AWSServiceRoleForTrustedAdvisor`**

Aggiungi la seguente istruzione alla policy delle autorizzazioni per permettere all'entità IAM di eliminare un ruolo collegato ai servizi.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

È inoltre possibile utilizzare una politica AWS gestita, ad esempio per fornire l'AdministratorAccessaccesso completo a. Trusted Advisor

Creazione di un ruolo collegato ai servizi per Trusted Advisor

Non devi creare manualmente il ruolo collegato al servizio `AWSServiceRoleForTrustedAdvisor`. Quando apri un AWS account, Trusted Advisor crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Se utilizzavi il Trusted Advisor servizio prima che iniziasse a supportare i ruoli collegati al servizio, allora hai Trusted Advisor già creato il `AWSServiceRoleForTrustedAdvisor` ruolo nel tuo account. Per ulteriori informazioni, consulta Comparsa di un nuovo ruolo nell'account IAM nella Guida per l'utente IAM.

Se l'account non ha un ruolo collegato ai servizi `AWSServiceRoleForTrustedAdvisor` collegato ai servizi, Trusted Advisor non funzionerà nel modo previsto. Questo potrebbe accadere se qualcuno nell'account ha disabilitato Trusted Advisor e ha eliminato il ruolo collegato ai servizi. In questo caso è possibile utilizzare IAM per creare il ruolo collegato ai servizi `AWSServiceRoleForTrustedAdvisor` collegato ai servizi per poi riabilitare Trusted Advisor.

Da abilitare Trusted Advisor (console)

1. Utilizza la console IAM o AWS CLI l'API IAM per creare un ruolo collegato al servizio per. Trusted Advisor Per ulteriori informazioni, consultare la pagina relativa alla creazione di un ruolo collegato ai servizi.
2. Accedi a AWS Management Console, quindi accedi alla Trusted Advisor console all'indirizzo. https://console.aws.amazon.com/trustedadvisor

   Nella console viene visualizzato il banner che indica lo stato Disabled Trusted Advisor (Truster Advisor disabilitato).
3. Scegli Abilita Trusted Advisor ruolo dal banner di stato. Se il `AWSServiceRoleForTrustedAdvisor` richiesto non viene rilevato, il banner di stato rimane disabilitato.

Modifica di un ruolo collegato ai servizi per Trusted Advisor

Dopo aver creato un ruolo collegato ai servizi, non è possibile modificarne il nome, perché potrebbero riferirvisi diverse entità. Tuttavia, puoi utilizzare la console IAM o l'API IAM per modificare la descrizione del ruolo. AWS CLI Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Trusted Advisor

Se non è necessario utilizzare le funzionalità o i servizi di Trusted Advisor, puoi eliminare il `AWSServiceRoleForTrustedAdvisor` ruolo. È necessario disattivarlo Trusted Advisor prima di poter eliminare questo ruolo collegato al servizio. Questo ti impedisce di rimuovere le autorizzazioni necessarie per eseguire le operazioni di Trusted Advisor . Quando si disattiva Trusted Advisor, si disattivano tutte le funzionalità del servizio, tra cui l'elaborazione e le notifiche offline. Inoltre, se disattivi Trusted Advisor un account membro, ne risentirà anche l'account di pagamento separato, il che significa che non riceverai Trusted Advisor assegni che identificano i modi per risparmiare sui costi. Non è possibile accedere alla console Trusted Advisor . Chiamate API per Trusted Advisor restituire un errore di accesso negato.

È necessario ricreare il ruolo collegato ai servizi `AWSServiceRoleForTrustedAdvisor` collegato ai servizi nell'account prima di poter riabilitare Trusted Advisor.

È necessario innanzitutto disabilitarlo Trusted Advisor nella console prima di poter eliminare il ruolo `AWSServiceRoleForTrustedAdvisor` collegato al servizio.

Per disabilitare Trusted Advisor

1. Accedi a AWS Management Console e vai alla Trusted Advisor console all'indirizzohttps://console.aws.amazon.com/trustedadvisor.
2. Nel riquadro di navigazione, scegli Preferences (Preferenze).
3. Nella sezione Service Linked Role Permissions (Autorizzazioni del ruolo collegato ai servizi), selezionare Disable Trusted Advisor(Disabilita &SERVICENAME;).
4. Nella finestra di dialogo di conferma, clicca su OK per disabilitare Trusted Advisor.

Dopo la disattivazione Trusted Advisor, tutte le Trusted Advisor funzionalità vengono disattivate e la Trusted Advisor console visualizza solo il banner di stato di disabilitazione.

Puoi quindi utilizzare la console IAM AWS CLI, l'o l'API IAM per eliminare il ruolo Trusted Advisor collegato al servizio denominato. `AWSServiceRoleForTrustedAdvisor` Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

AWS politiche gestite per AWS Support

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

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

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

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

Argomenti

AWS politiche gestite per AWS Support

AWS Support dispone delle seguenti politiche gestite.

Indice

- Modifica delle autorizzazioni per AWSSupportServiceRolePolicy

AWS politica gestita: AWSSupportServiceRolePolicy

AWS Support utilizza la politica AWSSupportServiceRolePolicy AWS gestita. Questa policy gestita è attribuita al ruolo collegato ai servizi `AWSServiceRoleForSupport`. La policy consente al ruolo collegato ai servizi di completare operazioni per tuo conto. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi per AWS Support.

Per un elenco delle modifiche della policy, consulta AWS Support aggiornamenti alle politiche AWS gestite e Modifica delle autorizzazioni per AWSSupportServiceRolePolicy.

AWS Support aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Support da quando questi servizi hanno iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti.

La tabella seguente descrive importanti aggiornamenti alle politiche AWS Support gestite dal 17 febbraio 2022.

AWS Support

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 17 nuove autorizzazioni ai seguenti servizi per eseguire azioni che aiutano a risolvere i problemi dei clienti relativi alla fatturazione, all'assistenza amministrativa e tecnica: • Amazon CloudWatch Network Monitor: per	22 marzo 2024

Modifica	Descrizione	Data
	risolvere i problemi relativi al servizio Network Monitor. • Amazon CloudWatch Logs: per eseguire il debug di problemi relativi ad Amazon CloudWatch Logs. • Amazon Managed Streaming for Apache Kafka: per eseguire il debug di problemi relativi ad Amazon Managed Streaming for Apache Kafka. • Amazon Managed Service for Prometheus: per risolvere i problemi relativi ad Amazon Managed Service for Prometheus.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 63 nuove autorizzazioni ai seguenti servizi per eseguire azioni che aiutano a risolvere i problemi dei clienti relativi alla fatturazione, all'amministrazione e al supporto tecnico: • AWS Camere bianche: per risolvere i problemi relativi alle camere bianche. AWS • CodeConnections — Per risolvere i problemi relativi a. CodeConnections • Amazon EKS: per eseguire il debug di problemi relativi ad Amazon EKS. • Image Builder: per eseguire il debug di problemi relativi a Image Builder. • Amazon Inspector2: per risolvere i problemi relativi ad Amazon Inspector2. • Amazon Inspector Scan: per eseguire il debug di problemi relativi ad Amazon Inspector Scan. • Amazon CloudWatch Logs: per risolvere i problemi relativi ad Amazon Logs. CloudWatch	17 gennaio 2024

Modifica	Descrizione	Data
	• AWS Outposts — Per risolvere i problemi relativi a. AWS Outposts • Amazon RDS: esecuzione e del debug di problemi relativi ad Amazon RDS. • AWS IAM Identity Center — Per risolvere i problemi relativi a. AWS IAM Identity Center • Amazon S3 Express: per eseguire il debug di problemi relativi ad Amazon S3 Express. • AWS Trusted Advisor — Per risolvere i problemi relativi a. AWS Trusted Advisor	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 126 nuove autorizzazioni ai seguenti servizi per eseguire azioni che aiutano a risolvere i problemi dei clienti relativi alla fatturazione, all'amministrazione e al supporto tecnico: • AWS Direct Connect — Per risolvere i problemi relativi al servizio. AWS Direct Connect • Amazon SageMaker : per risolvere i problemi relativi al servizio Amazon SageMaker . • Amazon AppStream : per eseguire il debug di problemi relativi ad Amazon AppStream. • Esploratore di risorse AWS — Per eseguire il debug di problemi relativi a. Esploratore di risorse AWS • Amazon Redshift serverless: per risolvere i problemi relativi ad Amazon Redshift serverless. • Amazon ElastiCache : per eseguire il debug di problemi relativi ad Amazon ElastiCache.	6 dicembre 2023

Modifica	Descrizione	Data
	• Amazon Comprehend: per risolvere problemi relativi ad Amazon Comprehend. • Amazon EC2: per risolvere i problemi relativi ad Amazon EC2. • Amazon Elastic Kubernetes Service: per eseguire il debug di problemi relativi ad Amazon Elastic Kubernetes Service. • AWS Elastic Disaster Recovery — Per risolvere problemi relativi a. AWS Elastic Disaster Recovery • AWS AppSync — Per eseguire il debug di problemi relativi a. AWS AppSync • Amazon CloudWatch Logs: per risolvere i problemi relativi ad Amazon Logs. CloudWatch • AWS Health — Per eseguire il debug di problemi relativi al Servizio. AWS Health • Amazon Connect: per eseguire il debug di problemi relativi ad Amazon Connect. • AWS Snowball — Per risolvere i problemi relativi a. AWS Snowball	

Modifica	Descrizione	Data
	• AWS Health Imaging: per risolvere i problemi relativi all'imaging. AWS Health	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 163 nuove autorizzazioni ai seguenti servizi per l'esecuzione di azioni che facilitano la soluzione di problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • Amazon CloudFront : per risolvere i problemi relativi al CloudFront servizio. • Amazon EC2: risoluzione di problemi relativi al servizio di Amazon EC2. • Amazon AppStream : per eseguire il debug di problemi relativi ad Amazon AppStream. • AWS WAF — Per eseguire il debug di problemi relativi al AWS Web Application Firewall. • Amazon Connect: risoluzione di problemi relativi ad Amazon Connect. • AWS IoT — Per eseguire il debug di problemi relativi a. AWS IoT • Amazon Route 53: risoluzione di problemi relativi ad Amazon Route 53.	27 ottobre 2023

Modifica	Descrizione	Data
	• AWS Accesso verificato: per risolvere i problemi relativi al servizio di accesso AWS verificato. • Amazon Simple Email Service: esecuzione del debug di problemi relativi ad Amazon Simple Email Service. • AWS Elastic Beanstalk — Per risolvere i problemi relativi a. AWS Elastic Beanstalk • Amazon DynamoDB: esecuzione del debug di problemi relativi ad Amazon DynamoDB. • AWS EC2 Image Builder — Per risolvere i problemi relativi a AWS EC2 Image Builder. • AWS Outposts — Per eseguire il debug di problemi relativi al Servizio. AWS Outposts • AWS Glue — Per eseguire il debug di problemi relativi a. AWS Glue • AWS Directory Service — Per risolvere i problemi relativi a. AWS Directory Service	

Modifica	Descrizione	Data
	• AWS Elastic Disaster Recovery — Per risolvere i problemi relativi a. AWS Elastic Disaster Recovery • AWS Step Functions — Per eseguire il debug di problemi relativi a. AWS Step Functions • Amazon EMR: risoluzione problemi relativi ad Amazon EMR. • Amazon Relational Database Service: risoluzione di problemi relativi ad Amazon Relational Database Service. • Amazon EC2 Systems Manager: esecuzione del debug di problemi relativi ad Amazon EC2 Systems Manager.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 176 nuove autorizzazioni ai seguenti servizi per l'esecuzione di azioni che facilitano la soluzione di problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • AWS Glue — Per risolvere i problemi relativi al servizio AWS Glue • Amazon EMR: risoluzione problemi relativi al servizio Amazon EMR. • Amazon Security Lake: esecuzione del debug di problemi relativi ad Amazon Security Lake. • AWS Systems Manager — Per eseguire il debug di problemi relativi al servizio Systems Manager. • Autorizzazioni verificate da Amazon: risoluzione di problemi relativi ad Autorizzazioni verificate da Amazon. • AWS IAM Access Analyzer: per eseguire il debug dei problemi relativi al servizio IAM Access Analyzer.	28 agosto 2023

Modifica	Descrizione	Data
	• AWS Backup — Per risolvere i problemi relativi a. AWS Backup • AWS Database Migration Service — Per risolvere i problemi relativi al servizio DMS. • Amazon DynamoDB: esecuzione del debug di problemi relativi a DynamoDB. • Amazon Elastic Container Registry (Amazon ECR): risoluzione di problemi relativi ad Amazon Elastic Container Registry (Amazon ECR). • Servizio di Amazon Elastic Container: esecuzione del debug di problemi relativi al servizio di Amazon Elastic Container. • Servizio di Amazon Elastic Kubernetes: risoluzio ne di problemi relativi al servizio di Amazon Elastic Kubernetes. • Amazon EMR Serverless: esecuzione del debug di problemi relativi al servizio di Amazon EMR Serverless. • AWS Identity and Access Management — Per	

Modifica	Descrizione	Data
	risolvere i problemi relativi a. AWS Identity and Access Management • AWS Network Firewall: per risolvere i problemi relativi al AWS Network Firewall. • AWS HealthOmics — Per eseguire il debug di problemi relativi a. AWS HealthOmics • Amazon QuickSight : per eseguire il debug di problemi relativi ad Amazon QuickSight. • Amazon Relational Database Service: risoluzione di problemi relativi ad Amazon Relational Database Service. • Amazon Redshift: risoluzione dei problemi relativi ad Amazon Redshift. • Amazon Redshift Serverless: esecuzione del debug di problemi relativi al servizio di Amazon Redshift Serverless. • Amazon SageMaker : per eseguire il debug di problemi relativi ad Amazon SageMaker.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 141 nuove autorizzazioni ai seguenti servizi per l'esecuzione di azioni che facilitano la soluzione di problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • Lambda: risoluzione di problemi relativi al servizio Lambda. • Amazon Lex: risoluzione di problemi relativi al servizio Amazon Lex. • AWS Trasferimento: per eseguire il debug dei problemi relativi al servizio Transfer. • AWS Amplify — Per eseguire il debug di problemi relativi al servizio Amplify. • Amazon EventBridge Pipes: per risolvere i problemi di autorizzazione e fatturazione relativi a Pipes. • Amazon EventBridge : per eseguire il debug di problemi relativi ad Amazon EventBridge • Amazon CloudWatch Logs: per risolvere i problemi	26 giugno 2023

Modifica	Descrizione	Data
	relativi ad Amazon Logs. CloudWatch • AWS Systems Manager — Per risolvere i problemi relativi a Systems Manager. • Amazon CloudWatch : per eseguire il debug di problemi relativi a CloudWatch. • Amazon ElastiCache : per risolvere i problemi relativi ad Amazon. ElastiCache • Amazon Athena: esecuzione e del debug di problemi relativi ad Athena. • AWS Elastic Disaster Recovery — Per risolvere i problemi relativi a Elastic Disaster Recovery. • Amazon CloudWatch : per risolvere i problemi relativi alle configurazioni di Amazon. CloudWatch • Amazon EC2: esecuzione e del debug di problemi relativi al servizio EC2. • AWS Certificate Manager — Per risolvere i problemi relativi a Certificate Manager. • Amazon EventBridge Scheduler: per risolvere i	

Modifica	Descrizione	Data
	problemi relativi a Scheduler . EventBridge • Amazon OpenSearch Service: per risolvere i problemi relativi a. OpenSearch • Amazon EventBridge Schemas: per eseguire il debug di problemi relativi agli EventBridge schemi. • AWS Notifiche utente: per risolvere i problemi relativi alle notifiche utente. • Amazon CloudWatch Application Insights: per risolvere i problemi relativi ad CloudWatch Application Insights. • Amazon DynamoDB: risoluzione di problemi relativi a DynamoDB. • Cluster elastici di Amazon DocumentDB: risoluzione di problemi relativi ai cluster Elastic DocumentDB.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 53 nuove autorizzazioni ai seguenti servizi per l'esecuzione di azioni che facilitano la soluzione di problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • Dimensionamento automatico: risoluzione di problemi relativi al servizio di dimensionamento automatico. • Amazon CloudWatch : per risolvere i problemi relativi ad Amazon. CloudWatch • AWS Compute Optimizer — Per risolvere i problemi relativi a Compute Optimizer . • Amazon CloudWatch Evidently — Per risolvere i problemi relativi a Evidently. • EC2 Image Builder: risoluzione di problemi relativi al servizio Image Builder. • AWS IoT TwinMaker — Per risolvere i problemi relativi a. AWS IoT TwinMaker • Amazon CloudWatch Logs: per risolvere i problemi relativi ad Amazon Logs. CloudWatch	02 maggio 2023

Modifica	Descrizione	Data
	• Amazon Pinpoint: per risolvere problemi relativi ad Amazon Pinpoint. • AWS OAM Link: per eseguire il debug di problemi relativi alle risorse OAM. • AWS Outposts — Per risolvere i problemi relativi a. AWS Outposts • Amazon RDS: esecuzion e del debug di problemi relativi ad Amazon RDS. • Esploratore di risorse AWS — Per risolvere i problemi relativi a Resource Explorer. • Amazon CloudWatch RUM: per risolvere i problemi di configurazione delle risorse del servizio RUM. • Amazon SNS: risoluzione problemi relativi ad Amazon SNS. • Amazon CloudWatch Synthetics: per risolvere i problemi relativi a Synthetic s. CloudWatch	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 52 nuove autorizzazioni ai seguenti servizi per l'esecuzione di azioni che facilitano la soluzione di problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • AWS Backup gateway — Per risolvere i problemi relativi al gateway di Backup. • Amazon S3: esecuzione del debug di problemi relativi ad Amazon S3. • AWS Application Migration Service — Per risolvere i problemi relativi al servizio di migrazione delle applicazioni. • AWS Camere pulite: per eseguire il debug dei problemi relativi alle AWS camere pulite; • AWS Systems Manager per SAP: per risolvere i problemi relativi a SAP. AWS Systems Manager • Amazon VPC Lattice: esecuzione del debug di problemi relativi ad Amazon VPC Lattice.	16 marzo 2023

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 220 nuove autorizzazioni ai seguenti servizi per eseguire azioni che contribuiscono a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • Amazon Athena: per consentire lo sviluppo AWS Support di strumenti che possono essere utilizzati per aiutare i clienti con le loro domande relative ad Athena. • Amazon Chime: per risolvere problemi relativi ad Amazon Chime. • Amazon CloudWatch Internet Monitor: per eseguire il debug di problemi relativi a Internet Monitor. • Amazon Comprehend: per risolvere problemi relativi ad Amazon Comprehend. • Amazon Elastic Compute Cloud: per eseguire il debug di problemi relativi a Transit Gateway Connect e alle funzionalità multicast (trasmissione uno a molti).	10 gennaio 2023

Modifica	Descrizione	Data
	• Amazon EventBridge Pipes: per risolvere i problemi relativi a EventBridge Pipes. • Amazon Interactive Video Service: AWS Support per consentire di interrogare le risorse Amazon IVS per risolvere i problemi dei clienti. • Amazon FSx: per consentire lo sviluppo di strumenti AWS Support per supportare l'importazione e l'esportazione per un repository di dati Amazon FSx. • Amazon GameLift : per risolvere i problemi relativi ad Amazon. GameLift • AWS Glue: per risolvere problemi relativi alla Qualità dei dati AWS Glue . • Flusso di video Amazon Kinesis: per risolvere problemi relativi ai flussi di video Kinesis. • Amazon Managed Service for Prometheus: per risolvere problemi relativi ad Amazon Managed Service for Prometheus. • Amazon Managed Streaming for Apache Kafka: per risolvere	

Modifica	Descrizione	Data
	problemi relativi ad Amazon MSK Connect. • AWS Network Manager — Per risolvere i problemi relativi a Network Manager. • Amazon Nimble Studio: per eseguire il debug di problemi relativi a Nimble Studio. • Amazon Personalize: per eseguire il debug di problemi relativi ad Amazon Personalize. • Amazon Pinpoint: per risolvere problemi relativi ad Amazon Pinpoint. • AWS HealthOmics — Per risolvere i problemi relativi a. HealthOmics • Amazon Transcribe: per eseguire il debug di problemi relativi ad Amazon Transcribe.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 47 nuove autorizzazioni ai seguenti servizi per eseguire operazioni che contribuiscono a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • AWS Application Migration Service — Per risolvere i problemi di replica e avvio. • AWS CloudFormation ganci: consentono lo sviluppo di strumenti AWS Support di automazione in grado di aiutare a risolvere i problemi. • Amazon Elastic Kubernetes Service: per risolvere i problemi relativi ad Amazon EKS. • AWS IoT FleetWise: risoluzione di problemi relativi a AWS IoT FleetWise. • AWS Mainframe Modernization — Per eseguire il debug di problemi relativi alla modernizzazione del mainframe. • AWS Outposts — Per aiutare a AWS Support ottenere un elenco di host e risorse dedicati.	4 ottobre 2022

Modifica	Descrizione	Data
	• AWS Private 5G: risoluzione di problemi relativi a Private 5G. • AWS Tiros: per eseguire il debug dei problemi relativi a Tiros.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 46 nuove autorizzazioni ai seguenti servizi per eseguire operazioni che contribuiscono a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • Amazon Managed Streaming for Apache Kafka: per risolvere i problemi relativi ad Amazon MSK. • AWS DataSync — Per risolvere i problemi relativi a. DataSync • AWS Elastic Disaster Recovery — Per risolvere i problemi di replica e avvio. • Amazon GameSparks : per risolvere i problemi relativi a. GameSparks • AWS IoT TwinMaker — Per eseguire il debug di problemi relativi a. AWS IoT TwinMaker • AWS Lambda — Per visualizzare la configura zione dell'URL di una funzione per la risoluzione dei problemi. • Amazon Lookout per le apparecchiature: per risolvere i problemi relativi	17 agosto 2022

Modifica	Descrizione	Data
	a Lookout per le apparecch iature. • Amazon Route 53 e Amazon Route 53 Resolver: per ottenere configurazioni di resolver in modo AWS Support da controllare il comportamento di risoluzio ne DNS di un VPC.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte nuove autorizzazioni ai seguenti servizi per eseguire operazioni che aiutino a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • Amazon CloudWatch Logs: per aiutare a risolvere i problemi relativi ai CloudWatch log. • Amazon Interactive Video Service: per aiutarti a AWS Support controllare le risorse Amazon IVS esistenti per i casi di assistenza relativi a frodi o account compromessi. • Amazon Inspector: per risolvere i problemi relativi ad Amazon Inspector. Autorizzazioni rimosse per servizi come Amazon WorkLink. Amazon WorkLink è stato dichiarato obsoleto il 19 aprile 2022.	23 giugno 2022

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 25 nuove autorizzazioni ai seguenti servizi per eseguire operazioni che aiutino a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • AWS Amplify UI Builder: per risolvere i problemi relativi alla generazione di componenti e temi. • Amazon AppStream : per risolvere i problemi recuperando le risorse per le funzionalità lanciate di recente. • AWS Backup — Per risolvere i problemi relativi ai processi di backup. • AWS CloudFormation — Per eseguire la diagnostica su problemi relativi a IAM, estensione e controllo delle versioni. • Amazon Kinesis: per risolvere i problemi relativi a Kinesis. • AWS Transfer Family — Per risolvere i problemi relativi a Transfer Family.	27 aprile 2022

Modifica	Descrizione	Data

AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 54 nuove autorizzazioni ai seguenti servizi per eseguire operazioni che aiutino a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico:
	• Amazon Elastic Compute Cloud
	  • Per risolvere i problemi relativi al cliente e agli elenchi prefissati gestite da AWS.
	  • Per risolvere i problemi relativi ad Amazon VPC IP Address Manager (IPAM).
	• AWS Network Manager — Per risolvere i problemi relativi a Network Manager.
	• Savings Plans: ottenere metadati sugli impegni del Savings Plan in sospeso.
	• AWS Serverless Application Repository — Migliorare e supportare le azioni di risposta nell'ambito della ricerca e della risoluzione dei casi di supporto.
	• Amazon WorkSpaces Web: per eseguire il debug e
		14 marzo 2022

Modifica	Descrizione	Data
	risolvere i problemi relativi ai servizi Web. WorkSpaces	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte 74 nuove autorizzazioni ai seguenti servizi per eseguire operazioni che aiutino a risolvere i problemi dei clienti relativi a fatturazione, supporto amministrativo e tecnico: • AWS Application Migration Service — Per supportare la replica senza agenti nell'Application Migration Service. • AWS CloudFormation — Per eseguire la diagnostica su problemi relativi a IAM, estensioni e versioni. • Amazon CloudWatch Logs: per convalidare le politiche relative alle risorse. • Cestino di riciclaggio Amazon EC2 – Per ottenere metadati sulle regole di conservazione del Cestino di riciclaggio. • AWS Elastic Disaster Recovery — Per risolvere i problemi di replica e avvio negli account dei clienti. • Amazon FSx – Per visualizzare la descrizione degli snapshot di Amazon FSx. • Amazon Lightsail – Per visualizzare i dettagli dei	17 febbraio 2022

Modifica	Descrizione	Data
	metadati e delle configura zioni per i bucket Lightsail. • Amazon Macie – Per visualizzare le configura zioni Macie, come processi di classificazione, identific atori di dati personalizzati, espressioni regolari e risultati. • Simple Storage Service (Amazon S3) – Per raccogliere metadati e configurazioni per i bucket Simple Storage Service (Amazon S3). • AWS Storage Gateway — Per visualizzare i metadati sulle politiche di creazione automatica dei nastri dei clienti. • Elastic Load Balancing - Per visualizzare la descrizio ne dei limiti delle risorse quando si utilizza la console Service Quotas. Per ulteriori informazioni, consulta Modifica delle autorizzazioni per AWSSuppor tServiceRolePolicy.	
Log delle modifiche pubblicato	Registro delle modifiche per le politiche AWS Support gestite.	17 febbraio 2022

Modifica delle autorizzazioni per AWSSupportServiceRolePolicy

La maggior parte delle autorizzazioni è stata aggiunta AWS Support per `AWSSupportServiceRolePolicy` consentire di chiamare un'operazione API con lo stesso nome. Tuttavia, alcune operazioni API richiedono autorizzazioni con un nome diverso.

Nella tabella seguente sono elencate solo le operazioni API che richiedono autorizzazioni con un nome diverso. Questa tabella descrive queste differenze a partire dal 17 febbraio 2022.

Data	Nome operazione API	Policy autorizzazioni richieste
Aggiunte autorizzazioni il 17 febbraio 2022	`s3.GetBucketAnalyticsConfiguration` `s3.ListBucketAnalyticsConfiguration`	`s3:GetAnalyticsConfiguration`
	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`
	`s3.GetBucketEncryption`	`s3:GetEncryptionConfiguration`
	`s3.GetBucketIntelligentTieringConfiguration` `s3.ListBucketIntelligentTieringConfiguration`	`s3:GetIntelligentTieringConfiguration`
	`s3.GetBucketInventoryConfiguration` `s3.ListBucketInventoryConfiguration`	`s3:GetInventoryConfiguration`
	`s3.GetBucketLifecycleConfiguration`	`s3:GetLifecycleConfiguration`

Data	Nome operazione API	Policy autorizzazioni richieste
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS politiche gestite per AWS Support App in Slack

> **Note**
>
> Per accedere e visualizzare i casi di assistenza in AWS Support Center Console, consultaGestisci l'accesso al AWS Support Centro.

AWS Support L'app ha le seguenti politiche gestite.

Indice

- AWS politica gestita: AWSSupportAppReadOnlyAccess
- AWS Support Aggiornamenti delle app alle politiche gestite AWS

AWS politica gestita: AWSSupportAppFullAccess

Puoi utilizzare la policy gestita AWSSupportAppFullAccess per concedere al ruolo IAM le autorizzazioni per configurare i canali Slack. Puoi anche collegare la policy AWSSupportAppFullAccess alle tue entità IAM.

Per ulteriori informazioni, consulta AWS Support App in Slack.

Questa policy concede le autorizzazioni che consentono all'entità di eseguire AWS Support azioni Service Quotas e IAM per l'app. AWS Support

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `servicequotas`: descrive le richieste e le quote di servizio esistenti e crea aumenti della quota di servizio per l'account.
- `support`: crea, aggiorna e risolve i casi di supporto. Aggiorna e descrive le informazioni sui casi, ad esempio file allegati, corrispondenze e livelli di gravità. Avvia le sessioni di live chat con un agente dell'assistenza.
- `iam`: crea un ruolo collegato ai servizi per Service Quotas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
```

```
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Per ulteriori informazioni, consulta Gestione degli accessi all'app AWS Support.

AWS politica gestita: AWSSupportAppReadOnlyAccess

La AWSSupportAppReadOnlyAccesspolicy concede autorizzazioni che consentono all'entità di eseguire azioni relative all'app di sola lettura AWS Support . Per ulteriori informazioni, consulta AWS Support App in Slack.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `support`: descrive i dettagli e le comunicazioni dei casi di supporto aggiunti ai casi di supporto.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Support Aggiornamenti delle app alle politiche gestite AWS

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

La tabella seguente descrive importanti aggiornamenti alle politiche gestite dall' AWS Support app dal 17 agosto 2022.

AWS Support App

Modifica	Descrizione	Data
AWSSupportAppFullAccesse AWSSupportAppReadOnlyAccess Nuove politiche AWS gestite per l' AWS Support app	Puoi utilizzare queste policy per il ruolo IAM che configuri per la configurazione del canale Slack. Per ulteriori informazioni, consulta Gestione degli accessi all'app AWS Support.	19 agosto 2022
Log delle modifiche pubblicato	Registro delle modifiche per le politiche gestite AWS Support dall'app.	19 agosto 2022

AWS politiche gestite per AWS Trusted Advisor

Trusted Advisor dispone delle seguenti politiche AWS gestite.

Indice

AWS politica gestita: AWSTrustedAdvisorPriorityFullAccess

La AWSTrustedAdvisorPriorityFullAccesspolitica garantisce l'accesso completo a Trusted Advisor Priority. Questa politica consente inoltre all'utente di aggiungere Trusted Advisor come servizio affidabile AWS Organizations e di specificare gli account di amministratore delegato per Trusted Advisor Priority.

Dettagli dell'autorizzazione

Nella prima espressione, la policy include le seguenti autorizzazioni per `trustedadvisor`:

- Descrive l'account e l'organizzazione.
- Descrive i rischi identificati da Trusted Advisor Priority. Le autorizzazioni consentono di scaricare e aggiornare lo stato del rischio.
- Descrive le configurazioni per le notifiche e-mail Trusted Advisor Priority. Le autorizzazioni ti consentono di configurare le notifiche e-mail e di disabilitarle per gli amministratori delegati.
- Si configura Trusted Advisor in modo che il tuo account possa essere abilitato. AWS Organizations

Nella seconda espressione, la policy include le seguenti autorizzazioni per `organizations`:

- Descrive il tuo Trusted Advisor account e la tua organizzazione.
- Elenca le organizzazioni Servizi AWS che hai abilitato all'uso.

Nella terza espressione, la policy include le seguenti autorizzazioni per `organizations`:

- Elenca gli amministratori delegati per Trusted Advisor Priority.
- Abilita e disabilita l'accesso attendibile con Organizations.

Nella quarta espressione, la policy include le seguenti autorizzazioni per `iam`:

- Crea il ruolo collegato al servizio `AWSServiceRoleForTrustedAdvisorReporting`.

Nella quinta espressione, la policy include le seguenti autorizzazioni per `organizations`:

- Consente di registrare e annullare la registrazione degli amministratori delegati per Trusted Advisor Priority.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
```

```
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowRegisterDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
   ],
   "Resource": "arn:aws:organizations::*:*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
```

```
    }
   }
  ]
}
```

AWS politica gestita: AWSTrustedAdvisorPriorityReadOnlyAccess

La AWSTrustedAdvisorPriorityReadOnlyAccesspolitica concede autorizzazioni di sola lettura a Trusted Advisor Priority, inclusa l'autorizzazione a visualizzare gli account degli amministratori delegati.

Dettagli dell'autorizzazione

Nella prima espressione, la policy include le seguenti autorizzazioni per `trustedadvisor`:

- Descrive il tuo account e la tua organizzazione. Trusted Advisor
- Descrive i rischi identificati da Trusted Advisor Priority e consente di scaricarli.
- Descrive le configurazioni per le notifiche e-mail Trusted Advisor prioritarie.

Nella seconda e terza espressione, la policy include le seguenti autorizzazioni per `organizations`:

- Descrive la tua organizzazione in Organizations.
- Elenca le organizzazioni Servizi AWS che hai abilitato all'uso.
- Elenca gli amministratori delegati per Priority Trusted Advisor

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
```

```
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

Policy gestita da AWS : AWSTrustedAdvisorServiceRolePolicy

Questa policy è attribuita al ruolo collegato ai servizi `AWSServiceRoleForTrustedAdvisor`. Consente al ruolo collegato ai servizi di eseguire operazioni per tuo conto. Non puoi collegare la AWSTrustedAdvisorServiceRolePolicy alle tue entità AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Trusted Advisor.

Questa policy concede autorizzazioni amministrative che consentono al ruolo collegato ai servizi di accedere a Servizi AWS. Queste autorizzazioni consentono ai controlli di valutazione dell' Trusted Advisor account.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `accessanalyzer`— Descrive le risorse AWS Identity and Access Management Access Analyzer
- `Auto Scaling`: Descrive le quote e le risorse dell'account Amazon EC2 Auto Scaling
- `cloudformation`— Descrive AWS CloudFormation (CloudFormation) le quote e gli stack degli account
- `cloudfront`— Descrive le CloudFront distribuzioni Amazon
- `cloudtrail`— Descrive AWS CloudTrail (CloudTrail) percorsi
- `dynamodb`: Descrive le quote e le risorse dell'account Amazon DynamoDB
- `dynamodbaccelerator`— Descrive le risorse di DynamoDB Accelerator
- `ec2`: Descrive le quote e le risorse dell'account Amazon Elastic Compute Cloud (Amazon EC2)
- `elasticloadbalancing`: descrive le quote e le risorse di Elastic Load Balancing (ELB)
- `iam`: Ottiene risorse IAM, ad esempio credenziali, policy di password e certificati
- `networkfirewall`— Descrive le risorse AWS Network Firewall
- `kinesis`: Descrive le quote dell'account Amazon Kinesis (Kinesis)
- `rds`: Descrive le risorse Amazon Relational Database Service (Amazon RDS)
- `redshift`: Descrive le risorse Amazon Redshift
- `route53`: Descrive le quote e le risorse dell'account Amazon Route 53
- `s3`: Descrive le risorse Amazon Simple Storage Service (Amazon S3)
- `ses`: Ottiene le quote di invio Amazon Simple Email Service (Amazon SES)
- `sqs`: Elenca le code di Amazon Simple Queue Service (Amazon SQS)
- `cloudwatch`— Ottiene le statistiche dei parametri di Amazon CloudWatch CloudWatch Events (Events)
- `ce`: Ottiene i consigli del servizio Cost Explorer (Cost Explorer)
- `route53resolver`— Ottiene gli endpoint Amazon Route 53 Resolver e le risorse Resolver
- `kafka`: ottiene Amazon Managed Streaming per risorse Apache Kafka
- `ecs`— Ottiene risorse Amazon ECS
- `outposts`— Ottiene risorse AWS Outposts

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "access-analyzer:ListAnalyzers"
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "dax:DescribeClusters",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeNatGateways",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpnConnections",
```

```
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:GetManagedPrefixListEntries",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "iam:ListSAMLProviders",
                "kinesis:DescribeLimits",
                "kafka:DescribeClusterV2",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "network-firewall:ListFirewalls",
                "network-firewall:DescribeFirewall",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
```

```
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:GetQueueAttributes",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: AWSTrustedAdvisorReportingServiceRolePolicy

Questa policy è associata al ruolo `AWSServiceRoleForTrustedAdvisorReporting` collegato al servizio che consente di Trusted Advisor eseguire azioni per la funzionalità di visualizzazione organizzativa. Non è possibile attribuire AWSTrustedAdvisorReportingServiceRolePolicy alle entità IAM. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Trusted Advisor.

Questa politica concede autorizzazioni amministrative che consentono al ruolo collegato al servizio di eseguire azioni. AWS Organizations

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations`: Descrive l'organizzazione ed elenca l'accesso al servizio, gli account, le entità padre, le entità figlio e le unità organizzative

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

Trusted Advisor aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per AWS Support e Trusted Advisor da quando questi servizi hanno iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti.

La tabella seguente descrive importanti aggiornamenti alle politiche Trusted Advisor gestite dal 10 agosto 2021.

Trusted Advisor

Modifica	Descrizione	Data
AWSTrustedAdvisorServiceRolePolicy Aggiornamento a una politica esistente.	Trusted Advisor ha aggiunto nuove azioni per concedere le `access-analyzer:ListAnalyzers` `cloudwatch:ListMetrics` ,`dax:DescribeClusters` ,`ec2:DescribeNatGateways` ,`ec2:DescribeRouteTables` ,`ec2:DescribeVpcEndpoints` ,`ec2:GetManagedPrefixListEntries` , `elasticloadbalancing:DescribeTargetHealth` `iam:ListSAMLProviders` , `kafka:DescribeClusterV2` `network-firewall:ListFirewalls` `network-firewall:DescribeFirewall` e `sqs:GetQueueAttributes` le autorizzazioni.	11 giugno 2024
AWSTrustedAdvisorServiceRolePolicy	Trusted Advisor ha aggiunto nuove azioni per concedere	18 gennaio 2024

Modifica	Descrizione	Data
Aggiornamento a una politica esistente.	`cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` `outposts:GetOutpost` le `outposts:ListOutposts` autorizzazioni `outposts:ListAssets` e.	
AWSTrustedAdvisorPriorityFullAccess Aggiornamento a una politica esistente.	Trusted Advisor ha aggiornato la politica `AWSTrustedAdvisorPriorityFullAccess` AWS gestita per includere gli ID delle dichiarazioni.	6 dicembre 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Aggiornamento a una politica esistente.	Trusted Advisor ha aggiornato la politica `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS gestita per includere gli ID delle dichiarazioni.	6 dicembre 2023
AWSTrustedAdvisorServiceRolePolicy: aggiornamento a una policy esistente	Trusted Advisor ha aggiunto nuove azioni per concedere le `ecs:ListTaskDefinitions` autorizzazioni `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` e.	9 novembre 2023

Modifica	Descrizione	Data
AWSTrustedAdvisorServiceRolePolicy: aggiornamento a una policy esistente	Trusted Advisor ha aggiunto nuove azioni `route53resolver:ListResolverEndpoints` IAM `kafka:ListClustersV2` e ha introdotto nuovi controlli `kafka:ListNodes` di resilienza. `route53resolver:ListResolverEndpointIpAddresses` `ec2:DescribeSubnets`	14 settembre 2023
AWSTrustedAdvisorReportingServiceRolePolicy V2 della policy gestita allegata al ruolo collegato al servizio Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting`	Aggiorna la policy AWS gestita alla V2 per il ruolo collegato al servizio. Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` La versione 2 aggiungerà un'altra azione IAM `organizations:ListDelegatedAdministrators`	28 febbraio 2023
AWSTrustedAdvisorPriorityFullAccess e AWSTrustedAdvisorPriorityReadOnlyAccess Nuove politiche AWS gestite per Trusted Advisor	Trusted Advisor sono state aggiunte due nuove politiche gestite che è possibile utilizzare per controllare l'accesso a Trusted Advisor Priority.	17 agosto 2022

Modifica	Descrizione	Data
AWSTrustedAdvisorServiceRolePolicy: aggiornamento a una policy esistente	Trusted Advisor ha aggiunto nuove azioni per concedere le `GetAccountPublicAccessBlock` autorizzazioni `DescribeTargetGroups` e. È richiesta l'autorizzazione `DescribeTargetGroup` per il Controllo dello stato del gruppo Auto Scaling per recuperare i non-Classic Load Balancers attribuiti a un gruppo Auto Scaling. È necessaria l'autorizzazione `GetAccountPublicAccessBlock` per consentire al controllo Autorizzazioni Bucket Amazon S3 di recuperare le impostazioni di blocco dell'accesso pubblico per un Account AWS.	10 agosto 2021
Log delle modifiche pubblicato	Trusted Advisor ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	10 agosto 2021

AWS politiche gestite per AWS Support Plans

AWS Support Plans dispone delle seguenti politiche gestite.

Indice

- AWS politica gestita: AWSSupportPlansReadOnlyAccess
- AWS Support Piani, aggiornamenti alle politiche AWS gestite

AWS politica gestita: AWSSupportPlansFullAccess

AWS Support I piani utilizzano la politica AWSSupportPlansFullAccess AWS gestita. L'entità IAM utilizza questa policy per completare le seguenti operazioni relative ai piani di supporto:

- Visualizza il piano di supporto per il tuo Account AWS
- Visualizzazione dei dettagli sullo stato di una richiesta di modifica del piano di supporto
- Modifica il piano di supporto per il tuo Account AWS
- Crea piani di supporto programmati per i tuoi Account AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

Per un elenco delle modifiche della policy, consulta la pagina AWS Support Piani, aggiornamenti alle politiche AWS gestite.

AWS politica gestita: AWSSupportPlansReadOnlyAccess

AWS Support I piani utilizzano la politica AWSSupportPlansReadOnlyAccess AWS gestita. L'entità IAM utilizza questa policy per completare le seguenti operazioni relative ai piani di supporto di sola lettura:

- Visualizza il piano di supporto per il tuo Account AWS

- Visualizzazione dei dettagli sullo stato di una richiesta di modifica del piano di supporto

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Per un elenco delle modifiche della policy, consulta la pagina AWS Support Piani, aggiornamenti alle politiche AWS gestite.

AWS Support Piani, aggiornamenti alle politiche AWS gestite

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

Nella tabella seguente sono descritti importanti aggiornamenti delle policy gestite dai piani di supporto a partire dal 29 settembre 2022.

AWS Support

Modifica	Descrizione	Data
AWSSupportPlansFullAccess - Aggiornamento a una policy esistente	Aggiungi azioni `CreateSupportPlanSchedule` alla policy gestita da `AWSSupportPlansFullAccess` .	8 maggio 2023

Modifica	Descrizione	Data
Log delle modifiche pubblicato	Log delle modifiche per le policy gestite dai piani di supporto.	29 settembre 2022

Gestisci l'accesso al AWS Support Centro

È necessario disporre delle autorizzazioni per accedere al Centro assistenza e creare di un caso di supporto.

È possibile utilizzare le seguenti opzioni per accedere al Centro assistenza:

- Utilizza l'indirizzo email e la password associati al tuo AWS account. Questa identità è chiamata utente root dell' AWS account.
- Usa AWS Identity and Access Management (IAM).

Se disponi di un piano Business, Enterprise On-Ramp o Enterprise Support, puoi anche utilizzare l'AWS Support API per accedere AWS Support e Trusted Advisor operare a livello di codice. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Support.

> **Note**
>
> Se non riesci ad accedere al Centro assistenza, puoi utilizzare la sezione Contattaci. Puoi utilizzare questa pagina per ricevere assistenza per problemi di fatturazione e account.

AWS account

Puoi accedere AWS Management Console e accedere al Support Center utilizzando l'indirizzo e-mail e la password del tuo AWS account. Questa identità è chiamata utente root dell' AWS account. Ti consigliamo tuttavia di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Ti consigliamo invece di utilizzare IAM che ti consente di controllare chi può eseguire determinate attività nel tuo account.

AWS azioni di supporto

È possibile eseguire le seguenti AWS Support azioni nella console. Puoi anche specificare queste AWS Support azioni in una policy IAM per consentire o negare azioni specifiche.

> **Note**
>
> Se rifiuti una delle seguenti azioni nelle tue policy IAM, il funzionamento del Centro di supporto potrebbe essere diverso da quello desiderato durante la creazione o l'interazione con un caso di supporto.

Azione	Descrizione
`DescribeSupportLevel`	Concede l'autorizzazione a restituire il livello di supporto di un identificatore di account AWS . Viene utilizzato internamente da AWS Support Center per identificare il livello di supporto.
`InitiateCallForCase`	Concede l'autorizzazione per avviare una chiamata su Center. AWS Support Viene utilizzato internamente da AWS Support Center per avviare una chiamata per conto dell'utente.
`InitiateChatForCase`	Concede l'autorizzazione ad avviare una chat su AWS Support Center. Viene utilizzat o internamente da AWS Support Center per avviare una chat per conto dell'utente.
`RateCaseCommunication`	Concede l'autorizzazione a valutare la comunicazione di un AWS Support caso.
`DescribeCaseAttributes`	Concede l'autorizzazione a consentire ai servizi secondari di leggere gli attributi dei casi AWS Support . Viene utilizzato internamente da AWS Support Center per contrassegnare gli attributi relativi al caso.

Azione	Descrizione
`DescribeIssueTypes`	Concede l'autorizzazione a restituire i tipi di problemi dei casi di AWS Support . Viene utilizzato internamente da AWS Support Center per ottenere i tipi di problemi disponibili per l'account.
`SearchForCases`	Concede l'autorizzazione a restituire un elenco di AWS Support casi che corrispondono agli input forniti. Viene utilizzato internamente da AWS Support Center per trovare i casi ricercati.
`PutCaseAttributes`	Concede l'autorizzazione a consentire ai servizi secondari di allegare attributi ai AWS Support casi. Viene utilizzato internamente da AWS Support Center per aggiungere tag operativi ai AWS Support casi.

IAM

Per impostazione predefinita, gli utenti IAM non possono accedere al Centro assistenza. È possibile utilizzare IAM per creare singoli utenti o gruppi. Quindi, colleghi le policy IAM a queste entità, in modo che abbiano l'autorizzazione a eseguire azioni e accedere alle risorse, ad esempio per aprire casi del Support Center e utilizzare l' AWS Support API.

Dopo aver creato gli utenti IAM, è possibile assegnare loro delle password individuali e una pagina di accesso specifica dell'account. Possono quindi accedere al tuo AWS account e lavorare nel Support Center. Gli utenti IAM che hanno AWS Support accesso possono vedere tutti i casi creati per l'account.

Per ulteriori informazioni, consulta Accedere AWS Management Console come utente IAM nella Guida per l'utente IAM.

Il modo più semplice per concedere le autorizzazioni consiste nell'allegare la policy AWS gestita AWSSupportAccessall'utente, al gruppo o al ruolo. AWS Support consente autorizzazioni a livello di azione per controllare l'accesso a operazioni specifiche. AWS Support AWS Support non fornisce

l'accesso a livello di risorsa, quindi l'elemento è sempre impostato su. `Resource` * Non è possibile consentire o negare l'accesso a casi di supporto specifici.

Example : Consenti l'accesso a tutte le azioni AWS Support

La policy AWS gestita AWSSupportAccessconcede a un utente IAM l'accesso a AWS Support. Un utente IAM con questa policy può accedere a tutte le AWS Support operazioni e le risorse.

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

Per ulteriori informazioni su come collegare la `AWSSupportAccess` policy alle entità, consulta la sezione Aggiungere autorizzazioni di identità IAM (console) nella Guida per l'utente IAM.

Example : Consenti l'accesso a tutte le azioni tranne l' ResolveCase azione

Inoltre puoi creare policy gestite dal cliente in ambiente IAM per specificare quali azioni consentire o negare. La seguente dichiarazione di policy consente a un utente IAM di eseguire tutte le azioni AWS Support tranne risolvere un caso.

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

Per ulteriori informazioni su come creare una policy IAM gestita dal cliente, consulta la sezione Creazione di policy IAM (console) nella Guida per l'utente IAM.

Se l'utente o il gruppo dispone già di una policy, puoi aggiungere la policy statement AWS Support-specific a quella policy.

> **Important**
>
> - Se non riesci a visualizzare i casi in nel Centro assistenza, assicurati di possedere le autorizzazioni necessarie. Potrebbe essere necessario contattare l'amministratore IAM. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per AWS Support.

Accesso a AWS Trusted Advisor

In AWS Management Console, un namespace `trustedadvisor` IAM separato controlla l'accesso a. Trusted Advisor Nell' AWS Support API, lo spazio dei nomi `support` IAM controlla l'accesso a. Trusted Advisor Per ulteriori informazioni, consulta Gestisci l'accesso a AWS Trusted Advisor.

Gestisci l'accesso ai piani AWS Support

Argomenti

Autorizzazioni per la console dei piani di supporto

Per accedere alla console dei piani di supporto, è necessario che l'utente disponga di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli relativi alle risorse dei piani di supporto nel tuo Account AWS.

Puoi creare una policy AWS Identity and Access Management (IAM) con il `supportplans` namespace. È possibile utilizzare questa policy per specificare le autorizzazioni per operazioni e risorse.

Quando crei una policy puoi specificare lo spazio dei nomi del servizio per consentire o negare un'operazione. Lo spazio dei nomi per i piani di supporto è `supportplans`.

Puoi utilizzare policy AWS gestite e collegarle alle tue entità IAM. Per ulteriori informazioni, consulta AWS politiche gestite per AWS Support Plans.

Operazioni dei piani di supporto

Puoi eseguire le seguenti operazioni dei piani di supporto nella console. Inoltre, puoi specificare queste operazioni dei piani di supporto in una policy IAM per consentire o negare operazioni specifiche.

Azione	Descrizione
`GetSupportPlan`	Concede l'autorizzazione per visualizzare i dettagli relativi al piano di supporto attuale per questo Account AWS.
`GetSupportPlanUpdateStatus`	Concede l'autorizzazione per visualizzare i dettagli relativi allo stato di una richiesta di aggiornamento di un piano di supporto.
`StartSupportPlanUpdate`	Concede l'autorizzazione per avviare la richiesta di aggiornamento del piano di supporto per questo Account AWS.
`CreateSupportPlanSchedule`	Concede l'autorizzazione a creare pianificazioni per i piani di assistenza per tale Account AWS.

Policy IAM di esempio per i piani di supporto

Puoi utilizzare le seguenti policy di esempio per gestire l'accesso ai piani di supporto.

Accesso completo ai piani di supporto

La policy seguente consente agli utenti di accedere in modo completo ai piani di supporto.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

Accesso in sola lettura ai piani di supporto

La policy seguente consente agli utenti di accedere in sola lettura ai piani di supporto.

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

Rifiuto dell'accesso ai piani di supporto

La policy seguente non consente agli utenti di accedere ai piani di supporto.

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

Risoluzione dei problemi

Consulta i seguenti argomenti per gestire l'accesso ai piani di supporto.

Quando provo a visualizzare o modificare il mio piano di supporto, la console dei piani di supporto mi comunica che non ho ricevuto l'autorizzazione **`GetSupportPlan`**

Gli utenti IAM devono disporre delle autorizzazioni necessarie per accedere alla console dei piani di supporto. Puoi aggiornare la policy IAM per includere l'autorizzazione mancante o utilizzare una policy gestita da AWS , ad esempio AWSSupportPlansFullAccess o AWSSupportPlansReadOnlyAccess. Per ulteriori informazioni, consulta AWS politiche gestite per AWS Support Plans.

Se non disponi dell'accesso per aggiornare le policy IAM, contatta l'amministratore del tuo Account AWS .

Informazioni correlate

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente IAM:

- Test delle policy IAM con il simulatore di policy IAM
- Risoluzione dei problemi dei messaggi di errore di accesso rifiutato

Dispongo delle corrette autorizzazioni per i piani di supporto, ma ricevo ancora lo stesso errore

Se il tuo Account AWS è un account membro di cui fa parte AWS Organizations, potrebbe essere necessario aggiornare la policy di controllo del servizio (SCP). Le policy di controllo dei servizi sono un tipo di policy che consentono di gestire le autorizzazioni nell'organizzazione.

Siccome i piani di supporto costituiscono un servizio globale, le policy che limitano le Regioni AWS potrebbero impedire agli account membri di visualizzare o modificare il loro piano di supporto. Per consentire i servizi globali per la tua organizzazione, ad esempio IAM e piani di supporto, devi aggiungere il servizio all'elenco di esclusione in tutte le SCP applicabili. Ciò significa che gli account dell'organizzazione possono accedere a questi servizi, anche se l'SCP nega una condizione specificata. Regione AWS

Per aggiungere piani di supporto come eccezione, inserisci `"supportplans:*"` nell'elenco `"NotAction"` nella SCP.

```
"supportplans:*",
```

L'aspetto della policy di controllo dei servizi dovrebbe essere simile al frammento seguente.

Example : SCP che consente l'accesso ai piani di supporto in un'organizzazione

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

Se disponi di un account membro e non riesci ad aggiornare la policy di controllo dei servizi, contatta il tuo amministratore Account AWS . Potrebbe essere necessario che l'account di gestione aggiorni la SCP affinché tutti gli account membri possano accedere ai piani di supporto.

> **Note per AWS Control Tower**
>
> - Se l'organizzazione utilizza un SCP con AWS Control Tower, è possibile aggiornare l'opzione di negazione dell'accesso in AWS base al Regione AWS controllo richiesto (comunemente denominato Region Deny Control).
> - Se aggiorni l'SCP AWS Control Tower per consentire`supportplans`, la riparazione della deriva rimuoverà l'aggiornamento a SCP. Per ulteriori informazioni, consulta Rileva e risolve il drift in. AWS Control Tower

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

- Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Configurazione del controllo di diniego della regione nella Guida per l'utente di AWS Control Tower
- Negare l'accesso a in AWS base a quanto richiesto Regione AWS nella Guida per l'AWS Control Tower utente

Gestisci l'accesso a AWS Trusted Advisor

Puoi accedere AWS Trusted Advisor da. AWS Management Console Tutti Account AWS hanno accesso a una selezione di Trusted Advisor controlli di base. Se hai sottoscritto un piano di supporto Business, Enterprise On-Ramp o Enterprise, puoi accedere a tutti i controlli. Per ulteriori informazioni, consulta AWS Trusted Advisor verifica riferimento.

Puoi usare AWS Identity and Access Management (IAM) per controllare l'accesso a Trusted Advisor.

Argomenti

Autorizzazioni per la console Trusted Advisor

Per accedere alla Trusted Advisor console, un utente deve disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli sulle Trusted Advisor risorse del tuo. Account AWS

Puoi utilizzare le seguenti opzioni per controllare l'accesso a Trusted Advisor:

- Utilizza la funzionalità di filtro dei tag della Trusted Advisor console. L'utente o il ruolo devono avere autorizzazioni associate ai tag.

  Puoi utilizzare politiche AWS gestite o politiche personalizzate per assegnare le autorizzazioni tramite tag. Per ulteriori informazioni, consulta Controllo dell'accesso a e per utenti e ruoli IAM mediante i tag.
- Crea una policy IAM con spazio dei nomi `trustedadvisor`. È possibile utilizzare questa policy per specificare le autorizzazioni per operazioni e risorse.

Quando crei una policy puoi specificare lo spazio dei nomi del servizio per consentire o negare un'operazione. Il namespace per è. Trusted Advisor `trustedadvisor` Tuttavia, non è possibile utilizzare lo spazio dei `trustedadvisor` nomi per consentire o negare le operazioni API nell' Trusted Advisor API. AWS Support Invece, devi utilizzare lo spazio dei nomi `support` per AWS Support .

> **Note**
>
> Se disponi delle autorizzazioni per l'AWS SupportAPI, il Trusted Advisor widget nella finestra AWS Management Console mostra una visualizzazione riassuntiva dei risultati. Trusted Advisor Per visualizzare i risultati nella Trusted Advisor console, devi disporre dell'autorizzazione per il `trustedadvisor` namespace.

Trusted Advisor azioni

È possibile eseguire le seguenti Trusted Advisor azioni nella console. Puoi anche specificare queste Trusted Advisor azioni in una policy IAM per consentire o negare azioni specifiche.

Azione	Descrizione
`DescribeAccount`	Concede l'autorizzazione a visualizzare il AWS Support piano e varie Trusted Advisor p referenze.
`DescribeAccountAccess`	Concede il permesso di visualizzare se Account AWS è abilitato o disabilitato. Trusted Advisor
`DescribeCheckItems`	Concede l'autorizzazione a visualizzare i dettagli degli elementi di controllo.
`DescribeCheckRefreshStatuses`	Concede l'autorizzazione a visualizzare gli stati di aggiornamento per i controlli Trusted Advisor .
`DescribeCheckSummaries`	Concede l'autorizzazione a visualizzare i riepiloghi degli Trusted Advisor assegni.
`DescribeChecks`	Concede l'autorizzazione a visualizzare i dettagli dei controlli. Trusted Advisor
`DescribeNotificationPreferences`	Concede l'autorizzazione a visualizzare le preferenze di notifica per l'account AWS .

Azione	Descrizione
`ExcludeCheckItems`	Concede l'autorizzazione a escludere i suggerimenti per i controlli Trusted Advisor .
`IncludeCheckItems`	Concede l'autorizzazione a includere suggerimenti per i controlli Trusted Advisor .
`RefreshCheck`	Concede l'autorizzazione ad aggiornare un assegno. Trusted Advisor
`SetAccountAccess`	Concede l'autorizzazione all'attivazione o alla disattivazione Trusted Advisor dell'account.
`UpdateNotificationPreferences`	Concede l'autorizzazione ad aggiornare le preferenze di notifica per Trusted Advisor.
`DescribeCheckStatusHistoryChanges`	Concede l'autorizzazione a visualizzare i risultati e gli stati modificati dei controlli negli ultimi 30 giorni.

Trusted Advisor azioni per la visualizzazione organizzativa

Le Trusted Advisor azioni seguenti riguardano la funzionalità di visualizzazione organizzativa. Per ulteriori informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor.

Azione	Descrizione
`DescribeOrganization`	Concede l'autorizzazione alla visualizzazione se Account AWS soddisfa i requisiti per abilitare la funzionalità di visualizzazione organizzativa.
`DescribeOrganizationAccounts`	Concede l'autorizzazione a visualizzare gli AWS account collegati presenti nell'organizzazione.
`DescribeReports`	Concede l'autorizzazione a visualizzare i dettagli dei report delle viste organizzative, ad

Azione	Descrizione
	esempio il nome del report, il runtime, la data di creazione, lo stato e il formato.
`DescribeServiceMetadata`	Concede l'autorizzazione a visualizzare informazioni sulla visualizzazione organizzativa, ad esempio i report di controllo delle categorie Regioni AWS, dei nomi di controllo e dello stato delle risorse.
`GenerateReport`	Concede l'autorizzazione a creare un rapporto per i Trusted Advisor controlli nell'organizzazione.
`ListAccountsForParent`	Concede l'autorizzazione a visualizzare, nella Trusted Advisor console, tutti gli account di un' AWS organizzazione contenuti da un'unità organizzativa principale o da un'unità organizzativa (OU).
`ListOrganizationalUnitsForParent`	Concede l'autorizzazione a visualizzare, nella Trusted Advisor console, tutte le unità organizzative (OU) di un'unità organizzativa principale o principale.
`ListRoots`	Concede l'autorizzazione a visualizzare, nella Trusted Advisor console, tutte le radici definite in un' AWS organizzazione.
`SetOrganizationAccess`	Concede l'autorizzazione ad abilitare la funzionalità di visualizzazione organizzativa per. Trusted Advisor

Trusted Advisor Azioni prioritarie

Se hai abilitato la Trusted Advisor priorità per il tuo account, puoi eseguire le seguenti Trusted Advisor azioni nella console. Inoltre, puoi specificare queste operazioni Trusted Advisor in una policy

IAM per consentire o negare operazioni specifiche. Per ulteriori informazioni, consulta Policy IAM di esempio per Trusted Advisor Priority.

> **Note**
>
> I rischi che appaiono in Trusted Advisor Priority sono raccomandazioni che il tuo Technical Account Manager (TAM) ha identificato per il tuo account. I consigli di un servizio, ad esempio un Trusted Advisor assegno, vengono creati automaticamente per te. I suggerimenti da parte del TAM vengono creati manualmente per te. Successivamente, il TAM invia questi consigli in modo che vengano visualizzati in Trusted Advisor Priority per il tuo account.

Per ulteriori informazioni, consulta Nozioni di base su AWS Trusted Advisor Priority.

Azione	Descrizione
`DescribeRisks`	Concede l'autorizzazione a visualizzare i rischi in Trusted Advisor Priority.
`DescribeRisk`	Concede l'autorizzazione a visualizzare i dettagli del rischio in Trusted Advisor Priority.
`DescribeRiskResources`	Concede l'autorizzazione per visualizzare le risorse interessate per un rischio in Trusted Advisor Priority
`DownloadRisk`	Concede l'autorizzazione a scaricare un file che contiene dettagli sul rischio in Trusted Advisor Priority.
`UpdateRiskStatus`	Concede l'autorizzazione per aggiornare lo stato di rischio in Trusted Advisor Priority
`DescribeNotificationConfigurations`	Concede l'autorizzazione a ricevere le preferenze di notifica e-mail per Trusted Advisor Priority.

Azione	Descrizione
`UpdateNotificationConfigurations`	Concede l'autorizzazione per creare o aggiornare le preferenze di notifica e-mail per Trusted Advisor Priority.
`DeleteNotificationConfigurationForDelegatedAdmin`	Concede l'autorizzazione all'account di gestione dell'organizzazione per eliminare le preferenze di notifica e-mail da un account amministratore delegato per Priority. Trusted Advisor

Trusted Advisor Intraprendi azioni

Se hai attivato Trusted Advisor Engage per il tuo account, puoi eseguire le seguenti Trusted Advisor azioni nella console. Puoi anche aggiungere queste Trusted Advisor azioni in una policy IAM per consentire o negare azioni specifiche. Per ulteriori informazioni, consulta Policy IAM di esempio per Trusted Advisor Engage.

Per ulteriori informazioni, consultare Nozioni di base di AWS Trusted Advisor Engage (anteprima).

Azione	Descrizione
`CreateEngagement`	Concede l'autorizzazione a creare un coinvolgimento in Trusted Advisor Engage.
`CreateEngagementAttachment`	Concede l'autorizzazione a creare un allegato di coinvolgimento in Trusted Advisor Engage.
`CreateEngagementCommunication`	Concede l'autorizzazione a creare una comunicazione di coinvolgimento in Trusted Advisor Engage.
`GetEngagement`	Concede l'autorizzazione a visualizzare un coinvolgimento in Engage. Trusted Advisor

Azione	Descrizione
`GetEngagementAttachment`	Concede l'autorizzazione a visualizzare un allegato di coinvolgimento in Engage. Trusted Advisor
`GetEngagementType`	Concede l'autorizzazione a visualizzare un tipo di coinvolgimento specifico in Engage. Trusted Advisor
`ListEngagementCommunications`	Concede l'autorizzazione a visualizzare tutte le comunicazioni un impegno su Trusted Advisor Engage.
`ListEngagements`	Concede l'autorizzazione a visualizzare tutte le interazioni in Engage. Trusted Advisor
`ListEngagementTypes`	Concede l'autorizzazione a visualizzare tutti i tipi di coinvolgimento in Engage. Trusted Advisor
`UpdateEngagement`	Concede l'autorizzazione ad aggiornare i dettagli di un coinvolgimento in Trusted Advisor Engage.
`UpdateEngagementStatus`	Concede l'autorizzazione ad aggiornare lo stato di un impegno in Trusted Advisor Engage.

Esempi di policy IAM

Le policy seguenti mostrano come consentire e negare l'accesso a Trusted Advisor. È possibile utilizzare una delle seguenti policy per creare una policy gestita dal cliente nella console IAM. Ad esempio, una policy di esempio può essere copiata e incollata nella Scheda JSON della console IAM. È quindi possibile attribuire la policy all'utente, al gruppo o al ruolo IAM.

Per ulteriori informazioni su come creare una policy IAM, consulta la sezione Creazione di criteri IAM (console) nella Guida per l'utente IAM.

Esempi

- Accesso completo a Trusted Advisor
- Accesso in sola lettura a Trusted Advisor
- Negare l'accesso a Trusted Advisor
- Operazioni specifiche consentite o negate
- Controlla l'accesso alle operazioni AWS Support API per Trusted Advisor
- Policy IAM di esempio per Trusted Advisor Priority
- Policy IAM di esempio per Trusted Advisor Engage

Accesso completo a Trusted Advisor

La seguente politica consente agli utenti di visualizzare e eseguire tutte le azioni relative a tutti i Trusted Advisor controlli nella Trusted Advisor console.

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

Accesso in sola lettura a Trusted Advisor

La seguente politica consente agli utenti l'accesso in sola lettura alla Trusted Advisor console. Gli utenti non possono apportare modifiche, ad esempio aggiornare i controlli o modificare le preferenze di notifica.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:Describe*",
                "trustedadvisor:Get*",
```

```
                "trustedadvisor:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Negare l'accesso a Trusted Advisor

La seguente politica non consente agli utenti di visualizzare o eseguire azioni per Trusted Advisor i controlli nella Trusted Advisor console.

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

Operazioni specifiche consentite o negate

La seguente politica consente agli utenti di visualizzare tutti i Trusted Advisor controlli nella Trusted Advisor console, ma non consente loro di aggiornare alcun controllo.

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

```
}
```

Controlla l'accesso alle operazioni AWS Support API per Trusted Advisor

In AWS Management Console, un namespace `trustedadvisor` IAM separato controlla l'accesso a. Trusted Advisor Non puoi utilizzare lo spazio dei `trustedadvisor` nomi per consentire o negare le operazioni API nell' Trusted Advisor API. AWS Support Al contrario, utilizza lo spazio dei nomi `support`. È necessario disporre delle autorizzazioni per l' AWS Support API per effettuare chiamate a livello di codice. Trusted Advisor

Ad esempio, se si desidera chiamare l'RefreshTrustedAdvisorCheckoperazione, è necessario disporre delle autorizzazioni per questa azione nella politica.

Example : Consenti solo le operazioni Trusted Advisor API

La seguente politica consente agli utenti di accedere alle operazioni AWS Support API per Trusted Advisor, ma non al resto delle operazioni AWS Support API. Ad esempio, gli utenti possono utilizzare l'API per visualizzare e aggiornare i controlli. Non possono creare, visualizzare, aggiornare o risolvere AWS Support casi.

Puoi utilizzare questa politica per richiamare le operazioni dell' Trusted Advisor API a livello di codice, ma non puoi utilizzare questa politica per visualizzare o aggiornare i controlli nella console. Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
```

```
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni su come IAM funziona con AWS Support and Trusted Advisor, consulta. Azioni

Policy IAM di esempio per Trusted Advisor Priority

Puoi utilizzare le seguenti politiche AWS gestite per controllare l'accesso a Trusted Advisor Priority. Per ulteriori informazioni, consulta AWS politiche gestite per AWS Trusted Advisor e Nozioni di base su AWS Trusted Advisor Priority.

Policy IAM di esempio per Trusted Advisor Engage

> **Note**
>
> Trusted Advisor Engage è in versione di anteprima e attualmente non dispone di policy AWS gestite. È possibile utilizzare una delle seguenti policy per creare una policy gestita dal cliente nella console IAM.

Un esempio di policy che garantisce l'accesso in lettura e scrittura in Trusted Advisor Engage:

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

```
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Un esempio di policy che garantisce l'accesso in sola lettura in Engage: Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Un esempio di policy che garantisce l'accesso in lettura e scrittura in Trusted Advisor Engage e la possibilità di abilitare l'accesso affidabile a: Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
```

```
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

Consulta anche

Per ulteriori informazioni sulle Trusted Advisor autorizzazioni, consulta le seguenti risorse:

- Operazioni definite da AWS Trusted Advisor nella Guida per l'utente IAM.
- Controllo dell'accesso alla console Trusted Advisor

Policy di controllo dei servizi di esempio per AWS Trusted Advisor

AWS Trusted Advisor supporta le politiche di controllo dei servizi (SCP). Le SCP sono policy che collegano agli elementi di un'organizzazione per gestire le autorizzazioni all'interno di tale organizzazione. Un SCP si applica a tutti gli AWS account appartenenti all'elemento a cui si collega l'SCP. Le SCP offrono un controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account dell'organizzazione. Possono aiutarti a garantire che i tuoi AWS account rispettino le linee guida per il controllo degli accessi della tua organizzazione. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Argomenti

Prerequisiti

Per utilizzare le SCP, effettua innanzitutto le seguenti operazioni:

- Abilitazione di tutte le caratteristiche nell'organizzazione. Per ulteriori informazioni, consulta la sezione Abilitazione di tutte le caratteristiche nell'organizzazione nella Guida per l'utente di AWS Organizations .
- Abilita l'utilizzo delle SCP all'interno dell'organizzazione. Per ulteriori informazioni, consulta Abilitazione e disabilitazione dei tipi di policy nella Guida per l'utente di AWS Organizations .
- Crea le SCP di cui hai bisogno. Per ulteriori informazioni sulla creazione delle SCP, consulta Creazione, aggiornamento ed eliminazione delle policy di controllo del servizio nella Guida per l'utente di AWS Organizations .

Policy di controllo dei servizi di esempio

Di seguito sono riportati alcuni esempi che mostrano come controllare vari aspetti della condivisione delle risorse in un'organizzazione.

Example : Impedisci agli utenti di creare o modificare interazioni in Engage Trusted Advisor

La seguente SCP impedisce agli utenti di creare nuovi impegni o di modificare quelli esistenti.

```
{
```

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

Example : Nega Trusted Advisor Engage e Priority Access Trusted Advisor

Il seguente SCP impedisce agli utenti di accedere o eseguire qualsiasi azione all'interno di Trusted Advisor Engage and Trusted Advisor Priority.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Risoluzione dei problemi di AWS Support identità e accesso

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

Argomenti

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 Support.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Support. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

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

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Desidero visualizzare le mie chiavi di accesso

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

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

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

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

Sono un amministratore e desidero consentire ad altri di accedere AWS Support

Per consentire ad altri di accedere AWS Support, devi creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che necessita dell'accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in AWS Support.

Per iniziare immediatamente, consulta Creazione dei primi utenti e gruppi delegati IAM nella Guida per l'utente di IAM.

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

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Support supporta queste funzionalità, consultaCome AWS Support funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Risposta agli incidenti

La risposta agli incidenti AWS Support è una AWS responsabilità. AWS ha una politica e un programma formali e documentati che regolano la risposta agli incidenti. Per ulteriori informazioni, consulta il white paper Introducing the AWS Security Incident Response.

Utilizza le seguenti opzioni per informarti sui problemi operativi:

- Visualizza i problemi AWS operativi di ampio impatto sul AWS Service Health Dashboard. Ad esempio, eventi che interessano un servizio o una regione che non è specifica per il tuo account.
- Visualizza i problemi operativi per i singoli account in AWS Health Dashboard. Ad esempio, eventi che influiscono sui servizi o sulle risorse del tuo account. Per ulteriori informazioni, consulta Nozioni di base su AWS Health Dashboard nella Guida per l'utente di AWS Health .

Registrazione e monitoraggio in AWS Support e AWS Trusted Advisor

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

- 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 CloudWatch tenere traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon Elastic Compute Cloud (Amazon EC2) e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon EventBridge offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. EventBridge abilita l'elaborazione automatizzata basata sugli eventi, poiché puoi scrivere regole che controllano determinati eventi e attivano azioni automatizzate in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon Simple Storage Service (Amazon S3) da te specificato. Puoi identificare quali utenti e account hanno effettuato la chiamata AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Per ulteriori informazioni, consulta Monitoraggio e logging per AWS Support e Monitoraggio e logging per AWS Trusted Advisor.

Convalida della conformità per AWS Support

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

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

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

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

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty

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

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

Resilienza in AWS Support

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.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta infrastruttura globale.AWS

Sicurezza dell'infrastruttura in AWS Support

In quanto servizio gestito, AWS Support è protetto dalle procedure di sicurezza della rete AWS globale descritte nel white paper Amazon Web Services: panoramica dei processi di sicurezza.

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

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

Analisi della configurazione e delle vulnerabilità in AWS Support

Infatti AWS Trusted Advisor, AWS gestisce attività di sicurezza di base come l'applicazione di patch al sistema operativo (OS) guest e al database, la configurazione del firewall e il disaster recovery.

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.

Esempi di codice per l' AWS Support utilizzo degli AWS SDK

I seguenti esempi di codice mostrano come utilizzarlo AWS Support con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati e negli esempi tra servizi.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Nozioni di base

Ciao AWS Support

L'esempio di codice seguente mostra come iniziare a utilizzare AWS Support.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
```

```
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- Per i dettagli sull'API, consulta la DescribeServicessezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
```

```
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
```

```
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Per i dettagli sull'API, consulta la DescribeServicessezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Richiama main() `per eseguire l'esempio.

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- Per i dettagli sull'API, consulta la DescribeServicessezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- Per i dettagli sull'API, DescribeServicesconsulta AWS SDK for Kotlin API reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
```

```
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- Per i dettagli sull'API, consulta DescribeServices AWSSDK for Python (Boto3) API Reference.

Esempi di codice

- Azioni per l'utilizzo degli SDK AWS SupportAWS
  - Utilizzo AddAttachmentsToSet con un AWS SDK o una CLI
  - Utilizzo AddCommunicationToCase con un AWS SDK o una CLI
  - Utilizzo CreateCase con un AWS SDK o una CLI

- Utilizzo DescribeAttachment con un AWS SDK o una CLI
- Utilizzo DescribeCases con un AWS SDK o una CLI
- Utilizzo DescribeCommunications con un AWS SDK o una CLI
- Utilizzo DescribeServices con un AWS SDK o una CLI
- Utilizzo DescribeSeverityLevels con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorCheckRefreshStatuses con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorCheckResult con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorCheckSummaries con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorChecks con un AWS SDK o una CLI
- Utilizzo RefreshTrustedAdvisorCheck con un AWS SDK o una CLI
- Utilizzo ResolveCase con un AWS SDK o una CLI

- Scenari per l' AWS Support utilizzo AWS degli SDK
  - Inizia con i AWS Support casi utilizzando un AWS SDK

Azioni per l'utilizzo degli SDK AWS SupportAWS

I seguenti esempi di codice mostrano come eseguire AWS Support azioni individuali con gli AWS SDK. Questi estratti richiamano l' AWS Support API e sono estratti di codice di programmi più grandi che devono essere eseguiti nel contesto. Ogni esempio include un collegamento a GitHub, dove è possibile trovare le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento delle API AWS Support.

Esempi

- Utilizzo AddAttachmentsToSet con un AWS SDK o una CLI
- Utilizzo AddCommunicationToCase con un AWS SDK o una CLI
- Utilizzo CreateCase con un AWS SDK o una CLI
- Utilizzo DescribeAttachment con un AWS SDK o una CLI
- Utilizzo DescribeCases con un AWS SDK o una CLI
- Utilizzo DescribeCommunications con un AWS SDK o una CLI
- Utilizzo DescribeServices con un AWS SDK o una CLI
- Utilizzo DescribeSeverityLevels con un AWS SDK o una CLI

- Utilizzo DescribeTrustedAdvisorCheckRefreshStatuses con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorCheckResult con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorCheckSummaries con un AWS SDK o una CLI
- Utilizzo DescribeTrustedAdvisorChecks con un AWS SDK o una CLI
- Utilizzo RefreshTrustedAdvisorCheck con un AWS SDK o una CLI
- Utilizzo ResolveCase con un AWS SDK o una CLI

Utilizzo **`AddAttachmentsToSet`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`AddAttachmentsToSet`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
```

```
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- Per i dettagli sull'API, consulta la AddAttachmentsToSetsezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per aggiungere un allegato a un set

L'`add-attachments-to-set`esempio seguente aggiunge un'immagine a un set che potete quindi specificare per una richiesta di supporto nel vostro AWS account.

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

Output:

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
```

```
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta AddAttachmentsToSet AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();

       } catch (SupportException | FileNotFoundException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
```

```
        }
        return "";
    }
```

- Per i dettagli sull'API, consulta la AddAttachmentsToSetsezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
```

```
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la AddAttachmentsToSetsezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- Per i dettagli sull'API, AddAttachmentsToSetconsulta AWS SDK for Kotlin API reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
```

```
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- Per i dettagli sull'API, consulta AddAttachmentsToSet AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`AddCommunicationToCase`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`AddCommunicationToCase`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- Per i dettagli sull'API, consulta la AddCommunicationToCasesezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per aggiungere una comunicazione a un caso

L'`add-communication-to-case`esempio seguente aggiunge comunicazioni a un caso di supporto nel tuo AWS account.

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

Output:

```
{
    "result": true
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta AddCommunicationToCase AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
       try {
```

```
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Per i dettagli sull'API, consulta la AddCommunicationToCasesezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
```

```
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la AddCommunicationToCasesezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
```

```
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- Per i dettagli sull'API, AddCommunicationToCaseconsulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: aggiunge il corpo di una comunicazione e-mail al caso specificato.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Esempio 2: aggiunge il corpo di una comunicazione e-mail al caso specificato più uno o più indirizzi e-mail contenuti nella riga CC dell'e-mail.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

- Per i dettagli sull'API, vedere AddCommunicationToCasein AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id,
            )
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- Per i dettagli sull'API, consulta AddCommunicationToCase AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CreateCase`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`CreateCase`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
```

```
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- Per i dettagli sull'API, consulta la CreateCasesezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per creare un caso

L'`create-case`esempio seguente crea una richiesta di supporto per il tuo AWS account.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

Output:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta CreateCase AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Per i dettagli sull'API, consulta la CreateCasesezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la CreateCasesezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- Per i dettagli sull'API, CreateCaseconsulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: crea un nuovo caso nel AWS Support Center. I valori per i CategoryCode parametri - ServiceCode e - possono essere ottenuti utilizzando il cmdlet Get-AsaService. Il valore per il SeverityCode parametro - può essere ottenuto utilizzando il cmdlet Get-ASA. SeverityLevel Il valore del IssueType parametro - può essere «assistenza clienti» o «tecnico». In caso di successo, viene emesso il numero del caso AWS Support. Per impostazione predefinita, il caso verrà gestito in inglese, per usare il giapponese aggiungi il parametro - Language «ja». I CommunicationBody parametri -ServiceCode, -CategoryCode, -Subject e - sono obbligatori.

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- Per i dettagli sull'API, vedere CreateCasein AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
```

```
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
```

```
            return case_id
```

- Per i dettagli sull'API, consulta CreateCase AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeAttachment`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeAttachment`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   /// <summary>
   /// Get description of a specific attachment.
   /// </summary>
   /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
   /// <returns>The attachment object.</returns>
   public async Task<Attachment> DescribeAttachment(string attachmentId)
   {
       var response = await _amazonSupport.DescribeAttachmentAsync(
```

```
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- Per i dettagli sull'API, consulta la DescribeAttachmentsezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per descrivere un allegato

L'`describe-attachment`esempio seguente restituisce informazioni sull'allegato con l'ID specificato.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Output:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeAttachment AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, consulta la DescribeAttachmentsezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la DescribeAttachmentsezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- Per i dettagli sull'API, DescribeAttachmentconsulta AWS SDK for Kotlin API reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
```

```
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- Per i dettagli sull'API, consulta DescribeAttachment AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeCases`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeCases`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
```

```
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- Per i dettagli sull'API, consulta la DescribeCasessezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per descrivere un caso

L'`describe-cases`esempio seguente restituisce informazioni sulla richiesta di assistenza specificata nel tuo AWS account.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

Output:

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeCases AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void getOpenCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                   .maxResults(20)
                   .afterTime(yesterday.toString())
                   .beforeTime(now.toString())
                   .build();

           DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
           List<CaseDetails> cases = response.cases();
           for (CaseDetails sinCase : cases) {
               System.out.println("The case status is " + sinCase.status());
               System.out.println("The case Id is " + sinCase.caseId());
               System.out.println("The case subject is " + sinCase.subject());
           }

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, consulta la DescribeCasessezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la DescribeCasessezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- Per i dettagli sull'API, DescribeCasesconsulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce i dettagli di tutti i casi di supporto.

```
Get-ASACase
```

Esempio 2: restituisce i dettagli di tutti i casi di supporto a partire dalla data e dall'ora specificate.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

Esempio 3: restituisce i dettagli dei primi 10 casi di supporto, inclusi quelli che sono stati risolti.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Esempio 4: restituisce i dettagli del singolo caso di supporto specificato.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Esempio 5: restituisce i dettagli dei casi di supporto specificati.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

Esempio 6: restituisce tutti i casi di supporto utilizzando il paging manuale. I casi vengono recuperati in lotti da 20.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Per i dettagli sull'API, vedere DescribeCasesin AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
```

```
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Per i dettagli sull'API, consulta DescribeCases AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeCommunications`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeCommunications`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- Per i dettagli sull'API, consulta la DescribeCommunicationssezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per descrivere la comunicazione più recente relativa a un caso

L'`describe-communications`esempio seguente restituisce la comunicazione più recente per il caso di assistenza specificato nel tuo AWS account.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Output:

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeCommunications AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Per i dettagli sull'API, consulta la DescribeCommunicationssezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la DescribeCommunicationssezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- Per i dettagli sull'API, DescribeCommunicationsconsulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce tutte le comunicazioni per il caso specificato.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Esempio 2: restituisce tutte le comunicazioni dalla mezzanotte UTC del 1° gennaio 2012 per il caso specificato.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

Esempio 3: restituisce tutte le comunicazioni a partire dalla mezzanotte UTC del 1° gennaio 2012 per il caso specificato, utilizzando l'impaginazione manuale. Le comunicazioni vengono recuperate in batch da 20.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Per i dettagli sull'API, vedere DescribeCommunicationsin AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
```

```
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

- Per i dettagli sull'API, consulta DescribeCommunications AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeServices`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeServices`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
```

```
            {
                Language = language
            });
        return response.Services;
    }
```

- Per i dettagli sull'API, consulta la DescribeServicessezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per elencare AWS i servizi e le categorie di servizi

L'`describe-services`esempio seguente elenca le categorie di servizi disponibili per la richiesta di informazioni generali.

```
aws support describe-services \
    --service-code-list "general-info"
```

Output:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
```

```
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeServices AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    // Return a List that contains a Service name and Category name.
```

```
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
               List<Category> categories = service.categories();
               for (Category cat : categories) {
                   System.out.println("The category name is: " + cat.name());
                   if (cat.name().compareTo("Security") == 0)
                       catName = cat.name();
               }
               index++;
           }

           // Push the two values to the list.
           sevCatList.add(serviceCode);
           sevCatList.add(catName);
           return sevCatList;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return null;
```

```
    }
```

- Per i dettagli sull'API, consulta la DescribeServicessezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }
```

```
            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Per i dettagli sull'API, DescribeServicesconsulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce tutti i codici di servizio, i nomi e le categorie disponibili.

```
Get-ASAService
```

Esempio 2: restituisce il nome e le categorie del servizio con il codice specificato.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

Esempio 3: restituisce il nome e le categorie per i codici di servizio specificati.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Esempio 4: restituisce il nome e le categorie (in giapponese) per i codici di servizio specificati. Attualmente sono supportati i codici di lingua inglese («en») e giapponese («ja»).

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- Per i dettagli sull'API, vedere DescribeServicesin AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
```

```
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services
```

- Per i dettagli sull'API, consulta DescribeServices AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeSeverityLevels`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeSeverityLevels`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

- Per i dettagli sull'API, consulta DescribeSeverityLevels in AWS SDK for .NET API Reference.

CLI

AWS CLI

Per elencare i livelli di gravità disponibili

L'`describe-severity-levels`esempio seguente elenca i livelli di gravità disponibili per un caso di supporto.

```
aws support describe-severity-levels
```

Output:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

Per ulteriori informazioni, consulta Scelta della gravità nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeSeverityLevels in AWS CLI Command Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static String displaySevLevels(SupportClient supportClient) {
       try {
           DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                   .language("en")
                   .build();

           DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
           List<SeverityLevel> severityLevels = response.severityLevels();
           String levelName = null;
           for (SeverityLevel sevLevel : severityLevels) {
               System.out.println("The severity level name is: " +
sevLevel.name());
               if (sevLevel.name().compareTo("High") == 0)
                   levelName = sevLevel.name();
           }
           return levelName;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Per i dettagli sull'API, consulta DescribeSeverityLevels in AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta DescribeSeverityLevels in AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- Per i dettagli sull'API, consulta DescribeSeverityLevels in AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce l'elenco dei livelli di gravità che possono essere assegnati a un caso AWS Support.

```
Get-ASASeverityLevel
```

Esempio 2: restituisce l'elenco dei livelli di gravità che possono essere assegnati a un caso AWS Support. I nomi dei livelli vengono restituiti in giapponese.

```
Get-ASASeverityLevel -Language "ja"
```

- Per i dettagli sull'API, vedere DescribeSeverityLevels in AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
 language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
 self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
```

```
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- Per i dettagli sull'API, consulta DescribeSeverityLevels in AWS SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeTrustedAdvisorCheckRefreshStatuses`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Per elencare gli stati di aggiornamento dei controlli di AWS Trusted Advisor

L'`describe-trusted-advisor-check-refresh-statuses`esempio seguente elenca gli stati di aggiornamento per due controlli Trusted Advisor: Amazon S3 Bucket Permissions e IAM Use.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Output:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Per ulteriori informazioni, consulta AWS Trusted Advisor nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeTrustedAdvisorCheckRefreshStatuses AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce lo stato corrente delle richieste di aggiornamento per i controlli specificati. Request-ASA TrustedAdvisorCheckRefresh può essere utilizzato per richiedere l'aggiornamento delle informazioni sullo stato dei controlli.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Per i dettagli sull'API, vedere DescribeTrustedAdvisorCheckRefreshStatusesin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeTrustedAdvisorCheckResult`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Per elencare i risultati di un controllo di AWS Trusted Advisor

L'`describe-trusted-advisor-check-result`esempio seguente elenca i risultati del controllo IAM Use.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Output:

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
```

```
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

Per ulteriori informazioni, consulta AWS Trusted Advisor nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeTrustedAdvisorCheckResult in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce i risultati di un controllo di Trusted Advisor. L'elenco dei controlli Trusted Advisor disponibili può essere ottenuto utilizzando Get-ASA TrustedAdvisor Checks. L'output è lo stato generale del controllo, il timestamp in cui il controllo è stato eseguito l'ultima volta e il checkid univoco per il controllo specifico. Per visualizzare i risultati in giapponese, aggiungi il parametro -Language «ja».

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Per i dettagli sull'API, vedere DescribeTrustedAdvisorCheckResult in AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeTrustedAdvisorCheckSummaries`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Per elencare i riepiloghi dei controlli di AWS Trusted Advisor

L'`describe-trusted-advisor-check-summaries`esempio seguente elenca i risultati di due controlli Trusted Advisor: Amazon S3 Bucket Permissions e IAM Use.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Output:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
```

```
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

Per ulteriori informazioni, consulta AWS Trusted Advisor nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeTrustedAdvisorCheckSummaries in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce il riepilogo più recente per il controllo Trusted Advisor specificato.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Esempio 2: restituisce i riepiloghi più recenti per i controlli Trusted Advisor specificati.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Per i dettagli sull'API, vedere DescribeTrustedAdvisorCheckSummaries in AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeTrustedAdvisorChecks`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeTrustedAdvisorChecks`.

CLI

AWS CLI

Per elencare i controlli AWS Trusted Advisor disponibili

L'`describe-trusted-advisor-checks`esempio seguente elenca gli assegni Trusted Advisor disponibili nell' AWS account. Queste informazioni includono il nome, l'ID, la descrizione, la categoria e i metadati dell'assegno. Nota che l'output è abbreviato per motivi di leggibilità.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Output:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

Per ulteriori informazioni, consulta AWS Trusted Advisor nella AWS Support User Guide.

- Per i dettagli sull'API, consulta DescribeTrustedAdvisorChecks AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce la raccolta di assegni Trusted Advisor. È necessario specificare il parametro Language che può accettare «en» per l'output in inglese o «ja» per l'output in giapponese.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- Per i dettagli sull'API, vedere DescribeTrustedAdvisorChecksin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`RefreshTrustedAdvisorCheck`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`RefreshTrustedAdvisorCheck`.

CLI

AWS CLI

Per aggiornare un controllo AWS Trusted Advisor

L'`refresh-trusted-advisor-check`esempio seguente aggiorna il check di Amazon S3 Bucket Permissions Trusted Advisor nel tuo account. AWS

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

Output:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
```

```
    }
}
```

Per ulteriori informazioni, consulta AWS Trusted Advisor nella AWS Support User Guide.

- Per i dettagli sull'API, consulta RefreshTrustedAdvisorCheck AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: richiede un aggiornamento per il controllo Trusted Advisor specificato.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Per i dettagli sull'API, vedere RefreshTrustedAdvisorCheckin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ResolveCase`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`ResolveCase`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Come iniziare con i casi

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }
```

- Per i dettagli sull'API, consulta la ResolveCasesezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per risolvere un caso di assistenza

L'`resolve-case`esempio seguente risolve un caso di assistenza nel tuo AWS account.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Output:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

Per ulteriori informazioni, consulta la sezione Gestione dei casi nella AWS Support User Guide.

- Per i dettagli sull'API, consulta ResolveCase AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();

           ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
           System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, consulta la ResolveCasesezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Per i dettagli sull'API, consulta la ResolveCasesezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
```

```
    }
}
```

- Per i dettagli sull'API, ResolveCaseconsulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce lo stato iniziale del caso specificato e lo stato corrente dopo il completamento della chiamata per risolverlo.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Per i dettagli sull'API, vedere ResolveCasein AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
```

```
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- Per i dettagli sull'API, consulta ResolveCase AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Support con un AWS SDK Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari per l' AWS Support utilizzo AWS degli SDK

I seguenti esempi di codice mostrano come implementare scenari comuni AWS Support con gli AWS SDK. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno. AWS Support Ogni scenario include un collegamento a GitHub, dove è possibile trovare istruzioni su come configurare ed eseguire il codice.

Esempi

- Inizia con i AWS Support casi utilizzando un AWS SDK

Inizia con i AWS Support casi utilizzando un AWS SDK

Gli esempi di codice seguenti mostrano come:

- Ottieni e visualizza i servizi e i livelli di gravità disponibili per i casi.
- Crea una richiesta di supporto utilizzando un servizio, una categoria e un livello di gravità selezionato.
- Ottieni e visualizza un elenco di casi aperti per il giorno corrente.
- Aggiungi un set di collegamenti e una comunicazione al nuovo caso.
- Descrivi il nuovo collegamento e la nuova comunicazione per il caso.
- Risolvi il caso.
- Ottieni e visualizza un elenco di casi risolti per il giorno corrente.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Esegui uno scenario interattivo al prompt dei comandi.

```
/// <summary>
```

```
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the
 list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
 { Profile = "default" })
                    .AddTransient<SupportWrapper>()
```

```
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);

            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);
```

```
            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));
```

```
        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();
```

```
        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");
```

```
        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
{openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
```

```
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);
```

```
        Console.WriteLine($"\tNew attachment set and communication added to
{caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
_supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
{communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");
```

```
        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
```

```
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

Metodi wrapper utilizzati dallo scenario per AWS Support le azioni.

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }


    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
```

```
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
```

```
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
    }



    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
```

```
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
```

```
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
```

```
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
```

```
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }


    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
            }
            else throw;
        }
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API AWS SDK for .NET .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase

- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLivelli
- ResolveCase

Java

SDK per Java 2.x

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Esegui varie AWS Support operazioni.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
```

```
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
```

```
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

   public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

   public static void main(String[] args) {
       final String usage = """

               Usage:
                   <fileAttachment>Where:
                   fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
               """;

       if (args.length != 1) {
           System.out.println(usage);
           System.exit(1);
       }

       String fileAttachment = args[0];
       Region region = Region.US_WEST_2;
       SupportClient supportClient = SupportClient.builder()
               .region(region)
               .build();

       System.out.println(DASHES);
       System.out.println("***** Welcome to the AWS Support case example
 scenario.");
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("1. Get and display available services.");
       List<String> sevCatList = displayServices(supportClient);
       System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("2. Get and display Support severity levels.");
        String sevLevel = displaySevLevels(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
```

```
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
```

```
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
```

```
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
```

```
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);
```

```
            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
```

```
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();
```

```
            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API AWS SDK for Java 2.x .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment

- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLivelli
- ResolveCase

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Esegui uno scenario interattivo nel terminale.

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};

const client = new SupportClient({ region: "us-east-1" });
```

```
// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

/**
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};

// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
```

```
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const selectedSeverityLevel = await inquirer.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *  selectedService: import('@aws-sdk/client-support').Service
 *  selectedCategory: import('@aws-sdk/client-support').Category
 *  selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};

// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);
```

```
  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases.",
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
 */
```

```
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0,
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const shouldResolve = await inquirer.confirm({
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};

/**
 * Find a specific case in the list of provided cases by case ID.
 * If the case is not found, and the results are paginated, continue
 * paging through the results.
 * @param {{
 *   caseId: string,
 *   cases: import('@aws-sdk/client-support').CaseDetails[]
 *   nextToken: string
 * }} options
 * @returns
 */
```

```
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      }),
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
```

```
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
the user to select one.
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases,
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`,
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

    // Create an attachment set.
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);

    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
```

```
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
 ${c.attachmentSet.length} attachments.`,
        )
        .join("\n"),
    );

    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`,
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
 time.",
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId),
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API AWS SDK for JavaScript .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLivelli
  - ResolveCase

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
```

```
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }
```

```
    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
 to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 30
            afterTime = yesterday.toString()
            beforeTime = now.toString()
            includeResolvedCases = true
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
```

```
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
```

```
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
```

```
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
```

```
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Kotlin.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLivelli
  - ResolveCase

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Esegui uno scenario interattivo al prompt dei comandi.

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
 preceding list:",
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service
```

```
    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity
```

```
    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id
```

```
    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.
```

```
        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
%(message)s")

        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
```

```
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Definisci una classe che racchiuda le operazioni di supporto al cliente.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
```

```
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
```

```
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
```

```
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
```

```
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
```

```
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
```

```
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
```

```
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
```

```
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Python (Boto3).
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLivelli
  - ResolveCase

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo AWS Support con un AWS SDK. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Monitoraggio e logging per AWS Support

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Support e delle altre soluzioni AWS. AWS fornisce i seguenti strumenti di monitoraggio per controllare AWS Support, segnalare eventuali problemi ed eseguire operazioni automatiche quando appropriato:

- Amazon EventBridge fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche nelle risorse AWS. EventBridge consente il calcolo automatizzato basato sugli eventi, così che tu possa scrivere le regole che osservano determinati eventi e attivano le operazioni automatizzate in altri servizi AWS quando si verificano gli eventi. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon EventBridge.
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti

Monitoraggio AWS Support dei casi con Amazon EventBridge

Puoi utilizzare Amazon EventBridge per rilevare e reagire ai cambiamenti dei tuoi AWS Support casi. 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 dell'evento, puoi inviare notifiche, acquisire informazioni sull'evento, intraprendere un'operazione correttiva, avviare eventi o eseguire altre operazioni. Ad esempio, puoi ricevere notifiche ogni volta che si verificano le seguenti azioni nel tuo account:

- Creazione di una richiesta di supporto
- Aggiungi una corrispondenza del caso a un caso di supporto esistente
- Risoluzione di un caso di supporto

- Riaprire un caso di supporto

> **Note**
>
> AWS Support distribuisce eventi sulla base del massimo sforzo. Non è sempre garantito che gli eventi vengano consegnati a EventBridge.

Creazione di una regola EventBridge per i casi AWS Support

Puoi creare una EventBridge regola per ricevere notifiche relative agli eventi del AWS Support caso. La regola monitorerà gli aggiornamenti per i casi di supporto nel tuo account, incluse le azioni eseguite da te, dagli utenti IAM o dagli agenti di supporto. Prima di creare una regola per i casi di eventi di AWS Support, dovresti assicurarti di:

- Acquisisci familiarità con eventi, regole e obiettivi in. EventBridge Per ulteriori informazioni, consulta What is Amazon EventBridge? nella Amazon EventBridge User Guide.
- Creare la destinazione da utilizzare nelle regole degli eventi. Ad esempio, puoi creare un argomento Amazon Simple Notification Service (Amazon SNS) in modo che ogni volta che viene aggiornato un caso di supporto, riceverai un messaggio di testo o un'e-mail. Per ulteriori informazioni, consulta Destinazioni EventBridge.

> **Note**
>
> AWS Support è un servizio globale. Per ricevere gli aggiornamenti per i casi di assistenza, puoi utilizzare una delle seguenti regioni: Regione Stati Uniti orientali (Virginia settentrionale), Regione Stati Uniti occidentali (Oregon) o Regione Europa (Irlanda).

Per creare una EventBridge regola per gli eventi AWS Support relativi ai casi

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Se non lo hai ancora fatto, utilizza il Selettore di regione nell'angolo in alto a destra della pagina e seleziona Stati Uniti orientali (Virginia settentrionale).
3. Nel pannello di navigazione, scegli Regole.
4. Scegli Crea regola.

5. Nella pagina Definisci dettagli della regola, inserisci un nome e una descrizione per la regola.
6. Mantiei i valori predefiniti di per Bus di eventi e Tipo di regola, quindi scegli Avanti.
7. Nella pagina Crea modello di evento, per Event source, scegli AWSeventi o eventi EventBridge partner.
8. Nel Modello di eventi, mantiene il valore predefinito per Servizi AWS.
9. Per Servizio AWS, scegli Support (Supporto).
10. Per Event type (Tipo di evento), scegliere (Support Case Update) Aggiornamento dei casi di supporto).
11. Seleziona Avanti.
12. Nella sezione Select targets (Seleziona destinazioni), scegli la destinazione creata per questa regola, quindi configurare le eventuali altre opzioni richieste per quel tipo. Ad esempio, se scegli Amazon SNS, assicurati che il tuo argomento SNS sia configurato correttamente in modo da ricevere una notifica via e-mail o SMS.
13. Seleziona Avanti.
14. (Facoltativo) Nella pagina Aggiungi tag, aggiungi tag alla chiave, quindi scegli Avanti.
15. Nella pagina Rivedi e crea, rivedi la configurazione della regola e fai in modo che soddisfi i requisiti di monitoraggio degli eventi.
16. Scegli Crea regola. La tua regola ora monitorerà i casi di eventi AWS Support che vanno successivamente inviati alla destinazione specificata.

> **Note**
>
> - Quando ricevi un evento, puoi usare il parametro `origin` per determinare se tu o un agente AWS Support avete aggiunto una corrispondenza del caso a un caso di supporto. Il valore per `origin` può essere `CUSTOMER` o `AWS`.
>
> Attualmente, solo eventi per l'azione `AddCommunicationToCase` avranno questo valore.
> - Per ulteriori informazioni sulla creazione di pattern di eventi, consulta Event pattern nella Amazon EventBridge User Guide.
> - Puoi inoltre creare un'altra regola per il tipo di evento Chiamata API AWS tramite CloudTrail. Questa regola monitorerà AWS CloudTrail registri per Chiamate API AWS Support nel tuo account.

Eventi di esempio AWS Support

I seguenti eventi vengono creati quando si verificano azioni di supporto nel tuo account.

Example : Creazione di un caso di supporto

Il seguente evento viene creato quando viene creato un caso di supporto.


```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```


Example : Aggiornamento di un caso di supporto

Il seguente evento viene creato quando AWS Support risponde a un caso di supporto.


```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
```

```
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example : Risoluzione di un caso di supporto

Il seguente evento viene creato quando viene risolto un caso di supporto.

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example : Riapertura di un caso di supporto

Il seguente evento viene creato quando viene riaperto un caso di supporto.

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
```

```
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

Consulta anche

Per ulteriori informazioni su come utilizzare EventBridge conAWS Support, consulta le seguenti risorse:

- Come automatizzare le AWS Support API con Amazon EventBridge
- AWS Supportcase activity notificator attivo GitHub

Registrazione delle chiamate API AWS Support con AWS CloudTrail

AWS Support è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in AWS Support. CloudTrail acquisisce le chiamate API AWS Support come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS Support e le chiamate di codice alle operazioni delle API AWS Support.

Se crei un percorso, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per AWS Support. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi).

Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad AWS Support, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

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

Informazioni su AWS Support in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività evento supportata in AWS Support, tale attività viene registrata in un evento CloudTrail insieme ad

altri eventi di servizio di AWS in Event history (Cronologia eventi). È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per AWS Support, crea un trail. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail 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 servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più Regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni dell'API AWS Support vengono registrate da CloudTrail e documentate nella Documentazione di riferimento delle API AWS Support.

Ad esempio, le chiamate alle operazioni `CreateCase`, `DescribeCases` e `ResolveCase` generano voci nei file di log di CloudTrail.

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

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Puoi inoltre aggregare file di log AWS Support da più Regioni AWS e da più account AWS in un singolo bucket Amazon S3.

Informazioni di AWS Trusted Advisor nella registrazione di CloudTrail

Trusted Advisor è una servizio AWS Support che ti consente di controllare il tuo account AWS per trovare soluzioni per risparmiare sui costi, migliorare la sicurezza e ottimizzare il tuo account.

Tutte le operazioni dell'API Trusted Advisor vengono registrate da CloudTrail e documentate nella Documentazione di riferimento delle API AWS Support.

Ad esempio, le chiamate alle operazioni `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` e `RefreshTrustedAdvisorCheck` generano voci nei file di log di CloudTrail.

> **Note**
>
> CloudTrail registra anche le operazioni della console Trusted Advisor. Per informazioni, consultare Registrazione delle azioni AWS Trusted Advisor della console con AWS CloudTrail.

Comprensione delle voci dei file di log di AWS Support

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine. Ogni evento include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Example : Voce di log per CreateCase

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione CreateCase.

```
{
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
```

```
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
         },
         "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
         "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
         "eventType": "AwsApiCall",
         "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example : Voce di log per RefreshTrustedAdvisorCheck

L'esempio seguente mostra una voce di log di CloudTrail per l'operazioneRefreshTrustedAdvisorCheck.

```
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Registrazione dell'app AWS Support nelle chiamate API Slack utilizzando AWS CloudTrail

L'app AWS Support in Slack è integrata con AWS CloudTrail. CloudTrail fornisce un record delle operazioni eseguite da un utente, un ruolo o un Servizio AWS nell'app AWS Support. Per creare questo record, CloudTrail acquisisce tutte le chiamate API pubbliche per l'app AWS Support come eventi. Queste chiamate acquisite includono le chiamate dalla console dell'app AWS Support e le chiamate di codice alle operazioni delle API pubbliche dell'app AWS Support. Se crei un percorso, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, Questi includono eventi per l'app AWS Support. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi. Puoi utilizzare le informazioni raccolte da CloudTrail per determinare se la richiesta è stata inviata all'app AWS Support. Puoi inoltre ottenere informazioni sull'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

Informazioni sull'app AWS Support in CloudTrail

CloudTrail è attivato sul tuo Account AWS al momento della creazione dell'account stesso. Quando si verifica un'attività dell'API pubblica nell'app AWS Support, tale attività viene registrata in un evento CloudTrail insieme ad altri eventi del servizio AWS in Event history (Cronologia eventi). Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'Account AWS, compresi gli eventi dell'app AWS Support, crea un trail. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri Servizi AWS per analizzare con maggiore dettaglio i dati evento raccolti nei registri CloudTrail e utilizzarli. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più Regioni e Ricezione di file di registro CloudTrail da più account

CloudTrail registra tutte le operazioni pubbliche dell'app AWS Support. Queste operazioni sono documentate anche nella documentazione di riferimento sull'API dell'app AWS Support in Slack. Ad esempio, le chiamate alle operazioni `CreateSlackChannelConfiguration`, `GetAccountAlias` e `UpdateSlackChannelConfiguration` generano voci nei file di log di CloudTrail.

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

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci di file di registro dell'app AWS Support

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sul operazione richiesta, data e ora dell'operazione, parametri richiesti e così via. I file di registro CloudTrail non sono una traccia dello stack ordinata delle chiamate API pubbliche. Ciò significa che i registri non vengono visualizzati in base a un ordine specifico.

Example : esempio di registro per **`CreateSlackChannelConfiguration`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione CreateSlackChannelConfiguration.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
```

```
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : esempio di registro per **`ListSlackChannelConfigurations`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione ListSlackChannelConfigurations.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : esempio di registro per **`GetAccountAlias`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione GetAccountAlias.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Monitoraggio e registrazione per i piani di AWS Support

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni dei piani di supporto e delle altre soluzioni AWS. AWS fornisce i seguenti strumenti di monitoraggio per controllare i piani di supporto, segnalare eventuali problemi ed eseguire operazioni automatiche quando appropriato:

- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti

Registrazione delle chiamate API dei piani di AWS Support con AWS CloudTrail

I piani di AWS Support sono integrati con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un Servizio AWS. CloudTrail acquisisce le chiamate API per i piani di AWS Support come eventi. Le chiamate acquisite includono le chiamate dalla console dei piani di AWS Support e le chiamate di codice alle operazioni delle API dei piani di AWS Support.

Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per i piani di AWS Support. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi.

Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ai piani di AWS Support, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

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

Informazioni sui piani di AWS Support in CloudTrail

CloudTrail è abilitato sul tuo Account AWS al momento della sua creazione. Quando si verifica un'attività evento supportata nei piani di AWS Support, tale attività viene registrata in un evento CloudTrail insieme ad altri eventi del Servizio AWS in Event history (Cronologia eventi). È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account . Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account, inclusi gli eventi dei piani di AWS Support, crea un trail. Un percorso consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. 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 Servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei registri CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più Regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni API dei piani di AWS Support sono registrate da CloudTrail. Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Puoi inoltre aggregare file di registro dei piani di AWS Support da più Regioni AWS e da più account in un singolo bucket Amazon S3.

Comprensione delle voci dei file di registro dei piani di AWS Support

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine. Ogni evento include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Example : voce di registro per **`GetSupportPlan`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione `GetSupportPlan`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
```

```
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : voce di registro per **`GetSupportPlanUpdateStatus`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione `GetSupportPlanUpdateStatus`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
```

```
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : voce di registro per **`StartSupportPlanUpdate`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione `StartSupportPlanUpdate`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : voce di registro per **`CreateSupportPlanSchedule`**

L'esempio seguente mostra una voce di registro di CloudTrail che illustra l'operazione `CreateSupportPlanSchedule`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
```

```
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Registrazione di log per le modifiche al piano AWS Support

> **Important**
>
> A partire dal 3 agosto 2022, le seguenti operazioni sono obsolete e non verranno visualizzate nei nuovi registri di CloudTrail. Per un elenco delle operazioni supportate, consulta Comprensione delle voci dei file di registro dei piani di AWS Support.

- `DescribeSupportLevelSummary`: Questa operazione compare nel log quando apri la pagina Piani di supporto.
- `UpdateProbationAutoCancellation`: Dopo aver effettuato l'iscrizione al Supporto per gli sviluppatori o al Supporto per le aziende e aver tentato di annullare entro 30 giorni, il piano verrà automaticamente annullato al termine di tale periodo. Questa operazione compare nel log quando scegli Rifiuta disattivazioni automatiche nel banner che compare nella pagina Piani di supporto. Riprenderai il piano per il Supporto per gli sviluppatori o il Supporto per le aziende.
- `UpdateSupportLevel`: questa operazione compare nel registro quando modifichi il piano di supporto.

> **Note**
>
> Il campo `eventSource` ha lo spazio dei nomi `support-subscription.amazonaws.com` per queste azioni.

Example : Voce di registro per DescribeSupportLevelSummary

L'esempio seguente mostra una voce di log di CloudTrail per l'operazione `DescribeSupportLevelSummary`.

```
{
```

```
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example : Voce di registro per UpdateProbationAutoCellation

L'esempio seguente mostra una voce di log di CloudTrail per l'operazione `UpdateProbationAutoCancellation`.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : Voce di registro per UpdateSupportLevel

L'esempio seguente mostra una voce di log di CloudTrail per l'operazione `UpdateSupportLevel` che consente di passare al Supporto per gli sviluppatori.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
```

```
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Monitoraggio e logging per AWS Trusted Advisor

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Trusted Advisor e delle altre soluzioni AWS. AWS fornisce i seguenti strumenti di monitoraggio per controllare Trusted Advisor, segnalare eventuali problemi ed eseguire operazioni automatiche quando appropriato:

- Amazon EventBridge fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche nelle risorse AWS. EventBridge consente il calcolo automatizzato basato sugli eventi, così che tu possa scrivere le regole che osservano determinati eventi e attivano le operazioni automatizzate in altri servizi AWS quando si verificano gli eventi.

  Ad esempio, Trusted Advisor fornisce il controllo delle Autorizzazioni di un Bucket Amazon S3. Questo controllo ti consente di identificare se hai dei bucket che dispongono di autorizzazioni di accesso aperto o che consentono l'accesso a qualsiasi utente AWS autenticato. Se viene modificata l'autorizzazione di un bucket, lo stato cambia per il controllo Trusted Advisor. EventBridge rileva questo evento e invia una notifica in modo da poter agire. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon EventBridge.
- AWS Trusted Advisor controlla modalità per ridurre i costi, aumentare le prestazioni e migliorare la sicurezza per il tuo account AWS. Puoi utilizzare EventBridge per monitorare lo stato dei controlli Trusted Advisor. Puoi quindi utilizzare Amazon CloudWatch per creare allarmi sui parametri Trusted Advisor. Questi allarmi ti avvisano quando lo stato cambia per un controllo Trusted Advisor, ad esempio quando viene aggiornata una risorsa oppure quando viene raggiunta una quota.
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo account AWS e fornisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti

Monitoraggio dei risultati dei AWS Trusted Advisor controlli con Amazon EventBridge

Puoi utilizzarla EventBridge per rilevare quando i controlli Trusted Advisor cambiano stato. Quindi, in base alle regole create, EventBridge richiama una o più azioni mirate quando lo stato passa a un valore specificato in una regola.

A seconda del cambiamento dello stato, puoi inviare notifiche, acquisire informazioni sullo stato, intraprendere un'azione correttiva, avviare eventi o eseguire altre operazioni. Ad esempio, è possibile specificare i seguenti tipi di destinazione se un controllo cambia lo stato da nessun problema rilevato (verde) a un'azione suggerita (rosso).

- Utilizza una funzione AWS Lambda per inoltrare una notifica a un canale Slack.
- Immetti dati sui controlli Amazon Kinesis per supportare un monitoraggio completo e in tempo reale dello stato.
- Invia un argomento Amazon Simple Notification Service sulla tua e-mail.
- Ricevi una notifica con un'azione di CloudWatch allarme di Amazon.

Per ulteriori informazioni su come utilizzare le funzioni Lambda EventBridge e sulle quali automatizzare le risposteTrusted Advisor, consulta Trusted Advisor gli strumenti in. GitHub

> **Note**
>
> - Trusted Advisor distribuisce eventi sulla base del massimo sforzo. Non è sempre garantito che gli eventi vengano consegnati a EventBridge.
> - Devi disporre di un piano AWS Support Business, Enterprise On-Ramp o Enterprise per creare una regola per i controlli Trusted Advisor. Per ulteriori informazioni, consulta Modifica AWS Support dei piani.
> - Trusted AdvisorTrattandosi di un servizio globale, tutti gli eventi vengono emessi EventBridge nella regione Stati Uniti orientali (Virginia settentrionale).

Segui questa procedura per creare una EventBridge regola per. Trusted Advisor Prima di creare regole per gli eventi, dovresti assicurarti di:

- Acquisisci familiarità con eventi, regole e obiettivi in. EventBridge Per ulteriori informazioni, consulta What is Amazon EventBridge? nella Amazon EventBridge User Guide.
- Creare la destinazione da utilizzare nella regola dell'evento.

Per creare una EventBridge regola per Trusted Advisor

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Per modificare la Regione, utilizza il Selettore di regione nell'angolo in alto a destra della pagina e seleziona Stati Uniti orientali (Virginia settentrionale).
3. Nel pannello di navigazione, scegli Regole.
4. Scegli Crea regola.
5. Nella pagina Definisci dettagli della regola, inserisci un nome e una descrizione per la regola.
6. Mantiei i valori predefiniti di per Bus di eventi e Tipo di regola, quindi scegli Avanti.
7. Nella pagina Crea modello di evento, per Event source, scegli AWSeventi o eventi EventBridge partner.
8. Nel Modello di eventi, mantiene il valore predefinito per Servizi AWS.
9. Per Servizio AWS, scegliere Trusted Advisor.
10. Per Event type (Tipo di evento), selezionare Verifica stato aggiornamento dell'elemento.
11. Scegli una delle seguenti opzioni per lo stato dei controlli:
    - Scegli Any status (Qualsiasi stato) per creare una regola che monitora eventuali modifiche di stato.
    - Scegli Specif status(es) (Stato/i specifico/i) e quindi i valori che desideri che vengano monitorati dalla regola.
        - ERROR – Trusted Advisor rileva un errore e consiglia un'azione per il controllo.
        - INFO – Trusted Advisor non è in grado di determinare lo stato del controllo.
        - OK – Trusted Advisor non rileva un problema per il controllo.
        - WARN – Trusted Advisor rileva un possibile problema per il controllo e suggerisce un'indagine.
12. Scegli una delle seguenti opzioni per i tuoi controlli:
    - Scegli Any check (Qualsiasi controllo).
    - Scegli Specific check(s) (Controllo/i specifico/i) e quindi uno o più nomi dei controlli dall'elenco.

13. Per le risorse AWS, scegliere una delle seguenti opzioni:
    - Scegli Any resource ID (Qualsiasi ID della risorsa) per creare una regola che monitora tutte le risorse.
    - Scegli Specific resource ID(s) by ARN (ID risorsa specifico per ARN) e quindi inserisci gli Amazon Resource Name (ARN) che desideri.
14. Seleziona Avanti.
15. Nella pagina Seleziona destinazioni scegli la tipologia di destinazione creata per questa regola, quindi configura le eventuali opzioni aggiuntive richieste per quel tipo. Ad esempio, potresti inviare l'evento a una coda Amazon SQS o a un argomento Amazon SNS.
16. Seleziona Avanti.
17. (Facoltativo) Nella pagina Aggiungi tag, aggiungi tag alla chiave, quindi scegli Avanti.
18. Nella pagina Rivedi e crea, rivedi la configurazione della regola e fai in modo che soddisfi i requisiti di monitoraggio degli eventi.
19. Scegli Crea regola. La tua regola ora monitorerà i controlli Trusted Advisor e poi invierà l'evento alla destinazione specificata.

Creazione di allarmi Amazon CloudWatch per monitorare i parametri AWS Trusted Advisor

Quando AWS Trusted Advisor aggiorna i controlli, Trusted Advisor pubblica i parametri sui risultati dei controlli su CloudWatch. Puoi visualizzare i parametri anche su CloudWatch. Puoi anche creare allarmi per individuare i cambiamenti dello stato per i controlli Trusted Advisor e i cambiamenti di stato per le risorse e gli utilizzi della quota di servizio (indicati in precedenza come limiti). Ad esempio, è possibile creare un allarme per monitorare le modifiche di stato per i controlli nella categoria Limiti di servizio. L'allarme ti avviserà quando raggiungi o superi una quota di servizio per il tuo account AWS.

Segui questa procedura per creare un allarme CloudWatch per un parametro Trusted Advisor specifico.

Argomenti

- Parametri e dimensioni di Trusted Advisor

Prerequisiti

Prima di creare allarmi CloudWatch per i parametri Trusted Advisor, verifica le seguenti informazioni:

- Scopri come CloudWatch utilizza parametri e allarmi. Per ulteriori informazioni, consulta la sezione Funzionamento di CloudWatch nella Guida per l'utente di Amazon CloudWatch.
- Utilizza la console Trusted Advisor o l'API AWS Support per aggiornare i controlli e ottenere i risultati più recenti. Per ulteriori informazioni, consulta Aggiorna i risultati di controllo.

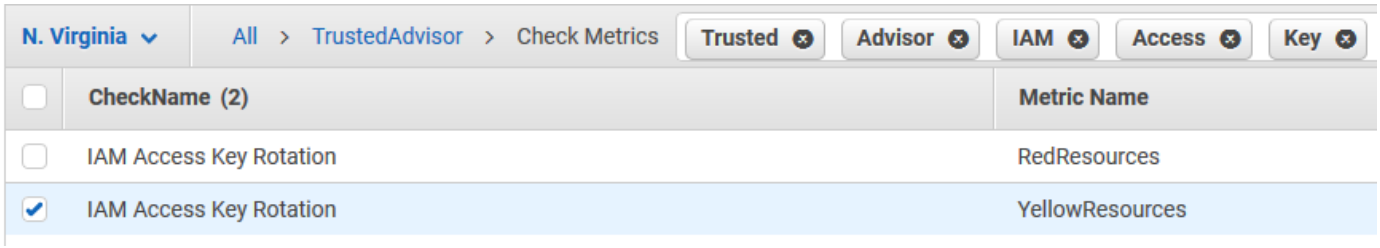
Come creare un allarme CloudWatch per i parametri Trusted Advisor

1. Aprire la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Utilizzare il selettore di Regione e scegliere la Regione AWS Stati Uniti orientali (Virginia settentrionale).
3. Nel riquadro di navigazione, seleziona Allarmi (Alarms).
4. Scegli Crea allarme.
5. Scegli Select Metric (Seleziona parametro).
6. Per Parametri, inserisci uno o più valori relativi alle dimensioni per filtrare l'elenco di parametri. Ad esempio, è possibile inserire il nome del parametro ServiceLimitUsage o la dimensione, come il nome del controllo Trusted Advisor.

   > **Tip**
   >
   > - È possibile cercare **`Trusted Advisor`** per elencare tutti i parametri del servizio.
   > - Per consultare un elenco dei nomi di parametri e dimensioni, consulta la sezione Parametri e dimensioni di Trusted Advisor.

7. Nella tabella dei risultati, seleziona la casella di controllo relativa al parametro.

   Nell'esempio seguente, il nome del controllo è IAM Access Key Rotation (Rotazione delle chiavi di accesso IAM) e il nome del parametro è YellowResources.

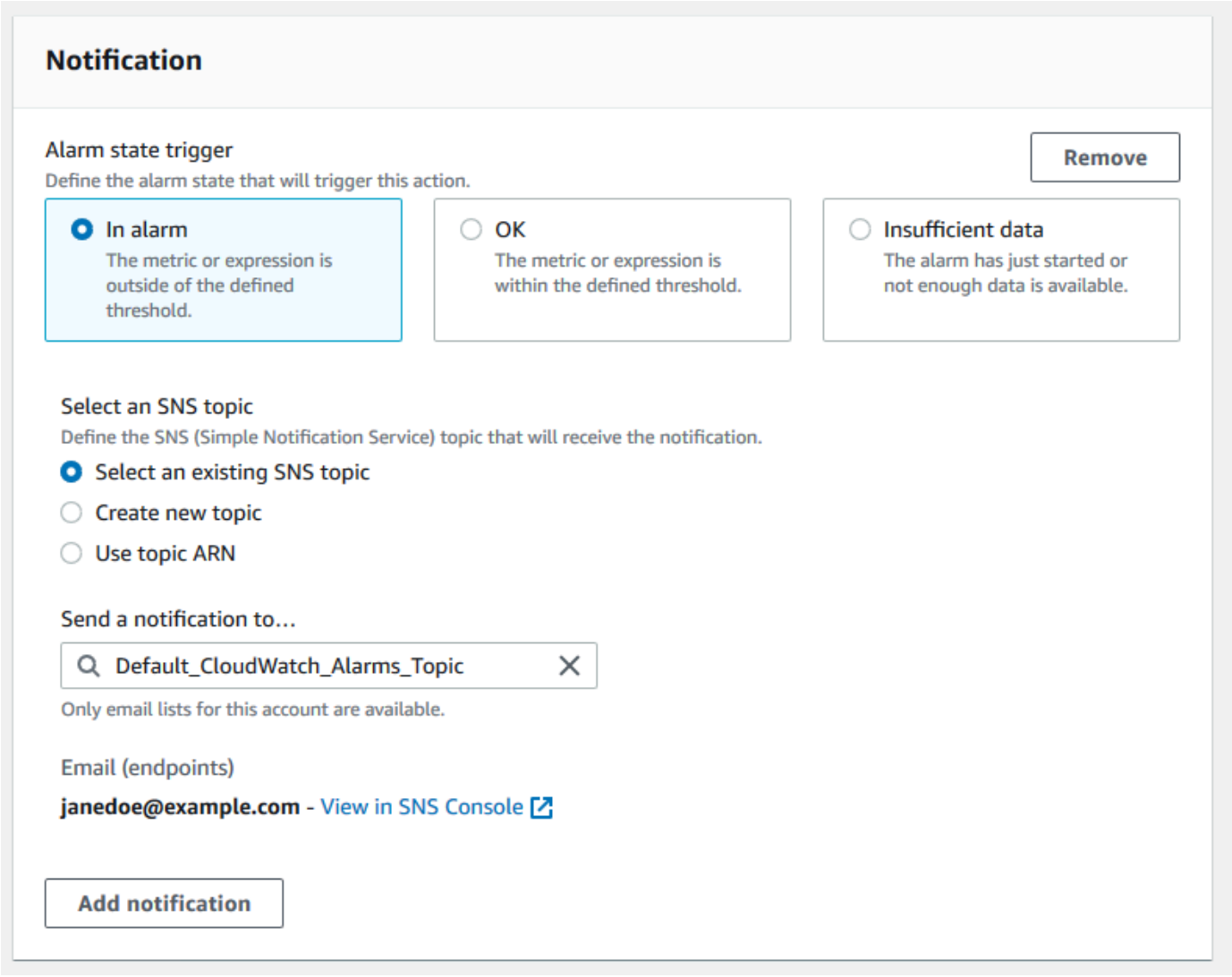


8. Scegli Select Metric (Seleziona parametro).
9. Nella pagina Specify metric and conditions (Specifica parametri e condizioni), verificare che il Metric name (Nome parametro) e il CheckName (NomeControllo) che hai scelto appaiano sulla pagina.
10. Per Period (Periodo), è possibile specificare il periodo di tempo in cui desideri far scattare l'allarme quando lo stato del controllo cambia, ad esempio 5 minuti.
11. Alla voce Conditions (Condizioni), scegli Static (Statico), quindi specificare la condizione di allarme per l'avvio dell'avviso.

    Ad esempio, scegliendo Greater/Equal >=threshold (Maggiore/Uguale >=soglia) e inserendo **1** per il valore-soglia, l'allarme inizia quando Trusted Advisor rileva almeno una chiave di accesso IAM che non è stata ruotata negli ultimi 90 giorni.

    > **Note**
    >
    > - Per i parametri GreenChecks, RedChecks, YellowChecks, RedResources e YellowResources, è possibile specificare questa soglia, che può essere qualsiasi numero intero maggiore o uguale a zero.
    > - Trusted Advisor non invia parametri per GreenResources, che sono risorse per le quali Trusted Advisor non ha rilevato alcun problema.

12. Seleziona Successivo.
13. Nella pagina Configure actions (Configurazione delle operazioni), alla voce Alarm state trigger (Attivazione dello stato di allarme), scegli In alarm (In allarme).
14. Per Select an SNS topic (Seleziona un argomento SNS), scegli un argomento Amazon Simple Notification Service (Amazon SNS) esistente o creane uno.



15. Seleziona Successivo.
16. Per Name and description (Nome e descrizione), inserisci un nome e una descrizione per il tuo allarme.
17. Seleziona Successivo.
18. Nella pagina Preview and create (Visualizza anteprima e crea), revisiona i dettagli dell'allarme, quindi scegli Create alarm (Crea allarme).

    Quando lo stato per il controllo Rotazione delle chiavi di accesso IAM diventa rosso per 5 minuti, l'allarme invierà una notifica al tuo argomento SNS.

Example : Notifica via e-mail per un allarme CloudWatch

Il seguente messaggio di posta elettronica mostra che un allarme ha rilevato una modifica per il controllo Rotazione delle chiavi di accesso IAM.

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
```

```
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

Parametri CloudWatch per Trusted Advisor

È possibile utilizzare la console di CloudWatch o la AWS Command Line Interface (AWS CLI) per trovare i parametri disponibili per Trusted Advisor.

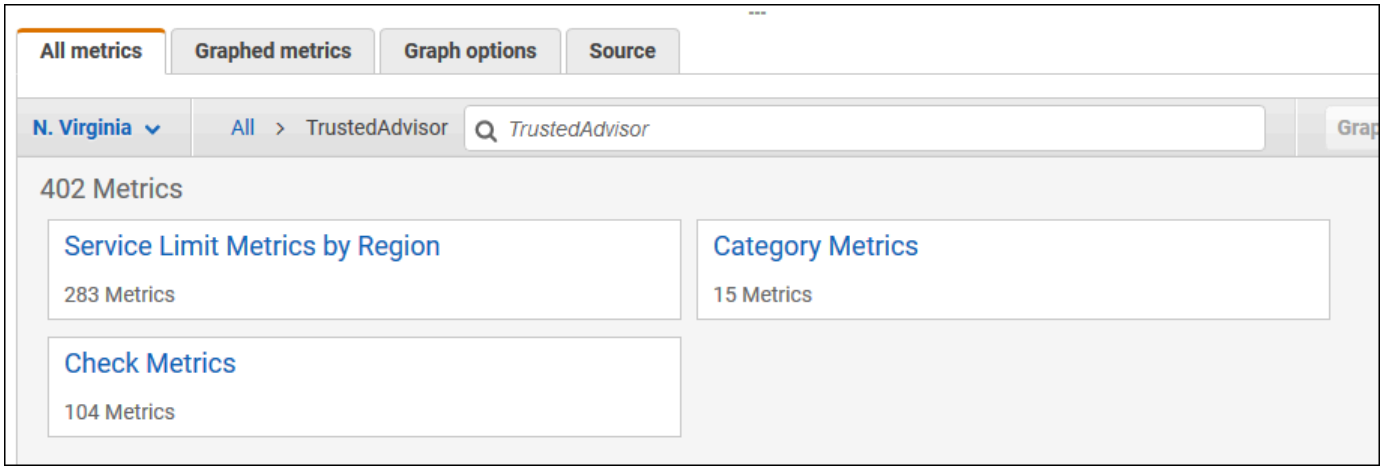
Per un elenco degli spazi dei nomi, dei parametri e delle dimensioni di tutti i servizi che pubblicano parametri, consulta Servizi AWS che pubblicano parametri CloudWatch nella Guida per l'utente di Amazon CloudWatch.

Visualizza i parametri Trusted Advisor (console)

È possibile accedere alla console CloudWatch e visualizzare i parametri disponibili per Trusted Advisor.

Per visualizzare i parametri Trusted Advisor disponibili (console)

1. Aprire la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Utilizzare il selettore di Regione e scegliere la Regione AWS Stati Uniti orientali (Virginia settentrionale).
3. Nel riquadro di navigazione, selezionare Parametri.
4. Inserire uno spazio dei nomi del parametro, ad esempio **`TrustedAdvisor`**.
5. Scegliere una dimensione del parametro, ad esempio Check Metrics (Parametri di controllo).



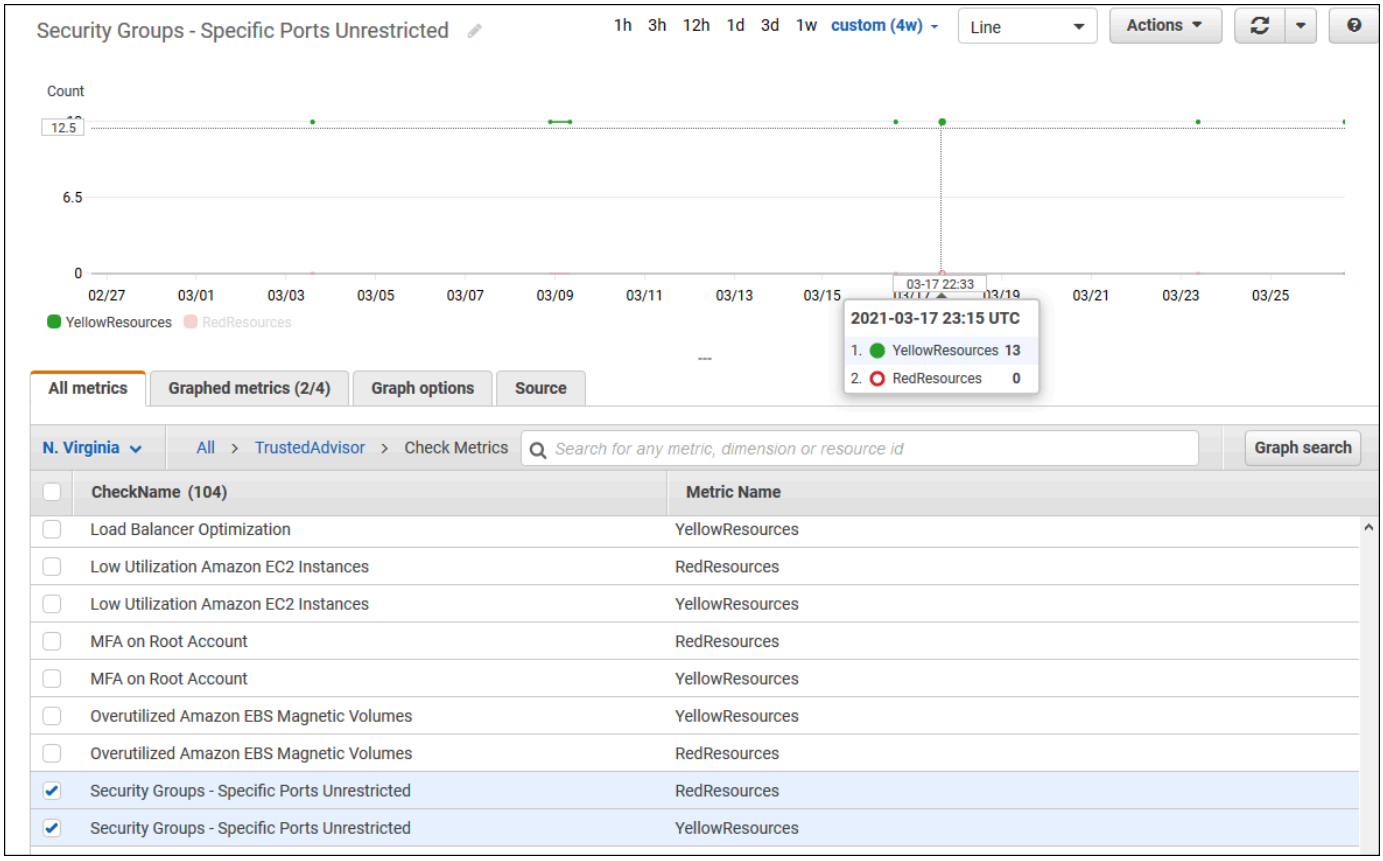
6. La scheda All metrics (Tutti i parametri) mostra tutti i parametri per quella dimensione nello spazio dei nomi. Puoi eseguire le operazioni indicate di seguito:

a. Per ordinare la tabella, utilizza l'intestazione della colonna.

b. Per creare il grafico di un parametro, seleziona la casella di controllo accanto al parametro. Per selezionare tutte i parametri, seleziona la casella di controllo nella riga dell'intestazione della tabella.

c. Per filtrare in base a un parametro, scegli il nome del parametro e quindi Add to search (Aggiungi alla ricerca).

L'esempio seguente mostra i risultati per il controllo Security Groups - Specific Ports Unrestricted (Gruppi di sicurezza: Porte specifiche senza restrizioni). Il controllo identificherà 13 risorse in giallo. Trusted Advisor consiglia di esaminare i controlli in giallo.



7. (Facoltativo) Per aggiungere il grafico a un pannello di controllo CloudWatch, seleziona Actions (Operazioni), quindi scegli Add to dashboard (Aggiungi a pannello di controllo).

Per ulteriori informazioni sulla creazione di un grafico per visualizzare i parametri, consulta Graphing a metric (Rappresentazione grafica di un parametro) nella Guida per l'utente di Amazon CloudWatch.

Visualizza i parametri Trusted Advisor (CLI)

Puoi utilizzare il comando list-metrics della AWS CLI per visualizzare i parametri disponibili per Trusted Advisor.

Example : Elenca tutti i parametri per Trusted Advisor

L'esempio seguente specifica lo spazio dei nomi `AWS/TrustedAdvisor` per visualizzare tutti i parametri per Trusted Advisor.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

Il risultato potrebbe essere simile al seguente.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
```

```
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : Elenca tutti i parametri per una dimensione

L'esempio seguente specifica lo spazio dei nomi `AWS/TrustedAdvisor` e la dimensione `Region` per visualizzare i parametri disponibili per la Regione AWS specificata.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

Il risultato potrebbe essere simile al seguente.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
```

```
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : Elenca i parametri per un nome parametro specifico

L'esempio seguente specifica lo spazio dei nomi `AWS/TrustedAdvisor` e il nome parametro `RedResources` per visualizzare i risultati solo per il parametro specificato.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

Il risultato potrebbe essere simile al seguente.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
```

```
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Parametri e dimensioni di Trusted Advisor

Consulta le seguenti tabelle per i parametri e le dimensioni Trusted Advisor utilizzabili per gli allarmi e i grafici di CloudWatch.

Parametri a livello di controllo di Trusted Advisor

Puoi utilizzare le seguenti parametri per i controlli Trusted Advisor.

Parametro	Descrizione
`RedResources`	Il numero di risorse in rosso (azione consigliata).
`YellowResources`	Il numero di risorse in giallo (indagine consigliata).

Parametri a livello di categoria di Trusted Advisor.

Puoi utilizzare i seguenti parametri per le categorie Trusted Advisor.

Parametro	Descrizione
`GreenChecks`	Il numero di controlli Trusted Advisor in verde (nessun problema rilevato).
`RedChecks`	Il numero di controlli Trusted Advisor in rosso (azione consigliata).
`YellowChecks`	Il numero di controlli Trusted Advisor in giallo (indagine consiglia ta).

Parametri a livello di quota di servizio Trusted Advisor

Puoi utilizzare i seguenti parametri per le quote Servizio AWS.

Parametro	Descrizione
`ServiceLimitUsage`	Percentuale di utilizzo delle risorse rispetto a una quota di servizio (precedentemente definita limiti).

Dimensioni per i parametri a livello di controllo

Puoi utilizzare le seguenti dimensioni per i controlli Trusted Advisor.

Dimensione	Descrizione
`CheckName`	Il nome del controllo Trusted Advisor. Puoi trovare tutti i nomi dei controlli nella console Trusted Advisor o in AWS Trusted Advisor verifica riferimento.

Dimensioni per i parametri a livello di categoria

Puoi utilizzare la dimensione seguente per le categorie di controllo Trusted Advisor.

Dimensione	Descrizione
`Category`	Nome di una categoria di controllo Trusted Advisor. Puoi trovare tutte le categorie di controllo nella console Trusted Advisor o nella pagina Visualizza le categorie di controllo.

Dimensioni per i parametri della quota di servizio

Puoi utilizzare le seguenti dimensioni per i parametri della quota di servizio Trusted Advisor.

Dimensione	Descrizione
`Region`	La Regione AWS per una quota di servizio.
`ServiceName`	Nome della Servizio AWS.
`ServiceLimit`	Il nome della quota di servizio. Per ulteriori informazioni sulle quote di servizio, consulta Quote di Servizio AWS nella Riferimenti generali di AWS.

Registrazione delle azioni AWS Trusted Advisor della console con AWS CloudTrail

Trusted Advisor è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Trusted Advisor. CloudTrail acquisisce azioni per eventi Trusted Advisor analoghi. Le chiamate acquisite includono le chiamate provenienti dalla Trusted Advisor console. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per. Trusted Advisor 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 Trusted Advisor, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

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

Trusted Advisor informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata nella Trusted Advisor console, 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 Trusted Advisor, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS . Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

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

Trusted Advisor supporta la registrazione di un sottoinsieme delle azioni della Trusted Advisor console come eventi nei CloudTrail file di registro. CloudTrail registra le seguenti azioni:

- BatchUpdateRecommendationResourceExclusion
- CreateEngagement
- CreateEngagementAttachment
- CreateEngagementCommunication
- CreateExcelReport
- DescribeAccount
- DescribeAccountAccess
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeChecks
- DescribeNotificationPreferences
- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks

- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

Per un elenco completo delle azioni della Trusted Advisor console, vedereTrusted Advisor azioni.

> **Note**
>
> CloudTrail registra anche le operazioni dell' Trusted Advisor API nell'AWS Support API Reference. Per ulteriori informazioni, consulta Registrazione delle chiamate API AWS Support con AWS CloudTrail.

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

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).

- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Esempio: voci dei file di Trusted Advisor registro

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

Example : Inserimento del registro per RefreshCheck

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`RefreshCheck`azione per il controllo (ID) di Amazon S3 Bucket Versioning. R365s2Qddf


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
```

```
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : Inserimento del log per UpdateNotificationPreferences

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`UpdateNotificationPreferences`azione.


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
```

```
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : Voce di registro per GenerateReport

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`GenerateReport`azione. Questa operazione crea un report per l'organizzazione AWS .


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
```

```
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Risorse per la risoluzione dei problemi

Per le risposte a domande comuni relative alla risoluzione dei problemi, consulta il Knowledge Center per AWS Support.

Per Windows, Amazon EC2 offre EC2Rescue, che i clienti possono utilizzare per esaminare le loro istanze di Windows per identificare i problemi più comuni, raccogliere file di registro e aiutare a AWS Support risolvere i problemi. Puoi anche utilizzare EC2Rescue per analizzare volumi di avvio di istanze non funzionali. Per ulteriori informazioni, consulta l'articolo su come utilizzare EC2Rescue per la risoluzione dei problemi più comuni relativi alla propria istanza EC2 Windows

Risoluzione dei problemi specifici dei servizi

La maggior parte Servizio AWS della documentazione contiene argomenti di risoluzione dei problemi che possono aiutarti a iniziare prima di contattare. AWS Support La tabella seguente fornisce i collegamenti agli argomenti per la risoluzione dei problemi ordinati in base ai servizi.

> **Note**
>
> La tabella seguente fornisce un elenco dei servizi più comuni. Per cercare altri argomenti per la risoluzione dei problemi, utilizza la casella di testo di ricerca nella Pagina iniziale della documentazione di AWS.

Servizio	Link
Amazon Web Services	Risoluzione degli errori relativi AWS alla versione 4 di Signature
Amazon API Gateway	Risoluzione dei problemi con le API HTTP
Amazon AppStream	Risolvi i problemi di Amazon AppStream
Amazon Athena	Risoluzione dei problemi in Athena
Amazon Aurora MySQL	Risoluzione dei problemi per Amazon Aurora
Amazon Aurora PostgreSQL	Soluzione dei problemi per Amazon Aurora

Servizio	Link
Dimensionamento automatico Amazon EC2	Risoluzione dei problemi di Auto Scaling
AWS Certificate Manager (ACM)	Risoluzione dei problemi
AWS CloudFormation	Risoluzione dei problemi di AWS CloudFormation
Amazon CloudFront	Risoluzione dei problemi | Risoluzione dei problemi delle distribuzioni RTMP
AWS CloudHSM	Risoluzione dei problemi
Amazon CloudSearch	Risoluzione dei problemi con Amazon CloudSearch
AWS CodeDeploy	Risoluzione dei problemi di AWS CodeDeploy
Amazon CloudWatch	Risoluzione dei problemi di
AWS Database Migration Service	Risoluzione dei problemi relativi alle attività di migrazione in AWS Database Migration Service
AWS Data Pipeline	Risoluzione dei problemi
AWS Direct Connect	Risoluzione dei problemi di AWS Direct Connect
AWS Directory Service	Risoluzione dei problemi di AWS Directory Service amministrazione
Amazon DynamoDB	Risoluzione dei problemi | Risoluzione dei problemi di creazione di una connessione SSL/TLS
AWS Elastic Beanstalk	Risoluzione dei problemi

Servizio	Link
Amazon Elastic Compute Cloud (Amazon EC2)	Risoluzione dei problemi delle istanze | Risoluzione dei problemi delle istanze Windows | Risoluzione dei problemi di VM Import/ Export | Risoluzione dei problemi di errori relativi a richieste API | Risoluzione dei problemi legati al pacchetto di gestione AWS | Risoluzione dei problemi AWS Systems Manager legati a Microsoft SCVMM | Diagnostica AWS per server Microsoft Windows
Amazon Elastic Container Service (Amazon ECS)	Risoluzione dei problemi legati ad Amazon ECS
Amazon Elastic Kubernetes Service (Amazon EKS)	Risoluzione dei problemi di Amazon EKS
Sistema di bilanciamento del carico elastico	Risoluzione dei problemi di Application Load Balancer | Risoluzione dei problemi di Classic Load Balancer
Amazon ElastiCache per Memcached	Risoluzione dei problemi delle applicazioni
Amazon ElastiCache per Redis	Risoluzione dei problemi delle applicazioni
Amazon EMR	Risoluzione dei problemi di un cluster
AWS Flow Framework	Suggerimenti per la risoluzione dei problemi e il debugging
AWS Glue	Risoluzione dei problemi AWS Glue
AWS Glue DataBrew	Risoluzione dei problemi di identità e accesso in AWS Glue DataBrew
AWS GovCloud (US)	Risoluzione dei problemi
AWS Identity and Access Management (IAM)	Risoluzione dei problemi di IAM

Servizio	Link
Amazon Keyspaces (per Apache Cassandra)	Risoluzione dei problemi di Amazon Keyspaces (per Apache Cassandra)
Flusso di dati Amazon Kinesis	Risoluzione dei problemi dei produttori di flussi di dati Amazon Kinesis | Risoluzione dei problemi degli utenti di flussi di dati Amazon Kinesis
Servizio gestito da Amazon per Apache Flink	Risoluzione dei problemi di prestazioni | Risoluzione dei problemi del Servizio gestito da Amazon per Apache Flink per applicazioni SQL
Amazon Data Firehose	Risoluzione dei problemi di Amazon Data Firehose
AWS Lambda	Risoluzione dei problemi e monitoraggio delle AWS Lambda funzioni con CloudWatch
OpenSearch Servizio Amazon	Risoluzione dei problemi con Amazon OpenSearch Service
AWS OpsWorks	Guida al debugging e alla risoluzione dei problemi
Amazon Personalize	Risoluzione dei problemi
Amazon QLDB	Risoluzione dei problemi di Amazon QLDB
Amazon QuickSight	Risoluzione dei problemi di Amazon QuickSight | Risoluzione degli errori relativi alle righe ignorate
AWS Resource Access Manager (AWS RAM)	Risoluzione dei problemi relativi a AWS RAM
Amazon Redshift	Risoluzione dei problemi di query | Risoluzione dei problemi dei carichi dati | Risoluzione dei problemi di connessione in Amazon Redshift | Risoluzione dei problemi di registrazione degli audit di Amazon Redshift | Risoluzione dei problemi delle query in Amazon Redshift Spectrum

Servizio	Link
Amazon Relational Database Service (Amazon RDS)	Risoluzione dei problemi | Risoluzione dei problemi delle applicazioni su Amazon RDS | Risoluzione dei problemi di database per Amazon RDS Custom
Amazon Route 53	Risoluzione dei problemi di Amazon Route 53
Amazon SageMaker	Risoluzione degli errori | Risoluzione dei problemi di Amazon Studio SageMaker
Amazon Silk	Risoluzione dei problemi
Amazon Simple Email Service (Amazon SES)	Risoluzione dei problemi di Amazon SES
Amazon Simple Storage Service (Amazon S3)	Risoluzione dei problemi
Amazon Simple Workflow Service (Amazon SWF)	AWS flow framework per Java: suggerimenti per la risoluzione dei problemi e il debug | AWS flow framework per Ruby: risoluzione dei problemi e debug dei flussi di lavoro
AWS Storage Gateway	Risoluzione dei problemi del gateway
AWS Systems Manager	Risoluzione dei problemi dell'agente SSM
Amazon Virtual Private Cloud (Amazon VPC) (Amazon VPC)	Risoluzione dei problemi
AWS Virtual Private Network (AWS VPN)	Risoluzione dei problemi del dispositivo gateway del cliente
AWS WAF	Test AWS WAF e ottimizzazione delle protezioni
Amazon WorkMail	Risoluzione dei problemi relativi all'applicazione WorkMail web Amazon
Amazon WorkSpaces	Risoluzione dei WorkSpaces problemi di Amazon | Risoluzione dei problemi dei WorkSpaces client Amazon

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione del AWS Support servizio.

- AWS Support Versione API: 15-04-2013
- AWS Support Versione dell'API dell'app: 2021-08-20

La tabella seguente descrive gli aggiornamenti importanti della AWS Trusted Advisor documentazione AWS Support e, a partire dal 10 maggio 2021. Puoi ora iscriverti a un feed RSS per ricevere notifiche sugli aggiornamenti.

Modifica	Descrizione	Data
Documentazione per AWSTrustedAdvisorServiceRolePolicy aggiornata	Sono state aggiunte nuove azioni IAM access-analyzer:ListAnalyzers cloudwatch:ListMetrics dax:DescribeClusters ec2:DescribeNatGateways ,ec2:DescribeRouteTables ,ec2:DescribeVpcEndpoints ,ec2:GetManagedPrefixListEntries ,elasticloadbalancing:DescribeTargetHealth ,iam:ListSAMLProviders ,, kafka:DescribeClusterV2 network-firewall:ListFirewalls network-f	11 giugno 2024

	`irewall:DescribeFirewall` e `sqs:GetQueueAttributes` nuovi controlli integrati. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSTrustedAdvisorServiceRolePolicy.	
Documentazione aggiunta per Recommendations AWS Support	Documentazione aggiunta per AWS Support Recommendations.	22 maggio 2024
Sono stati rimossi 5 AWS Trusted Advisor assegni dalla documentazione	Sono stati rimossi 5 AWS Trusted Advisor controlli che ora sono obsoleti. Per ulteriori informazioni, consulta Registro delle modifiche per i controlli. AWS Trusted Advisor	15 maggio 2024
Aggiunto 1 nuovo controllo AWS Trusted Advisor di sicurezza alla documentazione	Aggiunto 1 nuovo controllo AWS Trusted Advisor di sicurezza alla documentazione. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli.	15 maggio 2024
Sono stati rimossi 3 controlli di tolleranza agli errori dalla documentazione	Sono stati rimossi 3 controlli di tolleranza agli errori che ora sono obsoleti. Per ulteriori informazioni, consulta Registro delle modifiche per i controlli. AWS Trusted Advisor	25 aprile 2024

Documentazione aggiornata sulla tolleranza agli errori e sul controllo di sicurezza	Aggiunto 1 nuovo controllo della tolleranza ai guasti. Aggiornati 1 controllo di tolleranza agli errori e 1 controllo di sicurezza. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli.	29 marzo 2024
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	22 marzo 2024
Documentazione aggiornata per il piano AWS Support	Aggiornamenti alle funzionalità dei AWS Support piani. Per ulteriori informazioni, consulta AWS Support i piani.	11 marzo 2024
Documentazione aggiornata per Trusted Advisor	Aggiunto 1 controllo della tolleranza ai guasti. Per ulteriori informazioni, vedere Registro delle modifiche per AWS Trusted Advisor i controlli.	29 febbraio 2024

Documentazione aggiornata per Trusted Advisor	Aggiunto 1 controllo della tolleranza ai guasti. Per ulteriori informazioni, vedere Registro delle modifiche per AWS Trusted Advisor i controlli.	31 gennaio 2024
Documentazione per `AWSTrustedAdvisorServiceRolePolicy` aggiornata	Sono state aggiunte nuove azioni IAM `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` ,`outposts:GetOutpost` ,, `outposts:ListAssets` e `outposts:ListOutposts` nuovi controlli integrati . Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSTrustedAdvisorServiceRolePolicy.	18 gennaio 2024
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	17 gennaio 2024

Documentazione aggiornata per Trusted Advisor	Aggiornamento di 1 controllo di tolleranza ai guasti per modificare titolo e descrizione. Per ulteriori informazioni, vedere Registro delle modifiche per i AWS Trusted Advisor controlli.	8 gennaio 2024
Documentazione aggiornata per Trusted Advisor	È stato aggiornato 1 controllo di sicurezza per riflettere la modifica del periodo di deprecazione. Per ulteriori informazioni, consulta Registro delle modifiche per i controlli. AWS Trusted Advisor	21 dicembre 2023
Documentazione aggiornata per Trusted Advisor	Aggiunti 2 controlli di sicurezza e 2 controlli delle prestazioni. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli.	20 dicembre 2023
Documentazione aggiornata per Trusted Advisor	Aggiunto 1 controllo di sicurezza. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli.	15 dicembre 2023
Documentazione aggiornata per Trusted Advisor Engage	Documentazione Trusted Advisor Engage aggiornata con modifiche all'opzione di notifica via e-mail.	14 dicembre 2023

Documentazione aggiornata per Trusted Advisor Engage	Documentazione Trusted Advisor Engage aggiornata con modifiche agli impegni pianificati.	11 dicembre 2023
Documentazione aggiornata per Trusted Advisor	Aggiunti 2 nuovi controlli di tolleranza ai guasti e 1 controllo di ottimizzazione dei costi. Per ulteriori informazioni, vedere Registro delle modifiche per AWS Trusted Advisor i controlli.	7 dicembre 2023
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	6 dicembre 2023
Politiche AWS gestite aggiornate per Trusted Advisor	Le politiche `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS sono `AWSTrustedAdvisorPriorityFullAccess` state aggiornate e gestite per includere gli ID delle dichiarazioni. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Trusted Advisor.	6 dicembre 2023

Documentazione aggiornata per Trusted Advisor	Aggiunti 3 nuovi controlli di tolleranza ai guasti. Per ulteriori informazioni, vedere Registro delle modifiche per AWS Trusted Advisor i controlli.	17 novembre 2023
Documentazione aggiornata per Trusted Advisor	Aggiunti 37 nuovi controlli per Amazon RDS. Per ulteriori informazioni, consulta Change log for AWS Trusted Advisor checks.	15 novembre 2023
Documentazione per `AWSTrustedAdvisorServiceRolePolicy` aggiornata	Sono state aggiunte nuove azioni `ec2:DescribeRegions` IAM `ecs:DescribeTaskDefinition` e `ecs:ListTaskDefinitions` nuovi controlli integrati. `s3:GetLifecycleConfiguration` Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSTrustedAdvisorServiceRolePolicy.	9 novembre 2023
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	27 ottobre 2023

Documentazione aggiornata per Trusted Advisor	Aggiunti 64 nuovi controlli integrati da AWS Config. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli.	26 ottobre 2023
Documentazione aggiornata per Trusted Advisor	Sono stati aggiunti sei nuovi controlli di tolleranza ai guasti Trusted Advisor. Per ulteriori informazioni, consulta il registro delle modifiche per AWS Trusted Advisor i controlli.	12 ottobre 2023
Documentazione per `AWSTrustedAdvisorServiceRolePolicy` aggiornata	Sono state aggiunte nuove azioni IAM `route53resolver:ListResolverEndpoints`, `route53resolver:ListResolverEndpointIpAddresses`, `ec2:DescribeSubnets`, `kafka:ListClustersV2` e `kafka:ListNodes` per introdurre nuovi controlli di resilienza. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSTrustedAdvisorServiceRolePolicy.	14 settembre 2023

Documentazione per AWSSupportServiceRolePolicy aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	28 agosto 2023
Documentazione aggiornata per Trusted Advisor	Aggiunto 1 nuovo controllo dei limiti di servizio per AWS Lambda. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	17 agosto 2023
Documentazione aggiornata per Trusted Advisor	È stato aggiunto un nuovo controllo di tolleranza degli errori per Lambda. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	3 agosto 2023
Documentazione aggiornata per Trusted Advisor Engage	È stato aggiornata la Documentazione Trusted Advisor Engage con modifiche ai moduli per la creazione e la modifica degli impegni. È stata aggiunta una pagina con esempi di policy di controllo dei servizi per AWS Trusted Advisor.	27 luglio 2023

Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	26 giugno 2023
Documentazione aggiornata per Trusted Advisor	Sono stati aggiunti due nuovi controlli di tolleranza agli errori per Amazon MQ. È stato aggiunto un nuovo controllo di tolleranza agli errori e un nuovo controllo delle prestazioni per il file system di Amazon Elastic. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	1 giugno 2023
Documentazione aggiornata per Trusted Advisor	Sono stati aggiunti due nuovi controlli di tolleranza agli errori per il gateway NAT. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	16 maggio 2023

Documentazione aggiornata per AWS Support i piani	Aggiunta una nuova autorizzazione e CloudTrail documentazione per la creazione di pianificazioni dei piani di supporto. Per ulteriori informazioni, consulta Gestire l'accesso ai AWS Support piani, politiche AWS gestite per AWS Support i piani e Registrazione delle AWS Support chiamate API con AWS CloudTrail.	8 maggio 2023
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	2 maggio 2023
Documentazione aggiornata per Trusted Advisor Engage and Priority Trusted Advisor	Prerequisiti chiariti per Trusted Advisor Engage e Trusted Advisor Priority. È stato aggiunto un esempio di policy IAM con la possibilità di utilizzare Trusted Advisor Engage e consentire un accesso affidabile a Trusted Advisor.	28 aprile 2023

Documentazione aggiornata per Trusted Advisor	Sono stati aggiunti due nuovi controlli di tolleranza agli errori per AWS Resilience Hub Incident Manager. Per ulteriori informazioni, consulta il registro delle modifiche per AWS Trusted Advisor i controlli.	27 aprile 2023
Documentazione aggiunta per Trusted Advisor Engage	Puoi utilizzare AWS Trusted Advisor Engage per ottenere il massimo dai tuoi AWS Support piani semplificando la visualizzazione, la richiesta e il monitoraggio di tutti i tuoi impegni proattivi e la comunicazione con il tuo Account AWS team in merito agli impegni continui. Per ulteriori informazioni, consulta Nozioni di base su AWS Trusted Advisor Engage.	6 aprile 2023
Documentazione aggiornata per Trusted Advisor	Sono stati aggiunti due nuovi controlli di tolleranza agli errori per Amazon ECS. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	30 marzo 2023

Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	16 marzo 2023
Documentazione aggiunta per Trusted Advisor Priority	È stata aggiornata la console Trusted Advisor Priority: • I pulsanti Riconosci e Ignora hanno sostituito i pulsanti Accetta e Rifiuta. • Non è necessario inserire il titolo o il nome del processo per riconoscere, risolvere , ignorare o riaprire i suggerimenti. Per ulteriori informazioni, vedi Guida introduttiva a Trusted Advisor Priority.	16 febbraio 2023
Esempi di codice aggiornati per AWS Support	Sono stati aggiunti esempi di codice.NET, Java e Kotlin che mostrano come utilizzarli AWS Support con un kit di sviluppo AWS software (SDK). Per ulteriori informazioni, consulta Esempi di codice per AWS Support l'utilizzo degli SDK. AWS	16 gennaio 2023

Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	10 gennaio 2023
Documentazione aggiornata per l'app AWS Support	Puoi effettuare la ricerca dei casi di supporto in Slack utilizzando le opzioni di filtro o in base all'ID del caso. Per ulteriori informazioni, consulta la sezione Ricerca di casi di supporto in Slack.	29 dicembre 2022
Documentazione aggiornata per AWS Support l'app	Puoi anche usare Terraform per creare le tue risorse per l' AWS Support App. Per ulteriori informazioni, consulta Creare risorse per AWS Support l'app utilizzando Terraform.	22 dicembre 2022
Documentazione aggiornata per Trusted Advisor	Aggiunti tre nuovi controlli di tolleranza agli errori per Amazon MemoryDB ElastiCache, Amazon e. AWS CloudHSM Per ulteriori informazioni, consulta il registro delle modifiche per i AWS Trusted Advisor controlli.	15 dicembre 2022

Documentazione aggiornata per l' AWS Support app in Slack	Ora puoi richiedere l'assistenza tramite chat dal vivo per le seguenti opzioni: • Casi di supporto per account e fatturazione. • Supporto in lingua giapponese per casi di supporto tecnico. • Per ulteriori informazioni, consulta la sezione Creazione di casi di supporto in un canale Slack.	14 dicembre 2022
Documentazione aggiornata per AWS Support	È stata aggiunta la documentazione sui nuovi endpoint per l' AWS Support API. Per ulteriori informazioni, consulta Informazioni sull'API AWS Support.	14 dicembre 2022
È stata aggiunta la documentazione per AWS CloudFormation i modelli da utilizzare per l' AWS Support app in Slack	Puoi utilizzare i CloudFormation modelli per creare aree di lavoro e canali di configurazione Slack per in. Account AWS AWS Organizations Per ulteriori informazioni, consulta Creazione di risorse AWS Support per app con. AWS CloudFormation	5 dicembre 2022

Documentazione aggiornata per Trusted Advisor	Aggiunti due nuovi controlli di tolleranza ai guasti per AWS Resilience Hub. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	17 novembre 2022
È stata aggiunta la documentazione relativa ai AWS Security Hub risultati in Trusted Advisor	I risultati dei controlli del Security Hub vengono rimossi Trusted Advisor più rapidamente. Per ulteriori informazioni, consulta il registro delle modifiche per AWS Trusted Advisor i controlli.	17 novembre 2022
Documentazione aggiornata per AWS Trusted Advisor	Documentazione aggiunta per Trusted Advisor Recommendations. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	16 novembre 2022
Documentazione aggiornata per l' AWS Support app in Slack	È stata aggiunta la documentazione per il supporto della lingua giapponese. Per ulteriori informazioni, consulta la sezione Creazione di casi di supporto in un canale Slack.	11 novembre 2022
Documentazione aggiornata per i piani AWS Support	Sono state aggiunte informazioni sulla risoluzione dei problemi per consentire l'accesso ai piani di supporto in un'organizzazione. Per ulteriori informazioni, consulta Risoluzione dei problemi.	9 novembre 2022

Documentazione aggiornata per l' AWS Support app in Slack	È stata aggiunta la documentazione per le autorizzazioni `supportapp` . Per ulteriori informazioni, consulta Autorizzazioni necessarie per la connessione dell' AWS Support app a Slack.	1 novembre 2022
Documentazione aggiornata per l' AWS Support app in Slack	Puoi utilizzare l'operazione API `RegisterSlackWorkspaceForOrganization` per registrare uno spazio di lavoro Slack per il tuo Account AWS. Per chiamare questa API, il tuo account deve far parte di un'organizzazione in AWS Organizations. Per ulteriori informazioni, consulta la Documentazione di riferimento sull'API dell'App AWS Support in Slack.	19 ottobre 2022
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	4 ottobre 2022

Documentazione sui piani di supporto aggiornata	Ora puoi utilizzare AWS Identity and Access Management (IAM) per gestire le autorizzazioni per modificare il piano di supporto per il tuo Account AWS. Per ulteriori informazioni, consulta i seguenti argomenti: • Gestione dell'accesso per i piani AWS Support • AWS politiche gestite per AWS Support Plans • Modifica AWS Support dei piani • Registrazione delle chiamate all'API AWS Support Plans con AWS CloudTrail	29 settembre 2022
Documentazione aggiornata per l' AWS Support app in Slack	È stata aggiunta documentazione su come configurare un canale pubblico o privato da utilizzare con l' AWS Support app. Per ulteriori informazioni, consulta la pagina Configuring a Slack channel (Configurazione di un canale Slack).	22 settembre 2022
Documentazione aggiornata per AWS Support	È stata aggiunta una nuova sezione sulla sicurezza per i casi di supporto. Per ulteriori informazioni, consulta Sicurezza per i tuoi AWS Support casi.	9 settembre 2022

Documentazione aggiornata per Trusted Advisor	È stato aggiunto un nuovo controllo di sicurezza di Amazon EC2. Per ulteriori informazioni, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli.	1 settembre 2022
Documentazione aggiornata per l' AWS Support app in Slack	Vedi gli argomenti seguenti: Puoi utilizzare l' AWS Support App per gestire i casi di assistenza, richiedere aumenti delle quote di servizio e chattare con gli agenti dell'assistenza direttamente nei tuoi canali Slack. Per ulteriori informazioni, consulta la sezione App AWS Support nella documentazione di Slack. Puoi allegare policy AWS gestite ai tuoi ruoli IAM per utilizzare l' AWS Support App. Per ulteriori informazioni, consulta le politiche AWS gestite per AWS Support l'app in Slack. Nuovo riferimento API per l' AWS Support app. Consulta la documentazione di riferimento sull'API dell'app AWS Support.	24 agosto 2022

Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	17 agosto 2022
Documentazione aggiunta per Trusted Advisor Priority	Trusted Advisor Priority aggiunge il supporto per le seguenti funzionalità: • Amministratori delegati • Notifiche e-mail giornaliere e settimanali con riepiloghi dei suggerimenti • Possibilità di riaprire i suggerimenti risolti o rifiutati • AWS politiche gestite Per ulteriori informazioni, consulta Guida introduttiva a Trusted Advisor Priority.	17 agosto 2022
Documentazione aggiornata per Trusted Advisor	La pagina Preferenze nella Trusted Advisor console è stata aggiornata. Per ulteriori informazioni, consulta Guida introduttiva AWS Trusted Advisor.	15 luglio 2022

Documentazione aggiornata per Trusted Advisor	Sono stati aggiornati i controlli per includere le seguenti informazioni: • Criteri di avviso • Operazione consigliata • Risorse aggiuntive • Colonne del report Per ulteriori informazioni, consulta il riferimento dei controlli AWS Trusted Advisor.	7 luglio 2022
Documentazione aggiornata per AWS Support	Documentazione aggiunta che spiega come gestire i casi di supporto. • Aggiornamento di un caso di supporto esistente • Risoluzione dei problemi	28 giugno 2022
Documentazione per `AWSSupportServiceRolePolicy` aggiornata	Aggiornate autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	23 giugno 2022

Documentazione aggiornata per Trusted Advisor	Trusted Advisor supporta controlli standard di sicurezza aggiuntivi di AWS Foundatio nal Security Best Practices provenienti da. AWS Security Hub Per ulteriori informazi oni, consulta il Registro delle modifiche per i AWS Trusted Advisor controlli.	23 giugno 2022
Documentazione aggiornata per Trusted Advisor	Aggiunte informazioni su come richiedere aumenti delle quote di servizio. Per ulteriori informazioni, consulta Limiti del servizio.	21 giugno 2022
Documentazione aggiornata per AWS Support	L'esperienza di creazione dei casi è stata aggiornata nella console del Centro Support. Per ulteriori informazioni, consulta Creazione di casi di supporto e gestione dei casi.	18 maggio 2022
Documentazione aggiornata per Trusted Advisor	Aggiunti quattro controlli per Amazon EBS e AWS Lambda. Per ulteriori informazi oni, consulta Attivare AWS Compute Optimizer l'aggiunta di Trusted Advisor controlli.	4 maggio 2022

Documentazione per AWSSupportServiceRolePolicy aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	27 aprile 2022
Documentazione aggiornata per il controllo Exposed Access Keys	Questo controllo viene ora aggiornato automaticamente per te. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli.	25 aprile 2022
Documentazione aggiornata per Trusted Advisor	I AWS Direct Connect controlli nella categoria di tolleranza ai guasti vengono aggiornati. Per ulteriori informazioni, vedere Registro delle modifiche per AWS Trusted Advisor i controlli.	29 marzo 2022
Documentazione per AWSSupportServiceRolePolicy aggiornata	Aggiunte nuove autorizzazioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSupportServiceRolePolicy.	14 marzo 2022

Documentazione aggiunta per Trusted Advisor Priority	Puoi utilizzare Trusted Advisor Priority per visualizzare un elenco di consigli prioritar i forniti dal tuo Technical Account Manager (TAM). Per ulteriori informazioni, consulta Guida introduttiva a Priority. Trusted Advisor	28 febbraio 2022
Documentazione aggiornat a per l'utilizzo di Amazon EventBridge per Trusted Advisor	Puoi creare una EventBrid ge regola per monitorare le modifiche ai tuoi Trusted Advisor assegni. Per ulteriori informazioni, consulta Monitoraggio dei risultati dei AWS Trusted Advisor controlli con EventBridge.	21 febbraio 2022
Nuova documentazione per l'utilizzo di Amazon EventBrid ge per monitorare AWS Support i casi	Puoi creare una EventBrid ge regola per monitorar e e ricevere notifiche sui tuoi casi di assistenza. Per ulteriori informazioni, consulta Monitoraggio AWS Support dei casi con EventBridge.	21 febbraio 2022
Documentazione per `AWSSupportServiceR olePolicy` aggiornata	Aggiunte nuove autorizza zioni per offrire servizi di fatturazione, amministrativi e di supporto per il ruolo collegato ai servizi. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite da AWS : AWSSuppor tServiceRolePolicy.	17 febbraio 2022

Documentazione aggiunta per l'integrazione con AWS Security Hub	Nella Trusted Advisor console, ora puoi visualizzare i risultati dei controlli del Security Hub che fanno parte dello standard di sicurezza AWS Foundatio nal Security Best Practices . Per ulteriori informazioni, consulta Visualizzazione AWS Security Hub dei controlli nella AWS Trusted Advisor console.	18 gennaio 2022
Documentazione aggiornata per Trusted Advisor	Sono stati aggiunti tre nuovi controlli per le istanze Amazon EC2 che eseguono Microsoft SQL Server. • Consolidamento di istanze Amazon EC2 per Microsoft SQL Server • Istanze Amazon EC2 con provisioning eccessivo per Microsoft SQL Server • Fine del supporto per le istanze Amazon EC2 con Microsoft SQL Server Per ulteriori informazioni, consulta il riferimento dei controlli AWS Trusted Advisor.	20 dicembre 2021

Documentazione aggiornata per Trusted Advisor	Trusted Advisor ha aggiunto quattro nuovi controlli per AWS Well-Architected • Problemi ad alto rischio di AWS Well-Architected per l'ottimizzazione dei costi • Problemi ad alto rischio di AWS Well-Architected per le prestazioni • Problemi ad alto rischio di AWS Well-Architected per la sicurezza • Problemi ad alto rischio di AWS Well-Architected per l'affidabilità Per ulteriori informazioni, consulta il riferimento dei controlli AWS Trusted Advisor.	20 dicembre 2021
Documentazione aggiornata	Se disponi di un piano Enterprise On-Ramp Support, hai accesso a tutti i Trusted Advisor controlli e all' AWS Support API.	24 novembre 2021
Documentazione aggiornata per Trusted Advisor	Trusted Advisor ha aggiunto due nuovi controlli per Amazon Comprehend. Per ulteriori informazioni, consulta il riferimento dei controlli AWS Trusted Advisor.	29 settembre 2021

Documentazione aggiornata per Trusted Advisor	Il nome del controllo per Amazon OpenSearch Service Reserved Instance Optimization è stato aggiornato. Per ulteriori informazioni, consulta Change log for AWS Trusted Advisor checks.	8 settembre 2021
Documentazione aggiornata per i Trusted Advisor controlli	È stato aggiunto un argomento di riferimento per tutti i Trusted Advisor controlli. Per ulteriori informazioni, consulta la documentazione di riferimento ai controlli AWS Trusted Advisor.	1 settembre 2021
Documentazione aggiornata per le politiche Trusted Advisor gestite	Documentazione aggiornata per le politiche Trusted Advisor gestite. Per ulteriori informazioni, consulta le politiche AWS gestite per AWS Support e AWS Trusted Advisor.	10 agosto 2021
Documentazione aggiornata per Trusted Advisor	Documentazione aggiornata per la Trusted Advisor console. Per ulteriori informazioni, consulta la Guida introduttiva a AWS Trusted Advisor.	16 luglio 2021
Documentazione aggiornata per la creazione di AWS Support casi	Aggiunta documentazione su come creare un caso di supporto correlato per i casi chiusi in modo permanente. Per ulteriori informazioni, consulta la sezione Riapertura di un caso chiuso e Creazione di un caso correlato.	8 giugno 2021

Documentazione aggiornata per Trusted Advisor	Trusted Advisor sono stati aggiunti due nuovi controlli per lo storage di volumi Amazon Elastic Block Store (Amazon EBS). Per ulteriori informazioni, consulta Change log for AWS Trusted Advisor checks.	8 giugno 2021
Documentazione aggiornata	I seguenti argomenti sono stati aggiornati: • Procedure aggiornate e contenuti aggiunti all'argomento Creazione di CloudWatch allarmi Amazon per monitorare le AWS Trusted Advisor metriche • Aggiunta la sezione Quote di servizio per la sezione API AWS Support	12 maggio 2021

Aggiornamenti precedenti

Modifica	Descrizione	Data
Documentazione aggiornata per Trusted Advisor	Aggiunta documentazione per filtrare, aggiornare e scaricare i risultati del controllo. Per ulteriori informazioni, consulta le sezioni seguenti: • Filtra i controlli • Aggiorna i risultati di controllo • Scarica i risultati del controllo	16 marzo 2021
Documentazione aggiornata sulle politiche AWS gestite	Sono state aggiunte informazioni sulla politica `AWSSupportServiceRolePolicy` AWS gestita. Per ulteriori informazioni, consulta	16 marzo 2021

Modifica	Descrizione	Data
	Utilizzo di ruoli collegati ai servizi per AWS Support.	
Sono stati aggiunti controlli per AWS Lambda	Sono stati aggiunti quattro AWS Trusted Advisor controlli per Lambda in. Registro delle modifiche per AWS Trusted Advisor	8 marzo 2021
Controlli dei limiti del servizio aggiornati per Amazon Elastic Block Store	Sono stati aggiornati cinque AWS Trusted Advisor controlli per Amazon EBS in. Registro delle modifiche per AWS Trusted Advisor	5 marzo 2021
Documentazione aggiornata per la registrazione CloudTrail	CloudTrail supporta la registrazione delle azioni della console quando si modifica il AWS Support piano. Per ulteriori informazioni, consulta Registrazione di log per le modifiche al piano AWS Support.	9 febbraio 2021
Documentazione aggiornata per Trusted Advisor	Aggiornato l'argomento Come iniziare con Consigli per Trusted Advisor.	29 gennaio 2021
Documentazione aggiornata per i Trusted Advisor report	È stata aggiunta una Risoluzione dei problemi sezione per l'utilizzo Trusted Advisor dei report con altri AWS servizi.	4 dicembre 2020
È stato aggiunto AWS Trusted Advisor il supporto per la AWS CloudTrail registrazione	CloudTrail supporta la registrazione per un sottoinsieme di azioni della Trusted Advisor console. Per ulteriori informazioni, consulta Registrazione delle azioni AWS Trusted Advisor della console con AWS CloudTrail.	23 novembre 2020
Aggiunto un argomento del log delle modifiche	Visualizza le modifiche ai AWS Trusted Advisor controlli e alle categorie in. Registro delle modifiche per AWS Trusted Advisor	18 novembre 2020

Modifica	Descrizione	Data
Aggiunto il supporto per le unità organizzative	È ora possibile creare report per i Trusted Advisor controlli delle unità organizzative (OU). Per ulteriori informazioni, consulta Creazione di report di visualizzazione organizzativa.	17 novembre 2020
È stata aggiornata la registrazione con argomento AWS CloudTrail	È stata aggiunta una voce di registro di esempio per un'operazione Trusted Advisor API. Per informazioni, consulta Informazioni di AWS Trusted Advisor nella registrazione di CloudTrail.	22 ottobre 2020
AWS Support Quote aggiunte	Informazioni aggiunte sulle quote e le restrizioni correnti per AWS Support. Consulta la sezione Endpoint e quote AWS Support nella Riferimenti generali di AWS.	4 agosto 2020
Visualizzazione organizzativa per AWS Trusted Advisor	È ora possibile creare report per i Trusted Advisor controlli relativi agli account di cui fanno parte AWS Organizations. Per informazioni, consulta Visualizzazione organizzativa per AWS Trusted Advisor.	17 luglio 2020
Sicurezza e AWS Support	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di AWS Support e Trusted Advisor. Consulta Sicurezza in AWS Support	5 maggio 2020
Sicurezza e AWS Support	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di AWS Support.	10 gennaio 2020
Utilizzo Trusted Advisor come servizio web	Sono state aggiunte istruzioni aggiornate per aggiornare Trusted Advisor i dati dopo aver ottenuto l'elenco dei Trusted Advisor controlli.	1 novembre 2018
Utilizzo di ruoli collegati ai servizi	Aggiunta una nuova sezione.	11 luglio 2018

Modifica	Descrizione	Data
Nozioni di base sulla risoluzione dei problemi	Aggiunti link per la risoluzione dei problemi di Route 53 e AWS Certificate Manager.	1 settembre 2017
Esempio di gestione di casi: creazione di un caso	Aggiunta una nota relativa alla casella CC per gli utenti che hanno sottoscritto il piano di supporto Base.	1 agosto 2017
Monitoraggio dei risultati dei Trusted Advisor controlli con eventi CloudWatch	Aggiunta una nuova sezione.	18 novembre 2016
Gestione dei casi	Aggiornati i nomi dei livelli di gravità dei casi.	27 ottobre 2016
Registrazione delle AWS Support chiamate con AWS CloudTrail	Aggiunta una nuova sezione.	21 aprile 2016
Nozioni di base sulla risoluzione dei problemi	Aggiunti altri link alla risoluzione dei problemi.	19 maggio 2015
Nozioni di base sulla risoluzione dei problemi	Aggiunti altri link alla risoluzione dei problemi.	18 novembre 2014
Nozioni di base: gestione dei casi	Aggiornato per riflettere il Service Catalog nella AWS Management Console.	30 ottobre 2014
Programmare la durata di un caso AWS Support	Aggiunte informazioni sui nuovi elementi dell'API per aggiungere allegati ai casi e per omettere comunicazioni durante il recupero della cronologia dei casi.	16 luglio 2014

Modifica	Descrizione	Data
Accedendo AWS Support	Rimossi contatti di supporto designati come metodo di accesso.	28 maggio 2014
Nozioni di base	Aggiunta la sezione Nozioni di base.	13 dicembre 2013
Pubblicazione iniziale	Rilasciato AWS Support un nuovo servizio.	30 aprile 2013

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.