



Guida per l'utente

Supporto AWS



Versione API 2026-04-14

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

Supporto AWS: Guida per l'utente

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

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

Table of Contents

Inizia con Supporto AWS	1
Risoluzione dei problemi potenziata dall'intelligenza artificiale nella console di Support Center	2
Configura le autorizzazioni per utilizzare la risoluzione dei problemi basata sull'intelligenza artificiale	5
Crea un'interazione di supporto	8
Crea una richiesta di supporto da un'interazione di supporto	11
Visualizza le interazioni di supporto	16
Risoluzione dei problemi	16
Riunioni virtuali con Supporto AWS	17
Partecipa a una riunione virtuale	18
Sicurezza e privacy durante la riunione virtuale	18
Autorizzazioni IAM richieste per le riunioni virtuali	19
Risoluzione dei problemi relativi alle riunioni virtuali	19
Gestione dei casi	20
Descrizione del problema	21
Scelta di un livello di gravità iniziale	21
Comprensione dei Supporto AWS tempi di risposta	23
Modifica del livello di gravità di un caso di assistenza	25
Richiedi un aumento della quota di servizio.	27
Metodo legacy: creazione di casi di supporto e gestione dei casi	29
Creazione di un caso di supporto	30
Descrizione del problema	33
Scelta di un livello di gravità iniziale	33
Comprendere Supporto AWS i tempi di risposta	35
Modifica del livello di gravità di un caso di assistenza	36
Esempio: crea un caso di supporto per account e fatturazione	39
Esperienza precedente: aggiorna, risolvi e riapri i casi	44
Lavorare con AWS SDKs	50
Informazioni sull'API della console Support Center	52
Aggiungere policy IAM per le operazioni dell'API Support Center Console	52
Test delle chiamate API della console del Support Center	55
Informazioni sull' Supporto AWS API	57
Gestione dei casi di supporto	58

AWS Trusted Advisor	59
Endpoints	59
Support in AWS SDKs	60
Supporto AWS Piani	61
Caratteristiche dei piani Supporto AWS	62
Che cosa sono le operazioni unificate AWS	64
AWS Prezzi di Unified Operations	64
Vantaggi delle operazioni unificate	65
Team operativo unificato	66
Ciclo di vita delle operazioni unificate	68
Guida introduttiva a Unified Operations	71
Piani di modifica Supporto AWS	78
Informazioni correlate	80
Configura le notifiche di scadenza del piano promozionale	80
Visualizza le notifiche relative al piano promozionale	81
Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise	81
Fine del supporto Supporto per il piano di sviluppo	82
Fine Supporto del supporto per il piano aziendale	82
Fine del supporto per Enterprise On-Ramp	82
AWS Trusted Advisor	83
Inizia a usare i Trusted Advisor consigli	85
Accedi alla Trusted Advisor console	86
Visualizza le categorie di controllo	87
Visualizza controlli specifici	89
Filtra i controlli	90
Aggiorna i risultati di controllo	92
Scarica i risultati del controllo	93
Visualizzazione organizzativa	93
Preferenze	93
Inizia a usare l' Trusted Advisor API	95
Utilizzo Trusted Advisor come servizio web	97
Visualizza l'elenco dei controlli disponibili Trusted Advisor	97
Aggiorna l'elenco dei controlli disponibili Trusted Advisor	98
Esegui un Trusted Advisor sondaggio per verificare le modifiche allo stato	98
Richiedi il risultato di un Trusted Advisor controllo	101
Mostra i dettagli di un controllo Trusted Advisor	102

Visualizzazione organizzativa per AWS Trusted Advisor	102
Prerequisiti	103
Abilita visualizzazione organizzativa	104
Aggiorna Trusted Advisor i controlli	105
Creazione di report di visualizzazione organizzativa	106
Esamina il riepilogo del report	110
Scarica un report della visualizzazione organizzativa	111
Disattiva visualizzazione organizzativa	116
Utilizzo delle policy IAM per consentire l'accesso alla visualizzazione organizzativa	118
Utilizzo di altri AWS servizi per visualizzare Trusted Advisor i report	121
Visualizza Trusted Advisor i controlli forniti da AWS Config	131
risoluzione dei problemi	132
Visualizza i controlli CSPM del Security Hub in Trusted Advisor	133
Prerequisiti	134
Visualizza i risultati del Security Hub CSPM	135
Aggiorna i risultati del Security Hub CSPM	137
Disattiva Security Hub CSPM da Trusted Advisor	138
Risoluzione dei problemi	138
Attiva AWS Compute Optimizer i Trusted Advisor controlli	142
Informazioni correlate	143
Inizia a usare AWS Trusted Advisor Priority	143
Prerequisiti	145
Abilita Trusted Advisor la priorità	145
Visualizzare i suggerimenti prioritari	145
Riconoscimento di un suggerimento	148
Ignorare un suggerimento	151
Risolvere un suggerimento	153
Riapertura di un suggerimento	154
Scarica i dettagli sul suggerimento	156
Registrazione degli amministratori delegati	157
Annullamento della registrazione di amministratori delegati	158
Gestisci le notifiche Trusted Advisor prioritarie	158
Disattiva Trusted Advisor la priorità	159
Trusted Advisor controlla il riferimento	160
Ottimizzazione dei costi	161
Performance	224

Sicurezza	276
Tolleranza ai guasti	326
Limiti del servizio	446
Eccellenza operativa	467
Registro delle modifiche per AWS Trusted Advisor	512
Aggiornamenti precedenti	519
Nuovo controllo: Amazon RDS Continuous Backup non abilitato	520
Nuovo controllo: registrazione AWS CloudTrail degli eventi di gestione	520
Aggiornato il controllo Auto Scaling Group Resources	521
È stato aggiornato il controllo degli accessi esterni di IAM Access Analyzer	521
Aggiunto 1 nuovo controllo	521
3 controlli aggiornati	522
Aggiunti 4 controlli	522
3 controlli aggiornati	522
Aggiunti 9 nuovi controlli	522
Aggiornato 1 controllo di sicurezza e aggiunto 1 controllo di sicurezza	523
6 controlli di sicurezza aggiornati	523
1 controllo di tolleranza ai guasti aggiornato	523
9 controlli aggiornati	524
Rimossi 5 controlli e aggiunto 1 controllo	524
Controlli di tolleranza agli errori rimossi	525
Nuovi controlli di tolleranza agli errori	525
Tolleranza agli errori e controlli di sicurezza aggiornati	525
Nuovi controlli di tolleranza agli errori	525
Controllo aggiornato della tolleranza agli errori	526
Controllo di sicurezza aggiornato	526
Nuovi controlli di sicurezza e prestazioni	526
Nuovo controllo di sicurezza	526
Nuovi controlli di tolleranza agli errori e ottimizzazione dei costi	527
Nuovi controlli di tolleranza ai guasti	527
Nuovi controlli per Amazon RDS	527
Nuova API AWS Trusted Advisor	527
Trusted Advisor controlla la rimozione	528
Integrazione dei AWS Config controlli in Trusted Advisor	528
Nuovi controlli di tolleranza ai guasti	528
Nuova verifica dei limiti del servizio	529

Nuovi controlli di tolleranza agli errori	529
Nuovi controlli di prestazioni e di tolleranza agli errori	529
Nuovi controlli di tolleranza ai guasti	529
Nuovi controlli di tolleranza ai guasti	530
Espansione regionale dei controlli di tolleranza agli errori di Amazon ECS	530
Nuovi controlli di tolleranza ai guasti	530
Nuovi controlli di tolleranza ai guasti	526
Aggiornamenti all'integrazione con Trusted Advisor AWS Security Hub CSPM	531
Nuovi controlli di tolleranza ai guasti per AWS Resilience Hub	527
Aggiornamento alla console Trusted Advisor	532
Nuovi controlli per Amazon EC2	532
Aggiunti i controlli CSPM di Security Hub a Trusted Advisor	533
Sono stati aggiunti controlli da AWS Compute Optimizer	533
Aggiornamenti al controllo Exposed Access Keys	533
Controlli aggiornati per AWS Direct Connect	534
AWS Security Hub CSPM controlli aggiunti alla AWS Trusted Advisor console	535
Nuovi controlli per Amazon EC2 e Well-Architected AWS	536
Nome di controllo aggiornato per Amazon OpenSearch Service	536
Sono stati aggiunti controlli per l'archiviazione del volume Amazon Elastic Block Store	537
Sono stati aggiunti controlli per AWS Lambda	537
Trusted Advisor controlla la rimozione	538
Controlli aggiornati per Amazon Elastic Block Store	538
Trusted Advisor controlla la rimozione	539
Trusted Advisor verifica la rimozione	540
Supporto AWS App in Slack	541
Prerequisiti	542
Gestisci l'accesso al widget Supporto AWS dell'app	542
Gestisci l'accesso all' Supporto AWS app	544
Autorizzazione di un workspace Slack	550
Autorizzazione di più account	553
Configura un canale Slack	554
Aggiorna la configurazione del tuo canale Slack	559
Creazione di casi di supporto in Slack	560
Risposta ai casi di supporto in Slack	566
Partecipa a una sessione di chat dal vivo con Supporto AWS	568
Ricerca di casi di supporto in Slack	574

Utilizzo dei risultati della ricerca	576
Risoluzione dei casi di supporto in Slack	578
Riapertura dei casi di supporto in Slack	578
Eliminare una configurazione di canale Slack dall'app Supporto AWS	579
Elimina una configurazione dell'area di lavoro Slack dall'app Supporto AWS	580
Supporto AWS Comandi dell'app in Slack	581
Comandi del canale Slack	581
Comandi del canale della live chat	582
Visualizza le corrispondenze Supporto AWS dell'app nel AWS Support Center Console	582
Crea AWS CloudFormation risorse per l' Supporto AWS app in Slack	583
Supporto AWS App e CloudFormation modelli	583
Creazione di risorse di configurazione Slack per la tua organizzazione	584
Scopri di più su CloudFormation	589
Crea risorse Supporto AWS per app utilizzando Terraform	590
Sicurezza	591
Protezione dei dati	592
Sicurezza dei casi di supporto	593
Identity and Access Management	594
Destinatari	594
Autenticazione con identità	595
Gestione dell'accesso tramite policy	596
Come Supporto AWS funziona con IAM	597
Esempi di policy basate su identità	599
Uso di ruoli collegati ai servizi	602
AWS politiche gestite	610
Gestisci l'accesso al Centro Supporto AWS	693
Gestisci l'accesso ai piani Supporto AWS	701
Gestisci l'accesso a AWS Trusted Advisor	706
Esempi di politiche di controllo dei servizi per AWS Trusted Advisor	716
Risoluzione dei problemi	718
Risposta agli incidenti	721
Registrazione e monitoraggio in Supporto AWS e AWS Trusted Advisor	721
Convalida della conformità	722
Resilienza	722
Sicurezza dell'infrastruttura	722
Analisi della configurazione e delle vulnerabilità	723

Esempi di codice	724
Nozioni di base	725
ciao Supporto	726
Informazioni di base	733
Azioni	791
Scenari	866
Guida introduttiva a Support	866
Monitoraggio e registrazione per Supporto	875
Supporto AWS Integrazione in EDAs	875
Come indirizza gli eventi EventBridge Supporto AWS	876
Supporto AWS eventi	876
Creazione di modelli di eventi	877
Evento Support Case Update	878
Registrazione delle chiamate Supporto AWS API con AWS CloudTrail	882
Supporto AWS informazioni in CloudTrail	882
AWS Trusted Advisor informazioni relative alla registrazione CloudTrail	883
Comprensione delle Supporto AWS voci dei file di registro	884
Registrazione delle chiamate all'API Supporto AWS dell'app con CloudTrail	886
Supporto AWS Informazioni sull'app in CloudTrail	886
Comprensione delle Supporto AWS voci dei file di registro dell'app	887
Monitoraggio e registrazione per i piani di supporto	892
Registrazione delle chiamate API Supporto AWS Plans con AWS CloudTrail	892
Supporto AWS Informazioni sui piani in CloudTrail	893
Informazioni sulle voci dei file di registro Supporto AWS di Plans	894
Registrazione delle azioni della console relative alle modifiche al piano Supporto	900
Monitoraggio e registrazione per Trusted Advisor	904
Monitoraggio dei risultati dei Trusted Advisor controlli con EventBridge	905
Creazione di CloudWatch allarmi per monitorare le metriche Trusted Advisor	908
Prerequisiti	908
CloudWatch metriche per Trusted Advisor	913
Trusted Advisor metriche e dimensioni	919
Registrazione delle azioni AWS Trusted Advisor della console con AWS CloudTrail	920
Trusted Advisor informazioni in CloudTrail	921
Esempio: voci dei file di Trusted Advisor registro	924
Risorse per la risoluzione dei problemi	928
Risoluzione dei problemi specifici dei servizi	928

Cronologia dei documenti 933

Aggiornamenti precedenti 977

..... cmlxxxi

Iniziare con Supporto AWS

Supporto AWS offre una gamma di piani che forniscono l'accesso a strumenti e competenze che supportano il successo e lo stato operativo delle vostre AWS soluzioni. Tutti i piani di supporto forniscono round-the-clock l'accesso 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.

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support + offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support +](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

 Note

- Per creare un' interazione di supporto per utilizzare la risoluzione dei problemi generata dall'intelligenza artificiale per risolvere il problema e, facoltativamente, creare una richiesta di assistenza, consulta [Risoluzione dei problemi potenziata dall'intelligenza artificiale nella console del Support Center](#)
- Per ulteriori informazioni sui diversi Supporto AWS piani, [consulta Confrontare Supporto AWS](#) i piani e [Piani di modifica Supporto AWS](#)
- I piani di supporto offrono tempi di risposta diversi per i tuoi casi di assistenza. Consulta [Scelta del livello di gravità iniziale dei casi di assistenza](#) e [Comprensione dei Supporto AWS tempi di risposta](#).

Argomenti

- [Risoluzione dei problemi potenziata dall'intelligenza artificiale nella console del Support Center](#)
- [Riunioni virtuali con Supporto AWS](#)
- [Gestione dei casi](#)
- [Richiedi un aumento della quota di servizio.](#)
- [Esperienza precedente: creazione di casi di supporto e gestione dei casi](#)
- [Utilizzo Supporto AWS con un AWS SDK](#)

Risoluzione dei problemi potenziata dall'intelligenza artificiale nella console del Support Center

Le funzionalità di risoluzione dei problemi potenziate dall'intelligenza artificiale che consentono di risolvere i problemi in modo più rapido ed efficiente sono disponibili in modalità supportata. Regioni AWS Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare le funzionalità della console del Support Center per risolvere problemi tecnici e problemi relativi all'account e alla fatturazione. Se disponi di un Supporto piano Basic, puoi utilizzare le funzionalità della console di Support Center per la risoluzione di domande generali e per ricevere assistenza su problemi relativi all'account e alla fatturazione. L'utilizzo della risoluzione dei problemi potenziata dall'intelligenza artificiale semplifica l'esperienza di supporto utilizzando la consapevolezza contestuale e la diagnostica automatizzata per fornire soluzioni mirate per l'ambiente in uso. AWS

La risoluzione dei problemi basata sull'intelligenza artificiale nella console di Support Center è supportata nelle seguenti versioni: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Europa (Irlanda)

Note

Se operi in un ambiente Regione AWS che non supporta le funzionalità potenziate dall'intelligenza artificiale nella console di Support Center, utilizzerai il metodo legacy di gestione dei casi. Per ulteriori informazioni, consulta [Esperienza precedente: creazione di casi di supporto e gestione dei casi](#).

Quando accedi alla console Support Center, puoi inserire la descrizione del problema in linguaggio naturale, importare conversazioni Amazon Q pertinenti, ricevere indicazioni generative sulla risoluzione dei problemi di intelligenza artificiale e scegliere di creare una richiesta di supporto con campi precompilati, se necessario.

Puoi fornire informazioni contestuali sull'ambiente e sul problema per ricevere soluzioni personalizzate durante l'intero processo di risoluzione dei problemi.

La risoluzione dei problemi basata sull'intelligenza artificiale nella Supporto AWS console offre i seguenti vantaggi chiave:

- Risoluzione più rapida dei problemi: ottieni risposte immediate e soluzioni pertinenti non appena descrivi il problema.
- Conservazione del contesto: importa le conversazioni precedenti di Amazon Q per mantenere il contesto di risoluzione dei problemi.
- Creazione semplificata dei casi: utilizza il linguaggio naturale per descrivere i problemi anziché navigare tra più campi del modulo.
- Seguito intelligente: ricevi domande di follow-up pertinenti in base al tuo ambiente specifico. AWS

Per un elenco completo delle funzionalità disponibili nel tuo piano di Support, [consulta Compare Supporto AWS Plans](#).

 Note

- Per modificare il piano di supporto, consulta la sezione [Piani di modifica Supporto AWS](#).
- Per chiudere il tuo account, consulta [Chiusura di un account](#) nella Guida AWS Billing per l'utente.
- Per trovare gli argomenti più comuni per la risoluzione dei problemi Servizi AWS, consulta [Risorse 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 Supporto AWS 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 Supporto AWS piani all'interno di un'organizzazione](#)
 - [Supporto offerto da AWS Partner](#)

 Important

Prima di avviare un'interazione di supporto o creare una richiesta di assistenza, verifica eventuali eventi che influiscono sulle risorse del tuo account visitando il sito Health Dashboard at <https://phd.aws.amazon.com/phd/home#/>. Puoi verificare eventuali Servizio AWS problemi nella dashboard, anche se potrebbe verificarsi un leggero ritardo nella pubblicazione degli incidenti. Se non sei sicuro che sia in corso un incidente, apri una richiesta di assistenza.

Argomenti

- [Configura le autorizzazioni per utilizzare la risoluzione dei problemi basata sull'intelligenza artificiale](#)
- [Crea un'interazione di supporto](#)
- [Crea una richiesta di supporto da un'interazione di supporto](#)
- [Visualizza le interazioni di supporto](#)
- [Risoluzione dei problemi](#)

Configura le autorizzazioni per utilizzare la risoluzione dei problemi basata sull'intelligenza artificiale

Per accedere alle funzionalità di risoluzione dei problemi ottimizzate dall'intelligenza artificiale in Support Center, sono necessarie autorizzazioni specifiche AWS Identity and Access Management . Questa sezione descrive le autorizzazioni IAM necessarie e spiega come configurarle in modo da poter utilizzare appieno queste funzionalità.

La risoluzione dei problemi basata sull'intelligenza artificiale richiede autorizzazioni oltre alla tradizionale gestione dei casi di supporto. Le autorizzazioni richieste si dividono in tre categorie:

- Autorizzazioni di interazione di supporto: abilita il nuovo flusso di lavoro basato sull'interazione nel Support Center.
- Autorizzazioni di classificazione basate sull'intelligenza artificiale: consenti l'accesso alle funzionalità di classificazione dei problemi basate sull'intelligenza artificiale.
- Autorizzazioni di integrazione con Amazon Q: abilita l'importazione delle conversazioni da Amazon Q Developer.

Queste autorizzazioni integrano le Supporto AWS autorizzazioni esistenti e non le sostituiscono.

Puoi configurare le autorizzazioni per la risoluzione dei problemi basata sull'intelligenza artificiale in due modi:

[Opzione 1: utilizza la politica AWS gestita](#) (consigliata). Allega la policy `AWSSupportAccess` gestita ai tuoi utenti o ruoli. Questa politica include tutte le autorizzazioni richieste e viene aggiornata automaticamente quando vengono rilasciate nuove Supporto funzionalità.

[Opzione 2: crea una politica personalizzata con le autorizzazioni minime richieste](#). Questo approccio offre un maggiore controllo ma richiede aggiornamenti manuali quando vengono aggiunte nuove funzionalità.

Opzione 1: utilizza la politica AWS gestita (consigliata)

Se al momento è allegata la politica di gestione degli `AWSSupport` accessi, non sono necessarie autorizzazioni aggiuntive. Tuttavia, per continuare a utilizzare le funzioni incluse nell'[API della console di Support Center](#), devi aggiungere le operazioni della console di Support Center alle tue politiche IAM prima del 2 novembre 2026, se non le hai già. A tale scopo, aggiorna la policy Supporto AWS

gestita per includere le support-console:* azioni. Per ulteriori informazioni, consulta [Aggiungere policy IAM per le operazioni dell'API Support Center Console](#).

Opzione 2: creare una politica personalizzata con autorizzazioni minime richieste

Puoi consentire esplicitamente di elencare azioni specifiche invece di utilizzare caratteri jolly. Di seguito sono riportate le autorizzazioni necessarie per le interazioni di supporto, la creazione e la gestione dei casi:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportedLanguages",
        "support:DescribeSupportLevel",
        "support:GetInteraction",
        "support:InitiateCallForCase",
        "support:ListInteractionEntries",
        "support:ListInteractions",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:ResolveCase",
        "support:ResolveInteraction",
        "support:SearchForCases",
        "support:StartInteraction",
        "support:UpdateInteraction",
        "support-console:GetAccountState",
```

```
    "support-console:GetAccountGovCloudEnabled",
    "support-console:GetCaseDraft",
    "support-console:CreateCaseDraft",
    "support-console>DeleteCaseDraft",
    "support-console:GetBanner",
    "support-console:DescribeDynamicHelp",
    "support-console:CreateContact",
  ],
  "Resource": "*"
}
```

Note

L'utilizzo di una politica personalizzata richiede una manutenzione continua man mano che vengono Supporto AWS rilasciate nuove funzionalità. Per ulteriori informazioni sulle operazioni dell'API della console di Support Center, vedere [Aggiungere policy IAM per le operazioni dell'API Support Center Console](#). Per ulteriori informazioni su ciascuna operazione dell' Supporto API, consulta [Gestisci l'accesso al Centro Supporto AWS](#).

Autorizzazioni richieste per l'integrazione con Amazon Q

Per utilizzare la funzionalità di importazione delle conversazioni di Amazon Q in Support Center, le identità IAM necessitano delle autorizzazioni per le seguenti azioni di Amazon Q Developer:

- `q:StartConversation`: Inizia una nuova conversazione con Amazon Q.
- `q:SendMessage`: Invia messaggi all'interno di una conversazione.
- `q:GetConversation`: recupera i dettagli della conversazione. Questa azione è necessaria per l'accesso alla console.
- `q:ListConversations`: elenca le conversazioni disponibili. Questa azione è necessaria per l'accesso alla console e l'integrazione del Support Center.

L'integrazione di Amazon Q con Support Center Console richiede specificamente l'`q:ListConversations` autorizzazione a visualizzare le conversazioni recenti per l'importazione.

Per indicazioni dettagliate sulla configurazione delle autorizzazioni di Amazon Q Developer, consulta [Amazon Q Developer permissions reference](#) e [Manage access to Amazon Q Developer with policies](#).

Applicazione delle autorizzazioni necessarie per le interazioni di supporto

Per applicare le autorizzazioni ai tuoi utenti IAM, completa i seguenti passaggi:

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, selezionare Policies (Policy) e Create Policy (Crea policy).
3. Scegli la scheda JSON e incolla uno dei documenti di policy menzionati nelle sezioni precedenti.
4. Scegli Avanti: Tag, quindi Avanti: Revisione.
5. Inserisci il nome di una politica, ad esempio SupportConsoleInteractionsAccess e fornisci una descrizione che spieghi lo scopo della politica.
6. Scegli Crea policy.
7. Allega la policy ai tuoi utenti, gruppi o ruoli IAM che devono accedere al Support Center.

Se disponi già di allegati alla policy gestita di AWSSupport Access, allega la policy personalizzata supplementare alla policy gestita.

Crea un'interazione di supporto

Un'interazione di supporto è il modo in cui inizi il tuo coinvolgimento Supporto AWS. Per prima cosa descrivi il problema utilizzando il linguaggio naturale e ricevi assistenza su misura per te utilizzando la risoluzione dei problemi basata sull'intelligenza artificiale. L'interazione iniziale potrebbe includere il chiarimento di domande, soluzioni contestuali e la risoluzione automatica dei problemi, senza creare una richiesta di supporto. Queste interazioni potrebbero risolvere i problemi in modo indipendente o fungere da base per una richiesta di assistenza ripetuta con l'intervento di un tecnico umano, se necessario.

Supporto le interazioni differiscono dai casi di supporto in quanto i casi di supporto includono il coinvolgimento con un Cloud Support Engineer. Puoi scegliere di generare automaticamente una richiesta di supporto in base a una precedente interazione di supporto. Il caso di supporto mantiene tutto il contesto dell'interazione di supporto iniziale e include ulteriori approfondimenti generati dall'intelligenza artificiale per aiutare il Cloud Support Engineer a risolvere il problema. Questa potente combinazione di risoluzione dei problemi e assistenza potenziata dall'intelligenza artificiale

da parte dei tecnici del Cloud AWS Support porta potenzialmente a una risoluzione più rapida dei problemi e a una riduzione dei tempi di inattività.

Note

- Puoi tornare al metodo precedente di gestione dei casi scegliendo Usa la vecchia esperienza nel banner nella parte superiore della console di Support Center. Per ulteriori informazioni, consulta [Esperienza precedente: creazione di casi di supporto e gestione dei casi](#).
- Puoi accedere alla console del Support Center come utente AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Gestisci l'accesso al Centro Supporto AWS](#).
- Se non riesci ad accedere alla console del Support Center e a creare una richiesta di supporto, puoi invece utilizzare la pagina [Contattaci](#). Puoi utilizzare questa pagina per ricevere assistenza per problemi di fatturazione e account.

Per avviare un'interazione con l'assistenza, completa i seguenti passaggi:

1. Accedi alla [AWS Support Center Console](#).

Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

2. Sono disponibili diverse opzioni per avviare l'interazione con l'assistenza:
 - Inserisci i dettagli sui problemi per i quali hai bisogno di assistenza. In questo modo puoi iniziare una nuova interazione con l'assistenza. Inserisci informazioni dettagliate sul problema e sulle eventuali procedure di risoluzione dei problemi che hai già intrapreso.
 - Continua un'interazione di assistenza esistente: scegli tra un'interazione di assistenza recente mostrata nella sezione Descrivi il problema o continua con. Questa sezione mostra le due interazioni di assistenza più recenti. Accedi alla sezione Visualizzazione delle interazioni di supporto passate per visualizzare altre interazioni di supporto passate.

- Usa una trascrizione di Amazon Q: seleziona l'icona Amazon Q nel campo di testo per visualizzare un elenco di conversazioni Amazon Q recenti. Regione AWS Vengono mostrate le cinque conversazioni più recenti dal AWS GovCloud (Stati Uniti orientali). In alternativa, scegli tra un'interazione recente di Amazon Q mostrata nella sezione Descrivi il problema o continua con. Quando selezioni una conversazione, viene generato un riepilogo di quella conversazione e aggiunto alla casella di testo. Se selezioni una conversazione Amazon Q, visualizzerai un disclaimer relativo all' Regione AWS accessibilità degli utenti.
3. Scegli l'icona Invia in basso a destra nel campo di testo.
 4. Supporto AWS la risoluzione dei problemi generativi basata sull'intelligenza artificiale analizza la richiesta insieme all'ambiente specifico. AWS È possibile che venga richiesto di fornire informazioni aggiuntive per facilitare l'analisi. Se viene visualizzata una richiesta di informazioni aggiuntive, inserisci i dati richiesti, quindi scegli Invia. Se non conosci o non hai accesso alle informazioni richieste, puoi saltare questo passaggio e ricevere invece una risposta indicativa generale. Tieni presente che una risposta orientativa generale non è specifica per il tuo AWS ambiente.

Una volta completata l'analisi, viene visualizzato un riepilogo dei risultati, insieme alle fasi di correzione. Per visualizzare le fonti utilizzate nelle fasi di analisi e correzione, scegli Fonti.

5. Se hai bisogno di ulteriore assistenza, puoi completare una delle seguenti opzioni:
 - Continua con il supporto assistito dall'intelligenza artificiale: per perfezionare ulteriormente l'analisi assistita dall'intelligenza artificiale e generare una nuova risposta, scegli Aggiungi altri dettagli per una risposta migliore. Inserisci le informazioni nel campo Dettagli aggiuntivi, quindi scegli Invia. Tieni presente che questa opzione serve a contestualizzare ulteriormente il problema originale. Se devi inserire il contesto per un nuovo problema, seleziona Inizia una nuova interazione nella parte superiore o inferiore dello schermo.
 - Crea una richiesta di supporto: per creare una richiesta di supporto con Supporto AWS, scegli Crea una richiesta. Questa opzione avvia il flusso di lavoro per la creazione del caso. Molti dettagli del caso vengono compilati automaticamente in base all'interazione con l'assistenza. Puoi modificare queste informazioni in base alle tue esigenze. L'interazione con l'assistenza, inclusi i dettagli di eventuali passaggi di risoluzione forniti, viene aggiunta alla richiesta di assistenza. Per i dettagli su come creare una richiesta di supporto, consulta [Crea una richiesta di supporto da un'interazione di supporto](#).

In qualsiasi momento durante l'interazione con l'assistenza, puoi utilizzare le icone Pollice su e Pollice giù per fornire feedback sulla tua esperienza.

Crea una richiesta di supporto da un'interazione di supporto

Quando selezioni Crea richiesta durante l'interazione con l'assistenza, viene creata una richiesta di supporto con molti dettagli del caso, ad esempio l'oggetto, la descrizione, il tipo di caso, il servizio, la categoria e il livello di gravità compilati automaticamente. È possibile modificare queste informazioni in base alle esigenze. Assicurati di controllare la correttezza di queste informazioni. Per informazioni su come scegliere un livello di gravità per il tuo caso, vedi [Scelta del livello di gravità iniziale per i casi di supporto](#).

Important

Prima di creare una richiesta di assistenza, verifica gli eventi che influiscono sulle risorse del tuo account visitando il sito [Health Dashboard](#). Puoi verificare eventuali Servizio AWS problemi nella dashboard. Potrebbe esserci un leggero ritardo nella pubblicazione degli incidenti. Se non sei sicuro che sia in corso un incidente, apri una richiesta di assistenza.

Dopo aver scelto Crea caso, inserisci o verifica le seguenti informazioni:

1. Verifica l'oggetto di questo caso di supporto. L'Oggetto è una breve sinossi dell'argomento dell'interazione con l'assistenza.
2. Verifica la descrizione. La tua richiesta iniziale viene visualizzata nel campo Descrizione. Modificare queste informazioni in base alle esigenze. 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.
3. (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.
4. Per Tipo di caso, scegliete una delle seguenti opzioni:
 - Account e fatturazione
 - Tecnico
 - Quote di servizio. È possibile richiedere solo determinati tipi di aumenti della quota di servizio dalla console Support Center. Per ulteriori informazioni, consulta [Richiedi un aumento della quota di servizio](#).

 Note

Se disponi di un Supporto piano Basic, non puoi creare una richiesta di assistenza tecnica.

5. Verifica il servizio, la categoria e la gravità.
6. Nella sezione Preferenze di comunicazione, indica come AWS desideri comunicare con te. Puoi scegliere una delle seguenti opzioni:
 - a. E-mail: ricevi una risposta alla tua email.
 - b. Telefono: ricevi una telefonata da un agente dell'assistenza. Se si sceglie questa opzione, immetti le informazioni riportate di seguito:
 - Paese o regione
 - Numero di telefono
 - (Facoltativo) Estensione
 - c. Chat: avvia una chat dal vivo con un agente dell'assistenza. In caso di mancata connessione a una chat, consulta [Risoluzione dei problemi](#).

(Facoltativo) Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi inserire fino a 10 indirizzi e-mail aggiuntivi nei 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 del tuo account root, non è necessario includere il tuo 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 Il mio account riceve copie della corrispondenza relativa al caso, ma solo per i tipi specifici di account e fatturazione.

- Quando sei pronto per inviare la richiesta di assistenza, seleziona **Invia**. Verrai indirizzato alla pagina dei dettagli del caso, dove puoi vedere i dettagli del caso, l'interazione con l'assistenza e le corrispondenze del caso.

Seleziona i dettagli del caso per visualizzare le informazioni relative al caso, ad esempio gli allegati o il livello di gravità. Seleziona **Interazioni di supporto** per visualizzare le interazioni di supporto associate a questo caso.

Procedure ottimali e tempi di risposta prefissati per i casi di Enterprise Support

Prima di creare una richiesta di assistenza, verifica gli eventi che influiscono sulle risorse del tuo account visitando il sito [Health Dashboard](#). Puoi verificare eventuali Servizio AWS problemi nella dashboard. Potrebbe esserci un leggero ritardo nella pubblicazione degli incidenti. Se non sei sicuro che sia in corso un incidente, apri una richiesta di assistenza.

Quando crei la tua richiesta di assistenza, assicurati di scegliere il livello di gravità corretto e di fornire quante più informazioni possibili. Per ulteriori informazioni sul tipo di informazioni da fornire, vedere la seguente sezione sulle best practice relative ai casi di Enterprise Support.

Utilizza la seguente matrice per identificare la gravità corretta.

AWS ITIL Case Severity Matrix				
Urgency				
		Low	Medium	High
Impact	Low	Low	Normal	High
	Medium	Normal	High	Urgent
	High	High	Urgent	Critical

Per i casi critici o urgenti, assicurati di lasciare i dati di contatto in modo che possiamo contattarti, se necessario.

Note

Il modo più rapido per ricevere assistenza è utilizzare il metodo di contatto via chat o telefono.

Argomenti

- Tempi di risposta previsti per i casi di Enterprise Support
- Best practice di Enterprise Support

- Percorso di crescita dell'Enterprise Support

Tempi di risposta previsti per i casi di Enterprise Support

Il grafico seguente mostra i tempi di Supporto AWS risposta previsti per i diversi livelli di gravità dei casi.

ITIL Priority	Severity Level	How to Raise		Examples for reference
Critical	Business Critical System Down		15 minutes	Major outage; loss of entire enterprise or customer base. Has potential for large revenue loss or business risk.
Urgent	Production System Down		1 hour	Business significantly impacted, where important functions or applications aren't available.
High	Production System Impaired		4 hours	Critical functions of your applications are impaired or degraded.
Normal	System Impaired		12 hours	Non-critical applications are behaving abnormally; time-sensitive development question.
Low	General Guidance		24 hours	General development/ service questions or want to submit feature request.

Procedure ottimali per i casi di Enterprise Support

Invia la tua richiesta di supporto con il livello di gravità appropriato.

- Il livello di gravità appropriato aiuta a garantire la visibilità del caso AWS e consente al TAM di gestire il problema.
- Invia solo un caso per ogni evento o problema.
- Assicurati di sollevare i casi nel modo corretto Account AWS.

Fornisci quante più informazioni dettagliate possibili, rispondendo alle domande pertinenti fornite nel seguente elenco:

- Chi: chi ha fatto cosa? Chi è interessato? Chi dovrebbe essere collegato? Con chi hai già parlato?
- Cosa: cos'è successo, esattamente. Qual è il raggio d'impatto o il raggio dell'esplosione? Cosa hai già provato per risolvere il problema?
- Quando: quando è successo o è successo (data, ora, fuso orario)? Entro quando hai bisogno di una risposta?
- Dove: Regione AWS, zona di disponibilità, istanza o risorsa IDs specifica e altri identificatori.
- Perché: perché state aprendo questo caso (informazioni, aumento dei limiti, analisi degli eventi o RCA, interruzione)?

- Come: includi informazioni su come riprodurre il problema, su come aggravarlo e su come contattarti.

Note

Puoi modificare la gravità della richiesta di assistenza dopo averla creata. Per informazioni, consulta [Modifica del livello di gravità del caso di assistenza](#).

Enterprise Support aziendale critico o sistema di produzione inattivo

- In caso di guasto di sistemi aziendali critici o di sistemi di produzione, utilizza la chat o il telefono e assicurati che nell'organizzazione ci siano persone disponibili per risolvere il problema.
- Descrivi chiaramente il problema, includendo ciò che hai provato, cosa ti aspetti e il contesto. Riassumi l'impatto aziendale.
- Fornisci (o inizia a registrare) quante più metriche, tempistiche e sintomi possibile. Più dati significano diagnosi più rapide.
- Fornisci un ponte per conferenze. Quando si segnala un problema di inattività di un sistema di importanza critica per l'azienda, offri un ponte di conferenza a cui i team di supporto possano partecipare per aiutarli a risolvere il problema. Poiché i problemi di inattività di un sistema di importanza critica per l'azienda sono inattivi, è meglio coinvolgere tutti al telefono e definire un piano d'azione comune per risolverli.
- Assicurati che tutte le attività relative all'evento siano incluse nel caso di assistenza (aggiornamento dalla console, non tramite e-mail). L'opzione telefono è utile per le comunicazioni in tempo reale; tuttavia, assicurati di registrare gli aggiornamenti e i risultati nella richiesta di supporto.

Percorso di crescita dell'Enterprise Support

È possibile seguire la seguente step-by-step procedura quando si verifica un problema.

1. Controlla Health Dashboard se ritieni che il problema possa essere correlato a Servizio AWS operazioni anomale.
2. Valuta le informazioni sul caso come indicato nella precedente sezione Support Case Best Practices.
3. Seleziona la gravità appropriata e usa il telefono o la chat se è necessaria una risposta rapida.

4. Contatta il tuo TAM se hai bisogno di ulteriore assistenza o se non ricevi una risposta come previsto.

Visualizza le interazioni di supporto

Le interazioni passate con Supporto AWS vengono salvate per 10 anni. Puoi visualizzare le interazioni passate dalla Supporto dashboard selezionando l'icona Elenco. Quindi, scegli l'interazione che desideri visualizzare. Vengono visualizzati i dettagli dell' Supporto AWS interazione. Se scegli di creare una richiesta di supporto a partire da un'interazione, l'interazione non viene più visualizzata nell'elenco delle interazioni passate. L'interazione ora viene visualizzata nella pagina dei dettagli del caso del caso di supporto associato.

Puoi aggiungere ulteriori dettagli all'interazione per generare una nuova risposta. In alternativa, puoi scegliere di creare un Supporto caso dall'interazione selezionando Crea un caso nella schermata dei dettagli dell' Supporto AWS interazione.

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 Supporto AWS:
- La tua rete può accedere all'endpoint `*.connect.us-east-1.amazonaws.com`.

Note

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

- Il firewall supporta le connessioni Web socket.

Se ancora non riesci a connetterti alla finestra della chat, contatta Supporto AWS utilizzando le opzioni di contatto e-mail o telefoniche.

Riunioni virtuali con Supporto AWS

Le riunioni virtuali consentono di entrare in contatto con i Supporto AWS tecnici tramite videochiamate con funzionalità di condivisione dello schermo. Questa funzionalità consente di risolvere problemi tecnici complessi che richiedono dimostrazioni visive o collaborazione in tempo reale.

Quando un tecnico dell'assistenza stabilisce che il caso richiede assistenza visiva, può avviare una riunione virtuale. Riceverai un invito alla riunione nella pagina dei dettagli del caso nel AWS Support Center. Dopo aver accettato l'invito, partecipi a una videochiamata sicura in cui puoi condividere lo schermo e collaborare con il tecnico dell'assistenza.

Le riunioni virtuali si integrano con Amazon Connect e utilizzano la tecnologia WebRTC per fornire videoconferenze sicure basate su browser senza richiedere l'installazione di software aggiuntivo.

[Le riunioni virtuali sono disponibili solo nella versione commerciale. Regioni AWS](#)

Argomenti

- [Partecipa a una riunione virtuale](#)
- [Sicurezza e privacy durante la riunione virtuale](#)
- [Autorizzazioni IAM richieste per le riunioni virtuali](#)
- [Risoluzione dei problemi relativi alle riunioni virtuali](#)

Partecipa a una riunione virtuale

Le riunioni virtuali vengono avviate dal Supporto AWS tecnico che ti assiste nella richiesta di supporto. Per partecipare a una riunione virtuale, completa i seguenti passaggi.

1. Quando un tecnico dell'assistenza avvia una riunione virtuale, nella pagina dei dettagli del caso di supporto viene visualizzato un invito alla riunione. Per partecipare alla riunione, scegli **Partecipa alla riunione virtuale** per accettare l'invito.

Gli inviti alle riunioni scadono dopo 10 minuti. Se non ti iscrivi entro questo periodo, richiedi una nuova riunione al tuo tecnico dell'assistenza.

2. Concedi le autorizzazioni del browser per l'accesso alla videocamera e al microfono quando richiesto.

La riunione virtuale si apre in una nuova finestra e sarai connesso al tecnico dell'assistenza. Puoi disattivare e riattivare il microfono o disconnetterti dalla riunione utilizzando i pulsanti nella parte inferiore dello schermo.

Sicurezza e privacy durante la riunione virtuale

Le riunioni virtuali utilizzano gli stessi meccanismi di autenticazione e autorizzazione Supporto AWS delle altre operazioni. Le seguenti misure di sicurezza proteggono le tue riunioni:

- Convalida della titolarità dei casi: puoi partecipare alle riunioni solo per i casi che appartengono al tuo Account AWS.
- AWS Identity and Access Management Controllo degli accessi basato su (IAM): devi disporre delle autorizzazioni IAM appropriate per partecipare alle riunioni virtuali.
- Connessioni crittografate: tutti i dati delle riunioni vengono trasmessi tramite connessioni WebRTC crittografate.
- Registrazione di audit: tutte le attività delle riunioni vengono registrate AWS CloudTrail per scopi di conformità e controllo.

Important

Le riunioni virtuali vengono registrate per garantire la qualità e per scopi di formazione. Non condividere informazioni sensibili come password o chiavi di accesso durante la riunione.

Autorizzazioni IAM richieste per le riunioni virtuali

Per partecipare alle riunioni virtuali, il tuo utente o ruolo IAM deve disporre delle seguenti autorizzazioni:

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

Per ulteriori informazioni sulle autorizzazioni Supporto AWS, consulta [Gestisci l'accesso al Centro Supporto AWS](#).

Risoluzione dei problemi relativi alle riunioni virtuali

Non riesco a vedere l'invito alla riunione.

Verifica che il tecnico dell'assistenza abbia avviato la riunione. Aggiorna la pagina dei dettagli del caso. Se l'invito continua a non essere visualizzato, contatta il tecnico dell'assistenza tramite la corrispondenza relativa al caso.

L'invito alla riunione è scaduto.

Gli inviti alle riunioni scadono dopo 10 minuti per motivi di sicurezza. Richiedi un nuovo invito alla riunione dal tuo tecnico dell'assistenza.

Sto riscontrando problemi di connessione.

Verificare la connessione Internet. Assicurati che le impostazioni di sicurezza del firewall o della rete consentano il traffico WebRTC. Prova a utilizzare un browser o una connessione di rete diversi.

Ricevo un errore di autorizzazione.

Verifica che il tuo utente o ruolo IAM disponga delle autorizzazioni per `support:InitiateLiveContactForCase`.

Gestione dei casi

Note

Puoi tornare al metodo precedente di gestione dei casi scegliendo Usa la vecchia esperienza nel banner nella parte superiore della console del Support Center. Per ulteriori informazioni, consulta [Esperienza precedente: creazione di casi di supporto e gestione dei casi](#).

In Console di gestione AWS, puoi creare tre tipi di casi relativi ai clienti in Supporto:

- 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 [Piani di modifica Supporto AWS](#).
- 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, consulta [Risorse 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 Supporto AWS 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 Supporto AWS piani all'interno di un'organizzazione](#)
 - [Supporto offerto da AWS Partner](#)

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.

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

Scelta del livello di gravità iniziale dei casi di assistenza

Quando crei un caso di supporto, assicurati di definire il livello di gravità corretto e di fornire quante più informazioni possibili.

Potresti voler creare un caso di supporto con la massima severità consentita dal tuo piano di supporto. Tuttavia, è consigliabile scegliere la severità massima solo per i casi che non possono essere risolti o che influiscono direttamente sulle applicazioni di produzione. Per informazioni su come creare i servizi in modo che la perdita di una singola risorsa non influisca sulle applicazioni, consulta il documento tecnico [Building Fault-Tolerant Applications](#). AWS

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

Note

- Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi riassegnare il livello di gravità dei casi di supporto per riflettere le modifiche all'urgenza e all'impatto aziendale. Ad esempio, è possibile modificare la richiesta di assistenza da Sistema compromesso a Sistema di produzione compromesso. Quando si modifica la gravità del caso, Supporto AWS riceve una notifica e indirizza il caso in base al nuovo livello di gravità. Per ulteriori informazioni, consulta [Modifica del livello di gravità del caso di assistenza](#).
- Se disponi di un Supporto piano Basic, non puoi modificare il livello di gravità di un caso di assistenza dopo averlo creato. Se la situazione cambia, collabora con l' Supporto agente.
- Per ulteriori informazioni sul livello di gravità, consulta la [Documentazione di riferimento dell'API Supporto AWS](#).

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 caratteristica. (Piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Sistema di produzione impattato	high	4 ore	Funzioni importanti della tua applicazione sono danneggiate o mostrano un deterioramento. (Piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Sistema di produzione spento	urgent	1 ora	L'impatto sulla tua attività è notevole. Funzioni importanti della tua applicazione non sono disponibili. (Piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Sistema business-critical spento	critical	- AWS Business Support+: meno di 30 minuti - AWS Enterprise	La tua attività è a rischio. Funzioni critiche della tua applicazione non sono disponibili.

Gravità	Codice di livello di gravità	Tempo della prima risposta	Descrizione e piano di supporto
		e Support: meno di 15 minuti • AWS Operazio i unificate : 5 minuti da un tecnico addetto alla gestione degli incidenti	

Comprensione dei Supporto AWS tempi di risposta

Supporto AWS compie ogni ragionevole sforzo per rispondere alla richiesta iniziale entro il periodo di tempo indicato. Per informazioni sull'ambito del supporto per ciascun Supporto piano, consulta [Supporto AWS le funzionalità](#).

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, hai round-the-clock accesso al supporto tecnico.

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, l'assistenza in giapponese è disponibile durante l'orario lavorativo in Giappone, dalle 09:00 alle 18:00 ora solare giapponese (GMT+9), esclusi i giorni festivi e i fine settimana.
- Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in giapponese.

Se scegli il cinese come lingua di contatto preferita per i casi di assistenza, l'assistenza in cinese potrebbe essere disponibile come segue:

- 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in cinese.

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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in coreano.

Se scegli il turco come lingua di contatto preferita per i casi di assistenza, l'assistenza in turco potrebbe essere disponibile come segue:

- Se hai bisogno del servizio clienti per casi di supporto non tecnico, l'assistenza in turco è disponibile durante l'orario lavorativo in Türkiye, dalle 09:00 alle 18:00 (GMT+3), esclusi i giorni festivi e i fine settimana.
- Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in inglese.

Modifica del livello di gravità del caso di assistenza

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi riassegnare il livello di gravità dei casi di supporto per riflettere le modifiche all'urgenza e all'impatto aziendale. Ad esempio, è possibile modificare la richiesta di assistenza da Sistema compromesso a Sistema di produzione compromesso. Quando modificate la gravità del caso, Supporto AWS riceve una notifica e si occupa del caso in base al nuovo livello di gravità.

Note

I casi di fatturazione o account in giapponese (JP), Service Quota Increase Request (SQIR) e turco (TR) per account o casi di fatturazione creati in queste lingue hanno una gravità predefinita e non possono essere modificati.

Per modificare la gravità di un caso di supporto, completa i seguenti passaggi:

1. Accedi alla [AWS Support Center Console](#).

Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

2. Seleziona il caso per cui desideri modificare il livello di gravità.
3. Nei dettagli del caso, scegli l'icona a forma di matita accanto al campo Severità, come mostrato nell'esempio seguente.

Case details	
Subject [redacted]	Status Unassigned
Case ID [redacted]	Severity General guidance 
Created 2025-04-24T08:49:10.815Z	Category -
Case type Technical	Language Portuguese

4. Per Severità, scegli il nuovo livello di gravità tra le seguenti opzioni:

- Informazioni generali
 - Sistema impattato
 - Sistema di produzione impattato
 - Sistema di produzione spento
 - Sistema business-critical spento
5. In Motivo della modifica della gravità del caso, scegli tra le opzioni disponibili per il motivo per cui stai modificando la gravità del caso.
 6. (Facoltativo) Per ulteriori informazioni, inserisci ulteriori informazioni su questa modifica.
 7. Esegui una delle seguenti operazioni:
 - Se stai riducendo la gravità dei casi di assistenza o se la stai elevando da Linee guida generali a Sistema compromesso o Sistema di produzione compromesso, scegli Aggiorna.
 - Se stai innalzando la priorità a un sistema di produzione o a un sistema critico per l'azienda, utilizza una delle opzioni nella sezione Metodi di contatto per interagire Supporto AWS, quindi scegli Aggiorna. L'esempio seguente mostra le opzioni disponibili nella sezione Metodi di contatto.

The screenshot shows a modal dialog titled "Change case severity" with a close button (X) in the top right corner. The dialog contains the following sections:

- Severity:** A dropdown menu currently showing "Production system down".
- Reason for case severity change:** A dropdown menu currently showing a hyphen (-).
- Tell us more - optional:** A text input field with the placeholder text "Tell us more about the reason for the escalation".
- Contact methods:** A section with an "Info" link and a blue banner that reads "For high severity issues we recommend using our live contact mechanisms". Below this are three radio button options:
 - Web:** "We'll respond by email and Support Center." (radio button is unselected)
 - Chat(Recommended):** "Chat online with a representative." (radio button is selected)
 - Phone(Recommended):** "We'll call you back at your number." (radio button is unselected)

At the bottom right of the dialog are two buttons: "Cancel" and "Update".

Note

- Se si aggiorna la severità del caso di supporto impostando un sistema di produzione inattivo o un sistema critico per l'azienda, è necessario attendere 60 minuti prima di poter modificare nuovamente la gravità.
- Se la tua richiesta di assistenza è attualmente impostata su Business-critical system down, ti verrà richiesto di avviare un contatto in tempo reale Supporto AWS invece di assegnare un livello di gravità più elevato.
- Se stai innalzando il livello di gravità della richiesta di assistenza dopo averlo già innalzato almeno una volta, potresti incorrere in un periodo di attesa. Ad esempio, se modifichi la gravità da Sistema compromesso a Sistema di produzione compromesso alle 6:00, la richiesta di assistenza rientra nel tempo di prima risposta di 4 ore previsto per il livello di gravità compromesso dal sistema di produzione. In questo scenario, è possibile aggiornare nuovamente il livello di gravità alle 10:00, dopo la finestra di 4 ore. Per un elenco dei tempi di prima risposta per ogni livello di gravità, consulta la tabella in: [Comprensione dei Supporto AWS tempi di risposta](#)

Richiedi un aumento della quota di servizio.

Puoi richiedere aumenti delle quote di servizio (precedentemente denominate limiti) per supportare i requisiti del carico di lavoro.

Utilizza il servizio Service Quotas per richiedere aumenti direttamente per i tuoi servizi. Per ulteriori informazioni, consulta la seguente documentazione:

- [Che cos'è Service Quotas?](#) nella Guida per l'utente di Service Quotas
- [Richiesta di un aumento di quota](#) nella Guida per l'utente di Service Quotas.

Al momento, Service Quotas non supporta affatto le Servizi AWS quote di servizio. Regioni AWS
Se il tuo Servizio AWS o non Regione AWS è disponibile nella [console Service Quotas](#), completa i seguenti passaggi per creare una richiesta di supporto per richiedere l'aumento della quota:

1. Accedi alla [AWS Support Center Console](#).

 Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

2. Nella pagina Interazioni di supporto, inserisci i dettagli su questo aumento del limite di servizio. Quando richiesto, scegli Crea un caso. Molti campi del Supporto casi verranno precompilati con il testo che hai inserito durante l'interazione. Puoi modificare questi campi in base alle tue esigenze. Per ulteriori dettagli sulla creazione di un'interazione di supporto, consulta [Crea un'interazione di supporto](#).
3. Per Tipo di caso, seleziona Quote di servizio.
4. Per Assistenza, seleziona Aumento del limite di servizio.
5. Per Categoria, seleziona il tipo di aumento che stai richiedendo dall'elenco. Qui sono elencate solo le richieste di aumento del limite di servizio disponibili nel Support Center. Per altri tipi di richieste di limiti di servizio, vedere [Richiesta di un aumento della quota](#) nella Service Quotas User Guide.
6. (Facoltativo) Dal menu a discesa Lingua di contatto preferita, seleziona la lingua che desideri utilizzare Supporto AWS per comunicare con te.
7. Per Regione, seleziona la zona Regione AWS in cui richiedi l'aumento.

 Note

Regione AWS la selezione non è disponibile se hai selezionato Generale come Categoria.

8. (Facoltativo) Per richiedere aumenti multipli del limite, scegli Aggiungi un altro limite, quindi scegline un altro Regione AWS.
9. Inserisci una descrizione per questo o più aumenti della quota di servizio. È possibile allegare file, se necessario.
10. Scegli Passaggio successivo: risolvi ora o contattaci.
11. Per le opzioni di contatto, scegli 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
12. Quando sei pronto per inviare la richiesta di assistenza, seleziona **Invia**. Verrai indirizzato alla pagina dei dettagli del caso, dove puoi vedere i dettagli del caso, l'interazione con l'assistenza e le corrispondenze del caso.

Seleziona i dettagli del caso per visualizzare le informazioni relative al caso, ad esempio gli allegati o il livello di gravità. Seleziona **Interazioni di supporto** per visualizzare le interazioni di supporto associate a questo caso.

Esperienza precedente: creazione di casi di supporto e gestione dei casi

Important

Puoi tornare al metodo precedente di gestione dei casi scegliendo **Usa la vecchia esperienza** nel banner nella parte superiore della console del Support Center.

In Console di gestione AWS, puoi creare tre tipi di casi relativi ai clienti in Supporto:

- 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 [Piani di modifica Supporto AWS](#).
- 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, consulta [Risorse 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 Supporto AWS 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 Supporto AWS 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 Console di gestione AWS.

 Note

- Puoi accedere a Support Center come utente AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Gestisci l'accesso al Centro Supporto AWS](#).
- 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 Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

2. Scegli Crea caso.
3. Scegli una delle seguenti opzioni:
 - Account e fatturazione
 - Tecnico
 - Per aumentare la quota di servizio, scegli Cerchi aumenti della quota di servizio? e poi segui le istruzioni per [Richiedi un aumento della quota 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:
 - Console di gestione AWS
 - 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 Supporto.
- 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 si dispone di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, viene visualizzata l'opzione 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 iniziale dei casi di supporto

Potresti voler creare un caso di supporto con la massima severità consentita dal tuo piano di supporto. Tuttavia, è consigliabile scegliere la severità massima solo per i casi che non possono essere risolti o che influiscono direttamente sulle applicazioni di produzione. Per informazioni su come creare i servizi in modo che la perdita di una singola risorsa non influisca sulle applicazioni, consulta il documento tecnico [Building Fault-Tolerant Applications](#). AWS

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

Note

- Se disponi di un piano Enterprise Support o Enterprise On-Ramp, puoi riassegnare il livello di gravità dei casi di supporto in base alle modifiche relative all'urgenza e all'impatto aziendale. Ad esempio, è possibile modificare la richiesta di assistenza da Sistema compromesso a Sistema di produzione compromesso. Quando si modifica la gravità del caso, Supporto AWS riceve una notifica e indirizza il caso in base al nuovo livello di gravità. Per ulteriori informazioni, consulta [Modifica del livello di gravità del caso di assistenza](#).
- Se non disponi del supporto Enterprise o di un piano Enterprise On-Ramp, non puoi modificare il livello di gravità di un caso di supporto dopo averlo creato. Se la situazione cambia, contatta l' Supporto agente responsabile della tua richiesta di assistenza.
- Per ulteriori informazioni sul livello di gravità, consulta la [Documentazione di riferimento dell'API Supporto AWS](#).

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 caratteristica. (*Piano Developer, AWS Business Support +, AWS Enterprise Support o AWS Unified Operations)
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 Developer, AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Sistema di produzione impattato	high	4 ore	Funzioni importanti della tua applicazione sono danneggiate o mostrano un deterioramento. (Piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Sistema di produzione spento	urgent	1 ora	L'impatto sulla tua attività è notevole. Funzioni importanti della tua applicazione non sono disponibili. (Piano AWS Business Support +, AWS Enterprise Support o AWS Unified Operations)
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.

Comprendere Supporto AWS i tempi di risposta

Supporto AWS compie ogni ragionevole sforzo per rispondere alla richiesta iniziale entro il periodo di tempo indicato. Per informazioni sull'ambito del supporto per ciascun Supporto piano, consulta [Supporto AWS le funzionalità](#).

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, hai round-the-clock accesso al supporto tecnico. *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 Console di gestione AWS.

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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in giapponese.

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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in cinese.

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 coreano 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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile tutto il giorno, tutti i giorni in coreano.

Modifica del livello di gravità del caso di assistenza

Se disponi di un piano Enterprise Support o Enterprise On-Ramp, puoi riassegnare il livello di gravità dei casi di supporto in base alle modifiche relative all'urgenza e all'impatto aziendale. Ad esempio, è possibile modificare la richiesta di assistenza da Sistema compromesso a Sistema di produzione compromesso. Quando modificate la gravità del caso, Supporto AWS riceve una notifica e si occupa del caso in base al nuovo livello di gravità.

Note

I casi di fatturazione o account in giapponese (JP), Service Quota Increase Request (SQIR) e turco (TR) per account o casi di fatturazione creati in queste lingue hanno una gravità predefinita e non possono essere modificati.

Per modificare la gravità di un caso di supporto, completa i seguenti passaggi:

1. Accedi alla [AWS Support Center Console](#).

Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

2. Seleziona il caso per cui desideri modificare il livello di gravità.
3. Nei dettagli del caso, scegli l'icona a forma di matita accanto al campo Severità, come mostrato nell'esempio seguente.

4. Per Severità, scegli il nuovo livello di gravità tra le seguenti opzioni:
 - Informazioni generali
 - Sistema impattato
 - Sistema di produzione impattato
 - Sistema di produzione spento
 - Sistema business-critical spento
5. In Motivo della modifica della gravità del caso, scegli tra le opzioni disponibili per il motivo per cui stai modificando la gravità del caso.
6. (Facoltativo) Per ulteriori informazioni, inserisci ulteriori informazioni su questa modifica.
7. Esegui una delle seguenti operazioni:
 - Se stai riducendo la gravità dei casi di assistenza o se la stai elevando da Linee guida generali a Sistema compromesso o Sistema di produzione compromesso, scegli Aggiorna.
 - Se stai innalzando la priorità a un sistema di produzione o a un sistema critico per l'azienda, utilizza una delle opzioni nella sezione Metodi di contatto per interagire Supporto AWS, quindi

scegli **Aggiorna**. L'esempio seguente mostra le opzioni disponibili nella sezione **Metodi di contatto**.

The screenshot shows a 'Change case severity' dialog box with a close button (X) in the top right corner. It contains the following fields and options:

- Severity:** A dropdown menu with 'Production system down' selected.
- Reason for case severity change:** A dropdown menu with '-' selected.
- Tell us more - optional:** A text input field with the placeholder text 'Tell us more about the reason for the escalation'.
- Contact methods:** A section with an 'Info' link and a blue banner that reads 'For high severity issues we recommend using our live contact mechanisms'. It contains three radio button options:
 - Web:** 'We'll respond by email and Support Center.' (Not selected)
 - Chat(Recommended):** 'Chat online with a representative.' (Selected)
 - Phone(Recommended):** 'We'll call you back at your number.' (Not selected)

At the bottom right, there are 'Cancel' and 'Update' buttons.

Note

- Se si aggiorna la severità del caso di supporto impostando un sistema di produzione inattivo o un sistema critico per l'azienda, è necessario attendere 60 minuti prima di poter modificare nuovamente la gravità.
- Se la tua richiesta di assistenza è attualmente impostata su Business-critical system down, ti verrà richiesto di avviare un contatto in tempo reale Supporto AWS invece di assegnare un livello di gravità più elevato.
- Se stai innalzando il livello di gravità della richiesta di assistenza dopo averlo già innalzato almeno una volta, potresti incorrere in un periodo di attesa. Ad esempio, se modifichi la gravità da Sistema compromesso a Sistema di produzione compromesso alle 6:00, la richiesta di assistenza rientra nel tempo di prima risposta di 4 ore previsto per il livello di gravità compromesso dal sistema di produzione. In questo scenario, è possibile aggiornare nuovamente il livello di gravità alle 10:00, dopo la finestra di 4 ore. Per un elenco dei tempi di prima risposta per ogni livello di gravità, consulta la tabella in [Comprensione dei Supporto AWS tempi di risposta](#)

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.



Hello!

We're here to help.

Account: 123456789012 • Support plan: Basic • [Change](#) 

How can we help?

Choose the related issue for your case.

1

☒ Account and billing

[Looking for Service limit increase?](#)

☐ Technical

2

Service

Billing ▼

3

Category

Other Billing Questions ▼

4

Severity [Info](#)

General question ▼

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 si riferiscono alla prima risposta di Supporto AWS. 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 iniziale dei casi di assistenza](#).

 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.

Additional information

Describe your issue

✔ Case draft saved

1 Subject

I have an issue with my bill

Maximum 250 characters (222 remaining)

Description

Don't share any sensitive information in case correspondences, such as credentials, credit cards, signed URLs, or personally identifiable information.

[Learn more](#) 

2

I found a charge on my bill for unused resources.

Maximum 5000 characters (4951 remaining)

3

 **Attach files**

Up to 3 attachments, each less than 5MB



Description Guidance

Provide a detailed description of your issue. If you have a question about a charge, provide the date, amount, or any other details about the charge.

Cancel

Previous

Next step: Solve now or contact us

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

2. **Descrizione** – Descrivi il caso di supporto. Questa è l'informazione più importante che fornischi a Supporto. 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.

How can we help?
[Account and billing](#), [Billing](#),
[Dispute a Charge](#), [General ...](#)

Additional information
[I have an issue in my account](#)

Solve now or contact us

Solve now | **Contact us**

Preferred contact language

English ▲

🔍 |

English ✓

中文

한국어

日本語

☐ Phone
We'll call you back at your number.

☐ Chat
Chat online with a representative.

Cancel Previous Submit

✔ Case draft saved

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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile 24 ore su 24, 7 giorni su 7 in giapponese.

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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile 24 ore su 24, 7 giorni su 7 in cinese.

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 coreano 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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, il supporto tecnico è disponibile 24 ore su 24, 7 giorni su 7 in coreano.

Esperienza precedente: 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, ricevi un'email con la corrispondenza e un link al caso nel Support Center. 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

- È necessario accedere all'indirizzo Account AWS che ha inviato la richiesta 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 Centro Supporto AWS](#).
- Se non rispondi al caso entro pochi giorni, lo Supporto AWS risolve automaticamente.
- 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](#)
- [Risoluzione di un caso di supporto](#)
- [Riapertura di un caso risolto](#)
- [Creazione di un caso correlato](#)

- [Cronologia dei casi](#)

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.

Note

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi riassegnare il livello di gravità dei casi di supporto per riflettere le modifiche all'urgenza e all'impatto aziendale. Se non disponi di uno di questi piani di supporto, non puoi aggiornare la gravità del tuo caso. Per ulteriori informazioni, consultare [Scelta del livello di gravità iniziale dei casi di assistenza](#) e [Modifica del livello di gravità del caso di assistenza](#).

Aggiornamento di un caso di supporto esistente

1. Accedi alla [AWS Support Center Console](#).

Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

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. Seleziona 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. Accedi alla [AWS Support Center Console](#).

 Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

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 hai Supporto AWS risolto il tuo caso, puoi utilizzare il link di feedback per fornire ulteriori informazioni sulla tua esperienza con Supporto AWS.

Example: Link di feedback

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

Please let us know if we helped resolve your issue:

If YES, click here:

<https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes> 

If NO, click here:

<https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No> 

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. Accedi alla [AWS Support Center Console](#).

Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

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. Accedi alla [AWS Support Center Console](#).

i Tip

In Console di gestione AWS, puoi anche scegliere l'icona del punto interrogativo



e quindi scegliere Support Center.

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.

This case can't be reopened

This case has been permanently closed after 14 days of inactivity. If you're experiencing the same issue or a similar one, you can create a related case. If you're experiencing a different issue, create a new case.

Cancel

Create new case

Create related case

5. Per creare il caso, seguire la stessa procedura. Per informazioni, consulta [Creazione di un caso di supporto](#).

i 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.

Case ID 234567891 [Info](#) Resolve case

Case details

Subject Same issue is happening for my Amazon EC2 instances	Status Unassigned
Case ID 234567891	Severity General question
Created 2021-04-21T20:30:23.945Z	Category General Info and Getting Started
Case type Account	Additional contacts johndoe@example.com
Opened by janedoe@example.com	

Related cases

Subject	Case ID
Problem with EC2 instances	1234567890

Correspondence Reply

Jane Doe Wed Apr 21 2021 13:30:23 GMT-0700 (Pacific Daylight Time)	I keep getting an error for my EC2 instances. What do you recommend that I do to fix it?

Cronologia dei casi

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

Utilizzo Supporto AWS con un AWS SDK

AWS i kit di sviluppo software (SDKs) sono disponibili per molti linguaggi di programmazione popolari. 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 per C++	AWS SDK per C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK per Go	AWS SDK per Go esempi di codice
AWS SDK per Java	AWS SDK per Java esempi di codice
AWS SDK per JavaScript	AWS SDK per JavaScript esempi di codice
AWS SDK per Kotlin	AWS SDK per Kotlin esempi di codice
AWS SDK per .NET	AWS SDK per .NET esempi di codice
AWS SDK per PHP	AWS SDK per PHP esempi di codice
AWS Strumenti per PowerShell	AWS Strumenti per PowerShell esempi di codice
AWS SDK per Python (Boto3)	AWS SDK per Python (Boto3) esempi di codice
AWS SDK per Ruby	AWS SDK per Ruby esempi di codice
AWS SDK per Rust	AWS SDK per Rust esempi di codice
AWS SDK per SAP ABAP	AWS SDK per SAP ABAP esempi di codice
AWS SDK per Swift	AWS SDK per Swift esempi di codice

Esempio di disponibilità

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

Informazioni sull'API della console Support Center

L'API Support Center Console migliora la tua esperienza con la console Support Center. Di seguito sono riportati alcuni esempi delle funzionalità fornite dall'API della console Support Center:

- La possibilità di creare e aggiornare una bozza del caso di supporto
- La possibilità per la console del Support Center di visualizzare lo stato corrente del tuo account
- La possibilità per la console Support Center di visualizzare la guida dinamica per il servizio e la categoria selezionati

Per un elenco completo delle azioni fornite dall'API della console di Support Center, consulta la tabella in [Aggiungere policy IAM per le operazioni dell'API Support Center Console](#).

Important

Per continuare a utilizzare le funzioni incluse nell'API della console di Support Center, devi aggiungere le operazioni della console di Support Center alle tue AWS Identity and Access Management politiche prima del 2 novembre 2026. Dopo aver creato le policy IAM, aggiorna la policy Supporto AWS gestita per includere le `support-console:*` azioni. Per ulteriori informazioni, consulta [Aggiungere policy IAM per le operazioni dell'API Support Center Console](#).

Argomenti

- [Aggiungere policy IAM per le operazioni dell'API Support Center Console](#)
- [Test delle chiamate API della console del Support Center](#)

Aggiungere policy IAM per le operazioni dell'API Support Center Console

Prima del 2 novembre 2026, è necessario creare AWS Identity and Access Management politiche per le operazioni dell'API della console di Support Center. Se non crei queste politiche entro il 2 novembre 2026, riceverai `AccessDenied` degli errori.

Per aggiungere queste operazioni alle tue policy IAM, consulta [Create IAM policies \(console\)](#) nella Guida per l'AWS Identity and Access Management utente.

La tabella seguente riassume le operazioni della console.

 Note

Queste operazioni riguardano solo la console. Non sono disponibili per l'uso nell' AWS SDK o nel AWS CLI.

Operation	Livello di accesso	Description
GetAccountState	READ	Concede l'autorizzazione alla console per mostrare lo stato corrente dell'account.
GetAccountGovCloudEnabled	READ	Concede l'autorizzazione a determinare se l'account è GovCloud abilitato.
GetCaseDraft	READ	Concede l'autorizzazione alla console di mostrare la bozza del caso creata in precedenza.
CreateCaseDraft	WRITE	Concede l'autorizzazione a creare o aggiornare una bozza di caso per il tipo di caso specificato.
DeleteCaseDraft	WRITE	Concede l'autorizzazione a eliminare una bozza di caso per il tipo di caso specificato.
GetBanner	READ	Concede l'autorizzazione alla console di mostrare il Supporto banner visualizzato

Operation	Livello di accesso	Description
		durante gli eventi che hanno un impatto sui clienti.
DescribeDynamicHelp	READ	Concede l'autorizzazione alla console di mostrare risorse di aiuto dinamiche per il servizio e la categoria selezionati.
CreateContact	WRITE	Concede l'autorizzazione alla console per creare un contatto autenticato per il tipo di contatto selezionato.
CheckSubscription	READ	Concede l'autorizzazione alla console per verificare se l'account ha accesso al prodotto selezionato.
GetQuestionnaire	READ	Autorizza la console a mostrare il questionario di feedback dei clienti.
SaveFeedback	WRITE	Concede l'autorizzazione a salvare il feedback del questionario.

 Note

Se disponi di una configurazione VPN personalizzata, assicurati di configurare la VPN per inoltrare correttamente l'indirizzo IP del client all'endpoint API della console di Support Center. Quando utilizzi una VPN con AWS Identity and Access Management policy che includono [aws: SourceIp conditions](#), l'indirizzo IP del client specificato nella policy IAM deve essere inoltrato all'endpoint dell'API, non all'indirizzo IP della VPN. Se la VPN inoltra il proprio indirizzo IP anziché l'indirizzo IP del client, l'autorizzazione potrebbe non riuscire perché l'indirizzo IP non corrisponde alla `aws:SourceIp` condizione della policy IAM. La tabella seguente fornisce gli endpoint dell'API Support Center Console per Regione AWS.

Regione AWS	Endpoint dell'API Support Center Console
<code>https://api.us-east-1.prod.support-console.support.aws.dev</code>	Stati Uniti orientali (Virginia settentrionale)
<code>https://api.us-west-2.prod.support-console.support.aws.dev</code>	Stati Uniti occidentali (Oregon)
<code>https://api.eu-west-1.prod.support-console.support.aws.dev</code>	Europa (Irlanda)

Test delle chiamate API della console del Support Center

Per verificare che le chiamate API alla console funzionino, apri il [AWS Support Center Console](#). Se le chiamate non hanno esito positivo, viene visualizzato un banner che riporta gli errori.

È possibile utilizzarlo AWS CloudTrail per eseguire il debug delle chiamate API effettuate alla console del Support Center. L' CloudTrail evento per la chiamata API mostra se mancano delle policy IAM. Puoi anche esaminare i problemi di inoltro degli indirizzi IP confrontando gli indirizzi IP del browser con l'indirizzo IP del client in caso di evento. CloudTrail

Per visualizzare CloudTrail gli eventi relativi alle chiamate alla console del Support Center, completare i seguenti passaggi:

1. Accedi a Console di gestione AWS e apri la CloudTrail console all'indirizzo <https://console.aws.amazon.com/cloudtrail/>.
2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi). Viene visualizzato un elenco filtrato di eventi con gli eventi più recenti visualizzati per primi. Il filtro predefinito per gli eventi è di Read-only (Sola lettura), impostato su false (Falso). Per cancellare il filtro, scegli X a destra del filtro.

3. Scegli la fonte dell'evento `support-console.amazonaws.com`. Nella pagina dei dettagli dell'evento, è possibile visualizzare i dettagli dell'evento, visualizzare le risorse di riferimento e visualizzare il record dell'evento.

Informazioni sull' Supporto AWS API

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

L' Supporto AWS API fornisce l'accesso ad alcune funzionalità del [AWS Support Center](#).

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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations per utilizzare l' API Supporto AWS. Per ulteriori informazioni, consulta [Supporto](#).

Per ulteriori informazioni sulle operazioni e sui tipi di dati forniti da Supporto, consulta l'[Supporto AWS API Reference](#).

Argomenti

- [Gestione dei casi di supporto](#)
- [AWS Trusted Advisor](#)
- [Endpoints](#)
- [Support in AWS SDKs](#)

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' Supporto AWS API supporta la CloudTrail registrazione per le operazioni di gestione dei casi di supporto. Per ulteriori informazioni, consulta [Registrazione delle chiamate Supporto AWS API con AWS CloudTrail](#).

Per esempi di codice che dimostrano come gestire l'intero ciclo di vita di un caso di supporto, vedi [Esempi di codice per Supporto l'utilizzo AWS SDKs](#) di..

AWS Trusted Advisor

È possibile utilizzare le Trusted Advisor operazioni per eseguire le seguenti attività:

- Ottieni i nomi e gli identificatori per i controlli Trusted Advisor
- Richiedi l'esecuzione di un Trusted Advisor controllo sul tuo AWS account e sulle tue risorse
- Ottieni riepiloghi e informazioni dettagliate sui risultati dei Trusted Advisor controlli
- Aggiorna i tuoi assegni Trusted Advisor
- Ottieni lo stato di ogni assegno Trusted Advisor

L' Supporto AWS API supporta CloudTrail la registrazione Trusted Advisor delle operazioni. Per ulteriori informazioni, consulta [AWS Trusted Advisor informazioni relative alla registrazione CloudTrail](#).

Puoi utilizzare Amazon CloudWatch Events per monitorare le modifiche ai risultati del controllo di Trusted Advisor. Per ulteriori informazioni, consulta [Monitoraggio dei risultati dei AWS Trusted Advisor controlli con Amazon EventBridge](#).

Ad esempio, codice Java che dimostra come utilizzare le Trusted Advisor operazioni, vedi [Utilizzo Trusted Advisor come servizio web](#).

Endpoints

Supporto 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'endpoint 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 i seguenti endpoint per l'API: Supporto

- 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 richiami l'[CreateCase](#)operazione 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'[ResolveCase](#)operazione per risolverlo.
- Per chiamare le AWS Trusted Advisor operazioni nell' Supporto AWS API, devi utilizzare l'endpoint degli Stati Uniti orientali (Virginia settentrionale). Attualmente, gli endpoint degli Stati Uniti occidentali (Oregon) e dell'Europa (Irlanda) non supportano le operazioni. Trusted Advisor

Per ulteriori informazioni sugli AWS endpoint, consulta [Supporto AWS endpoint](#) e quote nel. Riferimenti generali di Amazon Web Services

Support in AWS SDKs

I AWS Command Line Interface (AWS CLI) e i AWS Software Development Kit (SDKs) includono il supporto per l' Supporto API.

Per un elenco delle lingue che supportano l' Supporto AWS API, scegliete il nome di un'operazione, ad esempio [CreateCase](#), e nella sezione [Vedere anche](#), scegliete la lingua preferita.

Supporto AWS Piani

AWS offre i seguenti Supporto AWS piani tra cui scegliere in base alle esigenze aziendali.

- Di base
- AWS Supporto aziendale+
- AWS Supporto aziendale
- AWS Operazioni unificate

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise.](#)

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

Argomenti

- [Caratteristiche dei piani Supporto AWS](#)
- [Che cosa sono le operazioni unificate AWS](#)
- [Piani di modifica Supporto AWS](#)
- [Configura le notifiche di scadenza del piano promozionale](#)
- [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#)

Caratteristiche dei piani Supporto AWS

Basic Support offre assistenza per domande relative all'account e alla fatturazione e per gli aumenti delle quote 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:

- One-on-one risposte a 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 con un piano Business Support+ hanno accesso a queste funzionalità aggiuntive:

- Risposte contestuali e in tempo reale tramite l'intelligenza artificiale generativa.
- Accesso via telefono, web e chat 24 ore su 24, 7 giorni su 7 ai tecnici del Cloud Support.
- Meno di 30 minuti di coinvolgimento umano per i casi di inattività dei sistemi aziendali critici.
- Più di 500 controlli con [AWS Trusted Advisor](#).
- L'API Supporto AWS per interagire con Support Center e Trusted Advisor. È possibile utilizzare l'API Supporto AWS 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.
- Supporta un numero illimitato di casi di supporto che possono essere aperti da qualsiasi utente con [autorizzazioni](#).

I clienti con un piano Enterprise Support hanno tutti i vantaggi disponibili con il piano AWS Business Support+, oltre ai seguenti vantaggi aggiuntivi:

- Un Technical Account Manager (TAM) designato.
- Risposta ai casi critici per la produzione fino a 15 minuti.
- Access to [AWS Security Incident Response](#), un servizio che ti aiuta a prepararti, rispondere e ricevere rapidamente indicazioni per aiutarti a riprenderti dagli incidenti di sicurezza. Ciò include incidenti come acquisizione di account, violazioni di dati e attacchi ransomware.
- Revisioni aziendali strategiche con esperti. AWS
- Accesso alla gestione degli eventi AWS Countdown. AWS Countdown fornisce un supporto specializzato guidato da TAM per aiutarvi ad avere successo durante gli eventi aziendali critici.

I clienti con un piano AWS Unified Operations hanno accesso ai seguenti vantaggi. Per i dettagli sul piano AWS Unified Operations, inclusi i dettagli sull'onboarding e le informazioni introduttive, consulta [Che cosa sono le operazioni unificate AWS](#)

- 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 termine con Supporto AWS per ottenere informazioni dettagliate del caso d'uso. Dopo l'analisi, fornisci le indicazioni sull'architettura e sul dimensionamento per un evento.
- AWS Technical Account Manager (TAM) e Domain Specialist Engineer (DSE) designati per casi d'uso e applicazioni specifici.
- [Un abbonamento periodico a Countdown Premium.AWS](#)
- Revisioni dei carichi di lavoro critici e runbook e procedure operative personalizzati.

Per ulteriori informazioni sulle funzionalità e sui prezzi di ciascun piano di supporto, [consulta Supporto AWS e Confronta Supporto AWS 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.

Note

[Se lavori con un AWS partner e desideri saperne di più sull'assistenza gestita dai partner, consulta AWS Partner-Led Support](#)

Che cosa sono le operazioni unificate AWS

AWS Unified Operations combina una comprovata esperienza con informazioni basate sull'intelligenza artificiale per contribuire a ridurre i rischi operativi e di sicurezza, risolvere i problemi più rapidamente e aiutarti a progettare soluzioni cloud più resilienti sin dall'inizio, accelerando le iniziative cloud più critiche. AWS Gli specialisti designati agiscono come un'estensione del tuo team attraverso i tuoi canali di collaborazione preferiti, conducendo revisioni del carico di lavoro, fornendo indicazioni strategiche e ottimizzando le prestazioni attraverso una profonda conoscenza del contesto. Grazie al monitoraggio della sicurezza e delle prestazioni 24 ore su 24, 7 giorni su 7, rileviamo e mitigiamo tempestivamente gli incidenti, riducendo al contempo il volume degli avvisi. Una risposta di cinque minuti, sensibile al contesto, per gli incidenti critici riduce ulteriormente i tempi di risoluzione e aiuta a mantenere le massime prestazioni operative.

AWS Prezzi di Unified Operations

AWS I prezzi di Unified Operations si basano sui requisiti specifici e sulla complessità del carico di lavoro. Per informazioni dettagliate sui prezzi, consulta [Supporto AWS Plan Pricing](#).

Indice

- [Vantaggi delle operazioni unificate](#)
- [Team operativo unificato](#)
 - [Responsabile tecnico degli account](#)
 - [Ingegnere specializzato in dominio](#)
 - [Specialista senior in fatturazione e account](#)
 - [Ingegnere della gestione degli incidenti](#)
 - [Ingegnere specializzato in migrazioni ed eventi](#)

- [AWS Team di risposta agli incidenti con i clienti](#)
- [Tecnico di supporto specializzato](#)
- [Ciclo di vita delle operazioni unificate](#)
 - [Preonboarding di Unified Operations](#)
 - [Onboarding delle operazioni unificate](#)
 - [Operazioni unificate Pianificazione preliminare o della migrazione](#)
 - [Unified Operations: migrazione o cutover degli eventi](#)
 - [Unified Operations dopo il Go-live o l'evento](#)
 - [Gestione degli incidenti di Unified Operations Workload](#)
 - [Operazioni unificate dopo l'incidente](#)
 - [Operazioni unificate Miglioramento continuo](#)
- [Guida introduttiva a Unified Operations](#)
 - [Operazioni unificate Guida introduttiva: prerequisiti](#)
 - [Operazioni unificate Guida introduttiva: integra gli allarmi critici per una rapida gestione degli incidenti](#)
 - [Unified Operations Guida introduttiva: come richiedere una risposta agli incidenti in 5 minuti](#)
 - [Operazioni unificate Guida introduttiva: piano per la copertura del dominio](#)
 - [Operazioni unificate Guida introduttiva: integra il tuo account per una gestione proattiva degli incidenti di sicurezza](#)
 - [Operazioni unificate Guida introduttiva: AWS le vostre aspettative](#)
 - [Operazioni unificate Guida introduttiva: cosa puoi aspettarti da AWS](#)

Vantaggi delle operazioni unificate

Unified Operations offre diversi vantaggi chiave.

- **AWS Esperti designati:** il tuo AWS team include Technical Account Manager designati (TAMs), AWS Domain Specialist Engineer e Senior Billing and Account Specialist. Il tuo AWS team si integra con i tuoi strumenti di collaborazione come Slack o Microsoft Teams.
- **Guida tecnica approfondita:** il tuo AWS team ti aiuta a rafforzare la resilienza attraverso approfondimenti specifici delle applicazioni, valutazioni di preparazione, supporto guidato ai test e runbook personalizzati su misura per il tuo ambiente. Il tuo AWS team offre una gestione finanziaria incentrata sul carico di lavoro e allinea strategicamente i costi agli obiettivi aziendali.

- Migrazioni, eventi e supporto al lancio: accelera le migrazioni critiche al cloud e gli eventi aziendali con AWS tecnici designati che aiutano a mitigare i rischi in modo proattivo, guidandoti dalla pianificazione all'esecuzione. Assistenza in tempo reale per eventi programmati, aumento della velocità di migrazione e lanci di successo.
- Monitoraggio proattivo del carico di lavoro 24 ore su 24, 7 giorni su 7: integra allarmi a livello di applicazione e infrastruttura grazie agli strumenti esistenti AWS e di terze parti per rilevare segnali di allarme precoce e promuovere una mitigazione proattiva con il team.
- Coinvolgi i responsabili AWS degli incidenti entro 5 minuti in caso di problemi di inattività del sistema critici per l'azienda: ricevi supporto proattivo dai tecnici della gestione degli incidenti entro 5 minuti da allarmi, avvisi sul carico di lavoro o problemi di inattività del sistema critici per l'azienda.
- Risposta al caso specifico: accesso a tecnici di supporto sensibili al contesto per promuovere la risoluzione degli incidenti. Runbook e playbook di risposta agli incidenti personalizzati per i flussi di lavoro, che semplificano la diagnosi e la risoluzione dei problemi in base alle esigenze aziendali specifiche.
- Guida e supporto in materia di sicurezza: monitoraggio proattivo degli eventi di sicurezza con analisi e indagini automatizzate, oltre all'accesso 24 ore su 24, 7 giorni su 7 al AWS Customer Incident Response Team per prepararsi, rispondere e ripristinare gli eventi di sicurezza nel vostro ambiente. AWS

Team operativo unificato

AWS Unified Operations riunisce un team designato di esperti specializzati che collaborano per supportare il tuo percorso verso il cloud. Ogni ruolo è progettato con cura per fornire una copertura completa in tutte le dimensioni tecniche, finanziarie, operative e di sicurezza dell'ambiente cloud. Dalla guida strategica al supporto tecnico, dall'ottimizzazione finanziaria alla risposta rapida agli incidenti, questi esperti agiscono come un'estensione del team, disponibili 24 ore su 24, 7 giorni su 7 per garantire che le operazioni cloud vengano eseguite in modo efficiente e sicuro.

Indice

- [Responsabile tecnico degli account](#)
- [Ingegnere specializzato in dominio](#)
- [Specialista senior in fatturazione e account](#)
- [Ingegnere della gestione degli incidenti](#)
- [Ingegnere specializzato in migrazioni ed eventi](#)
- [AWS Team di risposta agli incidenti con i clienti](#)

- [Tecnico di supporto specializzato](#)

Responsabile tecnico degli account

Lo stratega del cloud designato, il Technical Account Manager (TAM), orchestra il coinvolgimento complessivo e favorisce i risultati aziendali. TAMs dirige la pianificazione strategica, conduce revisioni aziendali trimestrali, fornisce indicazioni sulla resilienza e si coordina tra team specializzati per garantire il successo delle iniziative cloud. Rappresentano il punto di contatto principale per le escalation e le decisioni strategiche.

Ingegnere specializzato in dominio

Un Domain Specialist Engineer (DSE) è un esperto tecnico che conosce a fondo l'architettura specifica del carico di lavoro e. Servizi AWS DSEs condurre revisioni critiche del carico di lavoro, creare documentazione tecnica, sviluppare guide alla risoluzione dei problemi e fornire consulenza tecnica continua. Analizzano gli incidenti per prevenirne il ripetersi e mantengono la condivisione globale delle conoscenze per garantire una qualità del supporto costante.

Specialista senior in fatturazione e account

Il Senior Billing and Account Specialist (SBAS) è un esperto designato di ottimizzazione finanziaria che aiuta a bilanciare prestazioni e costi. Gestiscono le strategie di ottimizzazione dei costi, supervisionano i portafogli di istanze riservate e i piani di risparmio, conducono revisioni finanziarie delle attività e forniscono analisi dettagliate delle spese per massimizzare l'efficienza degli investimenti nel cloud.

Ingegnere della gestione degli incidenti

Gli Incident Management Engineer (IME) sono specialisti della risposta rapida che coordinano la risoluzione degli incidenti critici. IMEs forniscono tempi di risposta di 5 minuti, orchestrano i team tecnici durante gli incidenti, gestiscono le comunicazioni con le parti interessate. Durante gli incidenti attivi, IMEs conduci valutazioni in tempo reale della gestione degli incidenti e dell'efficacia della risposta. Su richiesta, documentano la sequenza degli eventi, le decisioni prese e i risultati immediati. Osservano e valutano l'esecuzione dei protocolli di risposta, il coordinamento del team e l'applicazione dei playbook esistenti mentre l'incidente è ancora in corso.

Ingegnere specializzato in migrazioni ed eventi

Esperti on-demand che guidano transizioni critiche come lanci e migrazioni. Convalidano le architetture, creano piani di esecuzione dettagliati, forniscono il monitoraggio in tempo reale durante

gli eventi e conducono analisi post-evento per acquisire conoscenze e ottimizzare le operazioni future.

AWS Team di risposta agli incidenti con i clienti

Il AWS Customer Incident Response Team (CIRT) è composto da esperti di sicurezza che forniscono assistenza specializzata 24 ore su 24, 7 giorni su 7 per eventi di sicurezza. Monitorano i risultati di sicurezza, forniscono una risposta guidata entro pochi minuti dal rilevamento e migliorano le capacità operative di sicurezza attraverso il supporto investigativo di esperti e linee guida sulle migliori pratiche.

Tecnico di supporto specializzato

Gli Specialist Support Engineer (SSE) sono esperti tecnici di grande esperienza che utilizzano strumenti contestuali avanzati per fornire soluzioni di supporto precise. Sfruttano i sistemi basati sull'intelligenza artificiale e una conoscenza tecnica approfondita per comprendere rapidamente l'ambiente e risolvere sfide tecniche complesse.

Ciclo di vita delle operazioni unificate

Il piano Unified Operations Support contiene diverse fasi, dal pre-onboarding al miglioramento continuo, che ti aiutano a ottenere il massimo dal tuo ambiente cloud. Questo argomento tratta i punti chiave di ogni fase.

Indice

- [Preonboarding di Unified Operations](#)
- [Onboarding delle operazioni unificate](#)
- [Operazioni unificate Pianificazione preliminare o della migrazione](#)
- [Unified Operations: migrazione o cutover degli eventi](#)
- [Unified Operations dopo il Go-live o l'evento](#)
- [Gestione degli incidenti di Unified Operations Workload](#)
- [Operazioni unificate dopo l'incidente](#)
- [Operazioni unificate Miglioramento continuo](#)

Preonboarding di Unified Operations

Durante le fasi di pre-onboarding, AWS raccoglie le informazioni necessarie per avviare il processo di onboarding, incluse le seguenti informazioni:

Scoperta dell'ambiente e convalida tecnica

- Comprensione dell'architettura del carico di lavoro e della chiave. Servizi AWS
- Le tue esigenze di pianificazione future, come la migrazione o gli eventi.
- Prerequisiti, come un elenco dei tuoi Account AWS e. Regioni AWS
- Le tue esigenze aziendali specifiche.

Onboarding delle operazioni unificate

Inizio dell'onboarding

- Incontra il team (cliente e AWS risorse assegnate).

Workshop di onboarding

- Identifica i carichi di lavoro critici.
- Esegui una revisione approfondita dell'architettura dei carichi di lavoro.
- Rivedi i ruoli e le responsabilità (revisione RACI AWS e i tuoi ruoli e responsabilità).
- Rivedi i flussi di lavoro di gestione degli incidenti e delle modifiche (ITSM).
- Protocollo di comunicazione: strumenti e processi, percorso di escalation, pianificazioni delle chiamate
- Identifica e definisci gli allarmi critici (in Amazon CloudWatch, nel tuo APM di terze parti o nello strumento di monitoraggio personalizzato).
- Crea runbook per allarmi critici.

Onboarding del servizio

- Il tuo Account AWS onboarding a. AWS Security Incident Response
- Attivazione degli allarmi critici per una rapida gestione degli incidenti.

Operazioni unificate Pianificazione preliminare o della migrazione

La pianificazione preliminare o della migrazione in AWS Unified Operations include i seguenti elementi chiave.

- Raccolta del contesto: individuazione e architettura del carico di lavoro.
- Operational Readiness Review (ORR): valutazione sistematica sulla base di AWS best practice e runbook per identificare potenziali problemi prima che abbiano un impatto sull'evento.
- Valutazioni dei rischi: identificazione, elenco dei rischi potenziali e piani di mitigazione.
- Rivedi gli eventi: assicurati il supporto per gli eventi di cut-over o di migrazione.

Unified Operations: migrazione o cutover degli eventi

La migrazione o il cutover degli eventi in Unified Operations include i seguenti elementi chiave.

- Un ponte verso la risoluzione in tempo reale: AWS gli esperti si uniscono ai vostri canali di comunicazione per monitorare gli eventi e risolvere i problemi durante i periodi lavorativi critici.
- Supporto completo 24 ore su 24, 7 giorni su 7: assistenza Round-the-clock esperta con guida immediata per le esigenze di scalabilità delle risorse.
- AWS progettazione: collabora direttamente con ingegneri che conoscono la vostra attività, offrendo soluzioni su misura.

Unified Operations dopo il Go-live o l'evento

Il processo post-go-live o post-evento in Unified Operations include i seguenti elementi chiave:

- Riduzione del coinvolgimento e risorse specifiche per gli eventi.
- Conduci revisioni degli eventi.
- Aggiorna i runbook e la documentazione in base agli apprendimenti.
- Esegui retrospettive per identificare le aree di miglioramento.

Gestione degli incidenti di Unified Operations Workload

La gestione degli incidenti relativi al carico di lavoro include i seguenti elementi chiave:

- Supporto AWS creazione di casi.

- Collaborazione con te e con un AWS Incident Management Engineer (IME) per una gestione degli incidenti basata sul contesto.
- Partecipazione o creazione di una chiamata bridge relativa agli incidenti.
- Monitoraggio dello Servizio AWS stato di salute e di eventi su larga scala (LSE).
- Ripristino rapido di applicazioni o carichi di lavoro critici.

Operazioni unificate dopo l'incidente

L'analisi post-incidente degli incidenti critici viene condotta dal Domain Specialist Engineer (DSE) assegnato. Dopo la risoluzione, DSE adotta un approccio analitico più ampio, conducendo un'analisi completa delle cause alla radice per identificare eventuali lacune nei processi o negli strumenti. Il DSE trasforma le informazioni in miglioramenti attuabili aggiornando i playbook di risposta, consigliando misure preventive e suggerendo miglioramenti dell'architettura per aiutare a prevenire incidenti simili in futuro.

Operazioni unificate Miglioramento continuo

Il miglioramento continuo include i seguenti elementi chiave:

- Aggiorna le revisioni critiche dei carichi di lavoro, proponendo raccomandazioni AWS specifiche per i servizi e linee guida sulla resilienza.
- Esamina continuamente i casi vecchi e nuovi e fornisci guide per la risoluzione dei problemi tecnici identificati.
- Applica le lezioni e supervisiona le implementazioni e i test.
- Discuti di problemi tecnici, configurazioni, progetti e traguardi passati e futuri.
- Rivedi i piani di implementazione di nuove funzionalità con valutazioni dei rischi e ottimizzazioni delle prestazioni.
- Effettua una revisione aziendale mensile o trimestrale (MBR/QBR).

Guida introduttiva a Unified Operations

In questo argomento vengono descritti i passaggi necessari per l'integrazione di Unified Operations. AWS

Indice

- [Operazioni unificate Guida introduttiva: prerequisiti](#)

- [Operazioni unificate Guida introduttiva: integra gli allarmi critici per una rapida gestione degli incidenti](#)
- [Unified Operations Guida introduttiva: come richiedere una risposta agli incidenti in 5 minuti](#)
- [Operazioni unificate Guida introduttiva: piano per la copertura del dominio](#)
- [Operazioni unificate Guida introduttiva: integra il tuo account per una gestione proattiva degli incidenti di sicurezza](#)
- [Operazioni unificate Guida introduttiva: AWS le vostre aspettative](#)
- [Operazioni unificate Guida introduttiva: cosa puoi aspettarti da AWS](#)

Operazioni unificate Guida introduttiva: prerequisiti

I seguenti elementi sono necessari per l'onboarding di Unified Operations AWS

Un contratto AWS Unified Operations firmato. Per ulteriori informazioni, contattate il vostro rappresentante AWS di vendita.

- Esigenze aziendali identificate, come migrazione, modernizzazione, eventi, uptime previsto e così via.
- Un elenco dei tuoi carichi di lavoro.
- Un elenco dei tuoi Account AWS e dei tuoi associati Regioni AWS.
- Stakeholder identificati tra i team addetti alle applicazioni, all'architettura, alle operazioni e alla sicurezza.

Operazioni unificate Guida introduttiva: integra gli allarmi critici per una rapida gestione degli incidenti

Per aiutarti a notificare rapidamente gli incidenti critici, completa i seguenti passaggi per integrare gli allarmi in Incident Detection and Response AWS

1. Definisci e configura gli allarmi critici per una rapida gestione degli incidenti. Per informazioni dettagliate, consulta [Definizione e configurazione degli allarmi in Incident Detection and Response](#) nella Incident Detection and Response User Guide.
 - a. Per i passaggi per configurare gli allarmi con Amazon CloudWatch, consulta [Definisci e configura gli allarmi in Incident Detection and Response nella Incident](#) Detection and Response User Guide. Per AWS consigli sui diversi tipi di allarmi critici Servizi AWS,

consulta [Incident Detection and Response \(IDR\)](#). Contatta il tuo team AWS Unified Operations se desideri AWS automatizzare la creazione di AWS allarmi critici per le risorse contrassegnate. AWS

- b. Per reindirizzare o importare allarmi critici da strumenti APM di terze parti con [EventBridge integrazione diretta di Amazon](#), ad esempio, e così via DataDog NewRelic, consulta la sezione Inserimento di [allarmi con integrazione diretta con Amazon EventBridge nella AWS Incident APMs Detection](#) and Response User Guide. È necessario implementare un set di AWS risorse (AWS Lambda e regole Amazon EventBridge Event Bus) per trasformare e reindirizzare l'allarme (evento) verso AWS Incident Detection and Response. Il tuo team AWS Unified Operations può aiutarti a fornire il CloudFormation modello per installare queste risorse.
 - c. Reindirizza o inserisci allarmi critici dal tuo strumento di monitoraggio personalizzato tramite uno strumento APM di terze parti che non ha un'integrazione diretta con Amazon. EventBridge Per ulteriori informazioni, consulta [Usare i webhook per inserire allarmi APMs senza integrazione diretta con Amazon EventBridge nella AWS Incident Detection and Response](#) User Guide. È necessario implementare una serie di AWS risorse (AWS Lambda funzioni API Gateway e regole del bus di EventBridge eventi Amazon) per trasformare e reindirizzare l'allarme (evento) a AWS Incident Detection and Response. Il tuo team AWS Unified Operations può aiutarti a fornire il CloudFormation modello per installare queste risorse.
2. Fornisci dettagli sull'architettura del carico di lavoro, informazioni sui punti di contatto e informazioni sul runbook sulle azioni di mitigazione degli allarmi critici. Per farlo, completa le seguenti fasi.
 - [Scarica e completa il questionario di onboarding del carico di lavoro di rilevamento e risposta agli AWS incidenti per ogni carico di lavoro o applicazione critica e il questionario di inserimento degli allarmi relativo a ciascun carico di lavoro unico.](#)

Le informazioni contenute in questi questionari aiutano il team a sviluppare un manuale per la risoluzione degli incidenti. AWS Questo runbook consente di intraprendere le azioni appropriate per risolvere rapidamente i problemi e correggere gli allarmi critici prima che causino interruzioni aziendali. Per esempi e informazioni di esempio, consulta i questionari sull'[onboarding del carico di lavoro e sull'inserimento degli allarmi in Incident Detection and Response](#). AWS

3. Fornisci l'accesso agli allarmi critici integrati al rilevamento e alla risposta agli incidenti AWS

- a. Implementa il ruolo `AWSServiceRoleForHealth_EventProcessor` collegato al servizio (SLR) nell' Account AWS esecuzione del carico di lavoro critico, affinché venga monitorato dal team di gestione degli incidenti. AWS Per ulteriori informazioni, consulta [Fornire l'accesso per l'inserimento degli avvisi in Incident Detection and Response](#). AWS

 Note

Per aiutarvi nell'onboarding di grandi dimensioni Account AWS, AWS possiamo fornirvi uno AWS Command Line Interface script per velocizzare la fornitura di questa reflex.

- b. (Facoltativo) Se i tuoi allarmi sono in Amazon CloudWatch, assicurati che l' AWS Identity and Access Management utente o il ruolo utilizzato per il test degli allarmi (prima del lancio) disponga dell'autorizzazione `cloudwatch:SetAlarmState` IAM nel tuo account Account AWS che esegue il carico di lavoro critico. È necessario per i test degli allarmi (gameday) dopo l'onboarding. Per ulteriori informazioni, consulta [Test dei carichi di lavoro integrati in Incident Detection and Response](#). AWS
4. Crea un Supporto AWS caso per sottoscrivere un carico di lavoro per una rapida gestione degli incidenti. Tieni presente che il tuo Account AWS è abilitato automaticamente alla gestione rapida degli incidenti in entrata, il che significa che puoi inoltrare un caso alla coda Unified Operations Incident Detection and Response tramite la console Support Center AWS Command Line Interface, l' o l' AWS SDK per un'azione rapida. AWS Per monitorare e creare incidenti in modo proattivo con un caso in uscita, crea un Supporto AWS caso per il tuo carico di lavoro critico. Supporto AWS Per farlo, completa le seguenti fasi.
 - a. Accedi a [AWS Support Center Console](#), seleziona Crea caso, quindi seleziona Supporto tecnico.
 - b. Per Assistenza, seleziona Incident Detection and Response.
 - c. Per Categoria, seleziona Nuovo carico di lavoro integrato.
 - d. Per Severità seleziona Linee guida generali.
 - e. In allegato i questionari Workload e Alarm che hai completato nel passaggio precedente.

Unified Operations Guida introduttiva: come richiedere una risposta agli incidenti in 5 minuti

AWS Unified Operations offre una risposta agli incidenti critici in 5 minuti. Per richiedere una risposta in entrata di 5 minuti, puoi [creare un caso di supporto da un'interazione di supporto](#) o utilizzare il metodo di creazione dei [casi di supporto legacy](#). Quando crei il tuo caso, assicurati di inserire le seguenti informazioni per assicurarti che il caso riceva una risposta entro 5 minuti:

1. Per Tipo di caso, scegli Tecnico.
2. Per Assistenza, scegli AWS Incident Detection and Response.
3. Per Categoria, scegli Active Incident.
4. Per Severità, scegli Business-critical system down.
5. Nella descrizione, includi le seguenti informazioni
 - a. Informazioni tecniche
 - Nome del carico di lavoro
 - ARN della AWS risorsa interessata
 - b. Informazioni aziendali
 - Descrizione dell'impatto sull'attività
 - (Facoltativo) Dettagli del Customer Bridge

Operazioni unificate Guida introduttiva: piano per la copertura del dominio

AWS Unified Operations offre competenze specializzate attraverso un approccio di copertura basato sul dominio. Ogni dominio è supportato da un team di specialisti di AWS dominio che forniscono i seguenti servizi:

- Competenze specializzate allineate alle aree tecnologiche specifiche.
- Copertura continua con disponibilità tramite i tuoi strumenti di collaborazione preferiti (Slack o Microsoft Teams) durante i giorni lavorativi.
- Guida proattiva sull'architettura, le migliori pratiche e le opportunità di ottimizzazione.
- Risposta migliorata agli incidenti grazie a una conoscenza approfondita del dominio e alla familiarità con i carichi di lavoro.
- Esperienza costante gestita da un team coordinato anziché da singoli individui.

Questo approccio alla copertura del dominio consente agli AWS specialisti di mantenere una profonda familiarità con i carichi di lavoro critici, fornendo al contempo un supporto completo per tutto lo stack tecnologico.

Per selezionare i domini, le organizzazioni mantengono l'autorità decisionale scegliendo tra 23 AWS domini e prendono in considerazione i seguenti fattori nella loro decisione:

- Servizi AWS Esecuzione principale di carichi di lavoro critici
- Servizio AWS Dipendenze critiche (come Amazon EC2, Amazon EKS o Amazon RDS)
- Principali eventi imminenti che richiedono una copertura di supporto 24 ore su 24, 7 giorni su 7 (migrazioni, lanci) pianificati entro 3-6 mesi

Queste informazioni, combinate con le indicazioni del vostro Technical Account Manager, consentono un allineamento preciso delle competenze di settore con le esigenze organizzative specifiche, aiutandovi a mantenere un supporto ottimale per i carichi di lavoro mission critical.

Operazioni unificate Guida introduttiva: integra il tuo account per una gestione proattiva degli incidenti di sicurezza

Unified Operations ti dà il diritto di aiutarti AWS Security Incident Response a prepararti, rispondere e riprenderti rapidamente dagli incidenti di sicurezza, come l'acquisizione di account, le violazioni dei dati e gli attacchi ransomware. AWS Security Incident Response valuta i risultati, analizza gli eventi e gestisce i casi critici, fornendo al contempo l'accesso al AWS Customer Incident Response Team (CIRT) per indagare sulle risorse interessate. Questo accesso consente di mitigare e risolvere efficacemente gli incidenti di sicurezza, riducendo al minimo l'impatto sulle operazioni. Per accedere a questa funzionalità di servizio, completa i seguenti passaggi:

1. Crea un modulo centralizzato Account AWS per. AWS Security Incident Response Account AWS Verrà utilizzato per configurare tutti gli altri Account AWS elementi che desideri monitorare, per gestire il team di risposta agli incidenti e per creare e visualizzare eventi di sicurezza. Ti consigliamo di allineare questo account con l'account che utilizzi per altri servizi di sicurezza come Amazon GuardDuty e AWS Security Hub CSPM. Puoi utilizzare un account di [AWS Organizations](#) gestione o un account amministratore AWS Organizations delegato come account di iscrizione a Security Incident Response. Per ulteriori informazioni, consulta [Selezione di un account di iscrizione](#) nella Guida per l'AWS Security Incident Response utente.
 - a. Scegli i dettagli di base dell'iscrizione. Per ulteriori informazioni, consulta [i dettagli dell'iscrizione alla configurazione](#) nella Guida AWS Security Incident Response per l'utente.

- b. Scegli come vuoi associare gli account a AWS Organizations. Per ulteriori informazioni, consulta [Associare gli account a AWS Organizations](#) nella Guida AWS Security Incident Response per l'utente.
 - c. (Facoltativo) Facoltativamente, puoi abilitare il flusso di lavoro di risposta proattiva e classificazione degli avvisi per consentire all'interno della tua organizzazione di monitorare e analizzare gli avvisi generati da Amazon e dalle integrazioni. GuardDuty AWS Security Hub CSPM Per ulteriori informazioni, consulta [Configurare i flussi di lavoro di risposta proattiva e di valutazione degli avvisi nella Guida per l'utente](#).AWS Security Incident Response
2. (Facoltativo) Abilita il contenimento proattivo di un potenziale incidente di sicurezza. AWS può eseguire azioni di contenimento per mitigare rapidamente l'impatto, come isolare gli host compromessi o ruotare le credenziali. Per attivare questa funzionalità, è necessario innanzitutto concedere le autorizzazioni necessarie al servizio. Per fare ciò, implementa un [Step Functions StackSet](#).

Operazioni unificate Guida introduttiva: AWS le vostre aspettative

Affinché le Unified Operations offrano il massimo valore, consigliamo il seguente approccio collaborativo:

Coinvolgimento del team

- Identifica gli esperti in materia del tuo team per collaborare con AWS gli ingegneri durante l'onboarding e il coinvolgimento continuo.
- Partecipa alle chiamate di esplorazione iniziali e alle riunioni successive per condividere i dettagli dell'architettura e i requisiti operativi.
- Stabilisci punti di contatto regolari per rivedere gli aggiornamenti dell'architettura o le modifiche del carico di lavoro.

Integrazione operativa

- Configura gli allarmi critici nel tuo account per consentire una gestione efficace degli incidenti.
- Implementa le azioni consigliate fornite dagli AWS specialisti,
- Partecipa alle esercitazioni della giornata di gioco per convalidare i processi di risposta agli incidenti.

Questo framework collaborativo consente di massimizzare il valore delle operazioni unificate, raggiungere gli obiettivi di uptime, mitigare i rischi operativi e ricevere un supporto completo per i carichi di lavoro mission critical.

Operazioni unificate Guida introduttiva: cosa puoi aspettarti da AWS

Quando entri a far parte di Unified Operations, puoi aspettarti quanto segue da AWS

- Mettete a disposizione un team di AWS esperti designati con competenze tecniche approfondite nel dominio e nei servizi del vostro carico di lavoro.
- Offri indicazioni proattive, ottimizzazione continua e consigli di miglioramento continuo per migliorare le prestazioni e la resilienza dei carichi di lavoro e accelerare il percorso verso le migrazioni e la modernizzazione.
- Contribuisci a fornire una risposta rapida agli incidenti, con tecnici attenti al contesto che intervengono entro 5 minuti dall'incidente critico.
- Offri un supporto completo per tutto il ciclo di vita dell'applicazione, dalla progettazione e migrazione all'avvio della produzione e alle operazioni a lungo termine.
- Monitora in modo proattivo le minacce alla sicurezza con il triaging automatico, riducendo i falsi positivi e aumentando gli incidenti per potenziali incidenti di sicurezza.
- Fornisci assistenza nella risoluzione dei problemi e nella mitigazione congiunta degli incidenti di sicurezza identificati o identificati. AWS

Piani di modifica Supporto AWS

Puoi utilizzare la console Supporto AWS 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). Per ulteriori informazioni, consultare [Gestisci l'accesso ai piani Supporto AWS](#) e [AWS politiche gestite per Supporto AWS Plans](#).

Per modificare il piano di supporto

1. Accedi alla console Supporto AWS Plans all'indirizzo <https://console.aws.amazon.com/support/plans/home>.
2. (Facoltativo) Per confrontare i piani di supporto, nella pagina Supporto AWS Piani, scegli Confronta tutti i Supporto piani e le funzionalità.

3. (Facoltativo) Per visualizzare i costi stimati per un piano di supporto, scegli il calcolatore dei prezzi. Nel calcolatore dei prezzi, seleziona un livello di supporto, inserisci una stima di quanto pensi di spendere per AWS ogni mese, quindi scegli Calcola.
4. Per effettuare il downgrade del piano Enterprise Support, contatta il Technical Account Manager (TAM).

Per effettuare il downgrade del piano Business Support+, nella pagina Gestisci [i piani di supporto](#), scegli Rivedi il downgrade nella sezione Piano di base Supporto .

Per passare a un piano AWS Enterprise Support o AWS Unified Operations, scegli Contatta l'ufficio vendite.

Per passare a un piano AWS Business Support+ da Basic Supporto, completa i seguenti passaggi:

- a. Scegli Inizia nella sezione AWS Business Support+.
- b. Se hai effettuato l'onboarding AWS Organizations e hai abilitato la modalità con tutte le funzionalità, puoi iscrivere l'intera organizzazione a Business Support+. Per informazioni sulla modalità con tutte le funzionalità, consulta [Abilitazione di tutte le funzionalità per un'organizzazione nella Guida per l' AWS Organizations](#)utente.AWS Organizations Per iscriverti a livello di organizzazione, seleziona il pulsante di opzione La mia organizzazione. Controlla i [dettagli e i prezzi del piano](#), quindi seleziona la casella per accettare i termini dell'abbonamento. Solo l'account di gestione della tua organizzazione può sottoscrivere l'intera organizzazione.

Oppure, per registrarti a livello di account, seleziona il pulsante di opzione Il mio account, quindi seleziona la casella per accettare i termini dell'abbonamento.
- c. Scegli Conferma aggiornamento per completare l'abbonamento al piano AWS Business Support+.

Note

Dopo aver sottoscritto l'intera organizzazione a AWS Business Support+, tutti i nuovi account creati all'interno di tale organizzazione vengono automaticamente abbonati a AWS Business Support+. Se un account precedentemente sottoscritto a AWS Business Support+ a livello di organizzazione lascia l'organizzazione, tale account viene declassato al piano di supporto Basic.

 Note

Se ti iscrivi a un piano di supporto a pagamento, sarai vincolato con un abbonamento a Supporto AWS per un minimo di un mese. Per ulteriori informazioni, consulta la [Supporto AWS FAQs](#).

Informazioni correlate

Per ulteriori informazioni sui piani, consulta la. Supporto AWS [Supporto AWS FAQs](#) 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.

Configura le notifiche di scadenza del piano promozionale

Puoi utilizzarlo [Notifiche all'utente AWS](#) per configurare le notifiche per informarti quando termina il periodo promozionale del tuo piano di supporto. Puoi iscriverti per ricevere notifiche via e-mail, in o in altri canali di chat a tua scelta. AWS Console Mobile Application

Configura le notifiche di scadenza del piano di supporto promozionale

1. Apri le notifiche utente in [Console di gestione AWS](#):
 - a. Scegli l'icona a forma di campana nella barra di navigazione in alto.
 - b. Scegli Centro notifiche.
 - c. Nel riquadro di navigazione, scegli Configurazione delle notifiche.
 - d. Scegli Crea configurazione di notifica.
 - e. Seleziona almeno un hub di configurazione. Per ulteriori informazioni, vedere [Archiviazione, elaborazione e replica delle notifiche utilizzando gli hub di notifica](#) in. Notifiche all'utente AWS
2. Per Event Rule, inserisci le seguenti informazioni:
 - Per Servizio AWS nome, inserisci Support Plans.
 - Per Tipo di evento, inserisci Scadenza della promozione del piano di supporto.

- Per le regioni, seleziona la fonte Regioni AWS in cui desideri ricevere le notifiche. Per questa opzione, scegli Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon).
3. Configura le impostazioni di aggregazione per ridurre la frequenza delle notifiche. Ti consigliamo di impostare l'aggregazione su Ricevi entro 5 minuti.
 4. Configura i canali di consegna in cui desideri ricevere le notifiche. Se non selezioni un canale di consegna, puoi visualizzare le notifiche selezionando l'icona a forma di campana nella barra Console di gestione AWS di navigazione.

Per istruzioni dettagliate sulla creazione di notifiche configurate dall'utente, consulta la [Fase 1: creazione di una configurazione di notifica nella Guida per l' Notifiche all'utente AWS utente](#).

Visualizza le notifiche relative al piano promozionale

Le notifiche vengono inviate al canale di consegna che hai scelto durante la configurazione. Puoi anche visualizzare le notifiche scegliendo l'icona a forma di campana nella barra di navigazione della console. L'icona a forma di campana mostra un contrassegno rosso quando sono disponibili nuove notifiche.

Per ulteriori informazioni sulla visualizzazione delle notifiche, consulta [Fase 2: Visualizzazione delle notifiche](#) nella Guida per l'Notifiche all'utente AWS utente.

Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise

Per informazioni sulla transizione a un nuovo piano, consulta le seguenti informazioni specifiche sul piano e le [Supporto AWS Domande frequenti](#).

Note

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

Fine del supporto Supporto per il piano di sviluppo

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i [dettagli del piano Business Support+](#).

Fine Supporto del supporto per il piano aziendale

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Fine del supporto per Enterprise On-Ramp

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

AWS Trusted Advisor

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

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.

AWS Trusted Advisor i controlli sono disponibili per i clienti con un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations.

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 ai [controlli selezionati](#) nelle categorie Security e Fault tolerance. Gli aggiornamenti con controllo automatico non sono disponibili nei piani Basic e Developer Support. È necessario aggiornare manualmente Trusted Advisor i controlli nella categoria Sicurezza. Per aggiornare manualmente un controllo, procedi come segue:

Se disponi di un piano Basic Support, puoi utilizzare la Trusted Advisor console per accedere a tutti i controlli nella categoria Service Limits e ai [controlli selezionati](#) nelle categorie Security e Fault tolerance. Gli aggiornamenti con controllo automatico non sono disponibili nei piani Basic e Developer Support. È necessario aggiornare manualmente Trusted Advisor i controlli nella categoria Sicurezza. Per aggiornare manualmente un controllo, procedi come segue:

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Seleziona il pulsante Aggiorna sulla spunta che desideri aggiornare.

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, 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 Console di gestione AWS. Per ulteriori informazioni sul controllo dell'accesso alla Trusted Advisor console, vedere [Gestisci l'accesso a AWS Trusted Advisor](#).

Per ulteriori informazioni, consulta [Trusted Advisor](#).

Argomenti

- [Inizia a usare i Trusted Advisor consigli](#)
- [Inizia a usare l' Trusted Advisor API](#)
- [Utilizzo Trusted Advisor come servizio web](#)
- [Visualizzazione organizzativa per AWS Trusted Advisor](#)
- [Visualizza AWS Trusted Advisor i controlli forniti da AWS Config](#)
- [Visualizzazione AWS Security Hub CSPM dei controlli in AWS Trusted Advisor](#)

- [Attiva AWS Compute Optimizer i Trusted Advisor controlli](#)
- [Inizia a usare AWS Trusted Advisor Priority](#)
- [AWS Trusted Advisor verifica riferimento](#)
- [Registro delle modifiche per AWS Trusted Advisor](#)

Inizia a usare i Trusted Advisor consigli

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

Puoi utilizzare la pagina Trusted Advisor Consigli della Trusted Advisor console per esaminare i risultati del controllo 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](#)
- [Visualizza le categorie di controllo](#)
- [Visualizza controlli specifici](#)
- [Filtra i controlli](#)
- [Aggiorna i risultati di controllo](#)
- [Scarica i risultati del controllo](#)
- [Visualizzazione organizzativa](#)
- [Preferenze](#)

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. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
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.

[Trusted Advisor](#) > Recommendations

Trusted Advisor Recommendations Refresh all checks Download all checks

Use this page to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. [Learn more](#)

Checks summary

42

Action recommended

Info

Security	30
Performance	1
Fault tolerance	9
Cost optimization	1
Service limits	1

127

Investigation recommended

Info

Fault tolerance	29
Performance	9
Operational Excellence	12
Cost optimization	14
Security	63

28

Checks with excluded items

Info

Security	11
Cost optimization	11
Service limits	1
Performance	2
Fault tolerance	3

Potential monthly savings

\$7,082.26

Trusted Advisor has identified 18 cost optimization checks that can save you money. For example, you might have unused resources in your AWS account that can be deleted. Choose a cost optimization check to view the recommendations.

[View all cost optimization checks](#)

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 da <https://console.aws.amazon.com/trustedadvisor/casa>.
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.

Cost optimization

Refresh all checks
Download all checks

Choose a check name to see recommendations for ways to help save money for your AWS account. Trusted Advisor might recommend that you delete unused and idle resources, or use reserved capacity.

Overview

Potential monthly savings
\$7,082.26

1
Action recommended
Info

14
Investigation recommended
Info

10
No problems detected
Info

11
Checks with excluded items
Info

Cost optimization checks

Filter by tag key [Learn more about using tags](#)

Tag Key
Tag Value
Reset
Apply filter

Search by keyword [Info](#)

Source
View

Filter checks
All sources
All checks

1 2 >

Amazon Comprehend Underutilized Endpoints

Checks the throughput configuration of your endpoints.

Last updated: 2 hours ago

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

- Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
- Nel pannello di navigazione, seleziona una categoria di controllo.
- 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.
- (Facoltativo) Per escludere gli elementi in modo che non vengano visualizzati nei risultati del controllo:
 - Seleziona un elemento e scegli Escludi e aggiorna.
 - Per visualizzare tutti gli elementi esclusi, seleziona Elementi esclusi.
- (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.
- Low Utilization Amazon EC2 Instances

Last updated: 14 hours ago

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

Additional Resources

[Monitoring Amazon EC2](#)

[Instance Metadata and User Data](#)

[Amazon CloudWatch Developer Guide](#)

[Auto Scaling Developer Guide](#)

Low Utilization Amazon EC2 Instances (38)

Exclude & Refresh

Included items

38 of 39 Amazon EC2 instances have low average daily utilization. Monthly savings of up to \$713.23 might be available by minimizing underutilized instances. 1 items have been excluded.

< 1 2 >

Region/AZ	Instance ID	Instance Name	Instance Type	Estimated Monthly Savings	CPU Utilization 14-Day Average
ca-central-1b	i-0f818268643c7ae32		t2.micro	\$9.22	0.1%
ca-central-1a	i-06c233a11aa626588		t2.micro	\$9.22	0.1%

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.

Filtra i controlli

Versione API 2026-04-14 90

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 da <https://console.aws.amazon.com/trustedadvisor/casa>.
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:

- [Supporto AWS 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 disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, aggiorna Trusted Advisor automaticamente i controlli nel tuo account su base settimanale.

Per aggiornare i controlli Trusted Advisor

1. Vai alla AWS Trusted Advisor console all'indirizzo <https://console.aws.amazon.com/trustedadvisor>.
2. Nella pagina dei Trusted Advisor consigli o di una categoria di assegni, 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 il tuo account, non puoi usare la Trusted Advisor console AWS Security Hub CSPM per aggiornare i controlli CSPM di Security Hub. Per ulteriori informazioni, consulta [Aggiorna i risultati del Security Hub CSPM](#).

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. Vai 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 della tua organizzazione. AWS 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](#) e [Trusted Advisor Priority](#).

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 [Gestisci le notifiche Trusted Advisor prioritarie](#).

Configura le preferenze di notifica

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
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 Gestione dei costi e fatturazione AWS 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 da <https://console.aws.amazon.com/trustedadvisor/casa>.
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 nel tuo account.

4. Puoi quindi eliminare manualmente il dal tuo account. Per ulteriori informazioni, consulta [Eliminazione di un ruolo collegato al servizio 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

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support + offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support +](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations per utilizzare l' Trusted Advisor API.
- Se chiami l' AWS Trusted Advisor API da un account che non dispone di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, 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 [ListRecommendationResources](#) API per visualizzare i consigli e gli account e le risorse corrispondenti.
- Utilizza l'operazione [UpdateRecommendationLifecycle](#) API per aggiornare il ciclo di vita di una raccomandazione gestita da Trusted Advisor Priority.
- Utilizza l'operazione [BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor
- Le chiamate [ListOrganizationRecommendationsGetOrganizationRecommendation](#), [ListOrganizationRecommendationResources](#), [ListOrganizationRecommendationAccounts](#), e [UpdateOrganizationRecommendationLifecycle](#) API 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

Il Supporto AWS 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](#)
- [Aggiorna l'elenco dei controlli disponibili Trusted Advisor](#)
- [Esegui un Trusted Advisor sondaggio per verificare le modifiche allo stato](#)
- [Richiedi il risultato di un Trusted Advisor controllo](#)
- [Mostra i dettagli di un controllo Trusted Advisor](#)

Visualizza l'elenco dei controlli disponibili Trusted Advisor

Il seguente frammento di codice Java crea un'istanza di un Supporto 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 [DescribeTrustedAdvisorChecks](#) API. 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 Supporto 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 [DescribeTrustedAdvisorCheckRefreshStatuses](#) API 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 [DescribeTrustedAdvisorChecks](#) API 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 la 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

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata,

tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

La visualizzazione organizzativa consente di visualizzare gli Trusted Advisor assegni per tutti gli account del tuo. [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, puoi utilizzare i report per identificare quali account della tua organizzazione utilizzano AWS Identity and Access Management (IAM) con il controllo IAM Use o se hai azioni consigliate per i bucket Amazon Simple Storage Service (Amazon S3) con il controllo Amazon S3 Bucket Permissions.

Argomenti

- [Prerequisiti](#)
- [Abilita visualizzazione organizzativa](#)
- [Aggiorna Trusted Advisor i controlli](#)
- [Creazione di report di visualizzazione organizzativa](#)
- [Esamina il riepilogo del report](#)
- [Scarica un report della visualizzazione organizzativa](#)
- [Disattiva visualizzazione organizzativa](#)
- [Utilizzo delle policy IAM per consentire l'accesso alla visualizzazione organizzativa](#)
- [Utilizzo di altri AWS servizi per visualizzare Trusted Advisor i report](#)

Prerequisiti

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

- I tuoi account devono essere membri di un. [AWS Organizations](#)

- 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 dell'organizzazione deve disporre di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations. Puoi trovare il tuo piano di supporto nel Supporto AWS Centro o nella pagina dei [piani di supporto](#). Consulta la sezione [Confronta piani Supporto AWS](#).
- 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, consulta [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 è abilitato come servizio affidabile nella tua organizzazione. Per ulteriori informazioni, consulta [Abilitazione di un accesso sicuro con altri servizi AWS](#) nella Guida per l'utente di AWS Organizations .
- `AWSServiceRoleForTrustedAdvisorReporting` service-linked-role viene creato per te nell'account di gestione della tua organizzazione. Questo ruolo include le autorizzazioni Trusted Advisor necessarie per chiamare 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 Trusted Advisor console.

Per abilitare la visualizzazione organizzativa

1. Accedi come amministratore nell'account di gestione dell'organizzazione e apri la AWS Trusted Advisor console all'indirizzo <https://console.aws.amazon.com/trustedadvisor>.
2. Nel riquadro di navigazione, in Preferences (Preferenze), scegli Your organization (La tua organizzazione).
3. In Abilita accesso affidabile con AWS Organizations, attiva 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 Supporto AWS piano determina quali Trusted Advisor controlli sono disponibili per un account.

Aggiorna Trusted Advisor i controlli

Prima di creare un rapporto per la propria organizzazione, si consiglia di aggiornare lo stato 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, aggiorna Trusted Advisor automaticamente i controlli nel tuo account su base settimanale.

 Note

Se nella tua organizzazione disponi di account con un piano di supporto Developer o Basic, un utente di tali account deve accedere alla Trusted Advisor console 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. Vai alla AWS Trusted Advisor console 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:

- Usa 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 AWS Trusted Advisor console all'indirizzo /trustedadvisor. https://console.aws.amazon.com](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 rapporto include tutti i controlli, le categorie di controllo Regioni AWS, i controlli e gli stati delle risorse. 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 Regione, specifica Regioni AWS o scegli Tutto.
 - 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 AWS Organizations, seleziona le unità organizzative (OUs) da includere nel rapporto. Per ulteriori informazioni OUs, vedere [Gestione delle unità organizzative](#) nella Guida AWS Organizations per l'utente.
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

Report filters

Choose the filter options for your report.

Report name

Trusted-Advisor-report

The report name can be up to 100 characters and can't start with a hyphen. Valid characters: A-Z, a-z, 0-9, and - (hyphen)

Format

JSON

Region

Choose Region

us-east-1 ✕

us-east-2 ✕

us-west-1 ✕

Check category

Choose category

Security ✕

Performance ✕

Checks

Choose check names

Resource status

Choose status

All ✕

Nell'esempio seguente, il rapporto include l'unità organizzativa del team di supporto e un AWS account che fanno parte dell'organizzazione.

AWS organization

You can select the organizational units (OUs) and individual AWS accounts to include in your report.

Organizational structure

▼ ☒  **Root**
r-xa9c

▶ ☐  **instance-management**
ou-xa9c-example1

▼ ☒  **support-team**
ou-xa9c-example2

☒  **Jane Doe**
111122223333 | janedoe@example.com

☒  **Mateo Jackson**
444455556666 | mateojackson@example.com

▶ ☐  **security-team**
ou-xa9c-example3

☒  **Ana Carolina Silva**
777788889999 | anacarolinasilva@example.com

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.

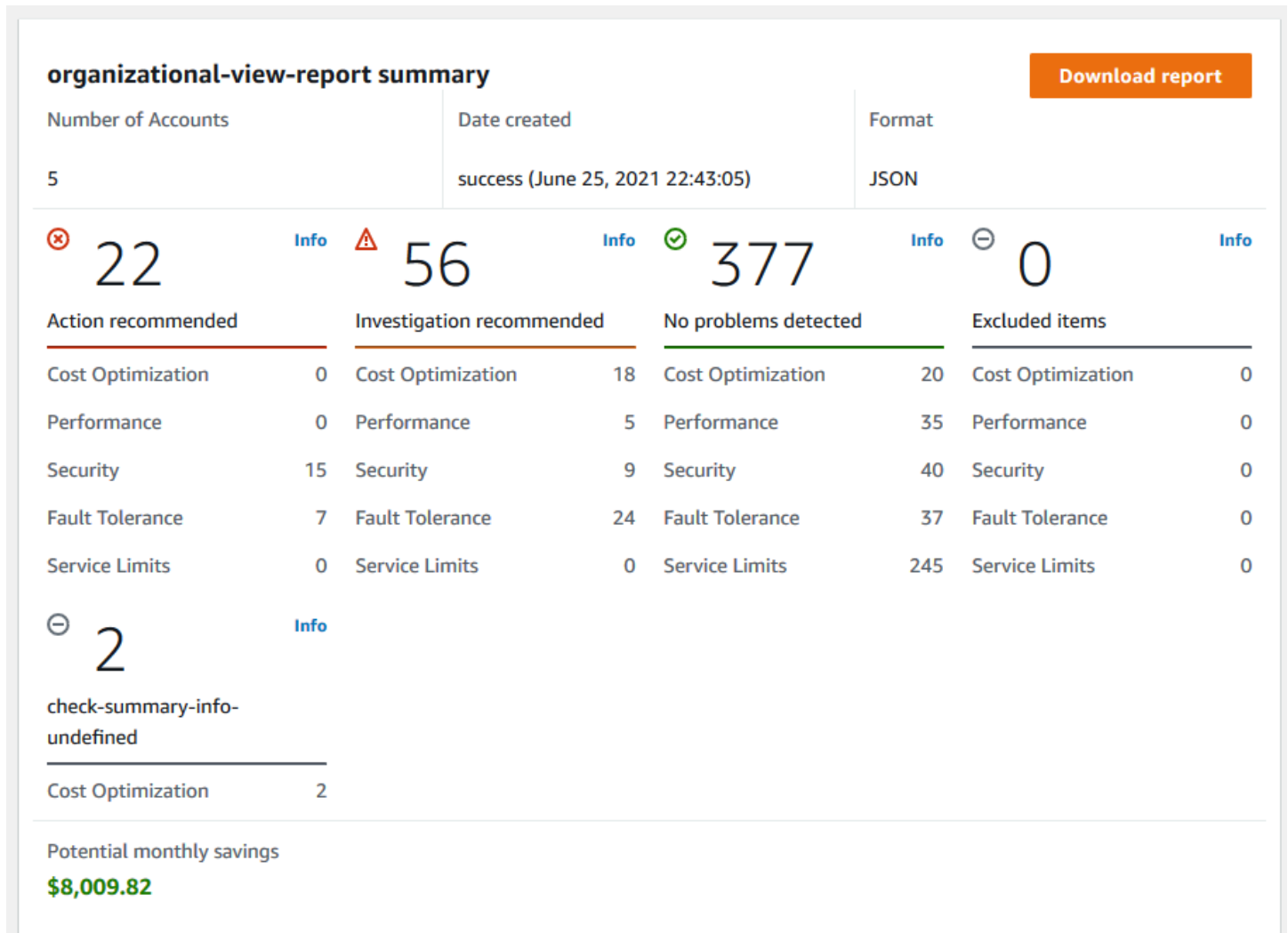
Esamina il riepilogo del report

Una volta che il report è pronto, puoi visualizzarlo dalla Trusted Advisor console. 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 AWS Trusted Advisor console 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

Quando il rapporto è pronto, scaricalo dalla Trusted Advisor console. 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 AWS Trusted Advisor console 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.

Organizational View

With AWS organizations, you can create reports for check results across all AWS accounts within an organization. This provides you a centralized view for all AWS Trusted Advisor checks. You can also view and download reports on this page. Use this report to identify issues and take action for accounts in your organization. [Learn more](#) .

Reports (50)

Create reportDownload report

	Report name	Date generated	Status	Format
☐	all-regions-check-report	June 15, 2021 18:43:42	Success	JSON
☐	json-us-east-1-region-only	June 14, 2021 20:54:29	Success	JSON
☐	security-checks-only-all-accounts	June 10, 2021 03:33:59	Success	JSON

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 controllare i risultati:

- **Green**— Trusted Advisor non rileva alcun problema durante il controllo.
- **Yellow**— Trusted Advisor rileva un possibile problema durante il controllo.
- **Red**— Trusted Advisor rileva un errore e consiglia un'azione per il controllo.
- **Blue**— non è in Trusted Advisor 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. L'esempio seguente include le proprietà IDs e per i controlli IAM Password Policy (Yw2K9puPzl) e IAM Key Rotation (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 Trusted Advisor controllo
- L'ID della risorsa
- Il timestamp del report
- Il nome completo dell' Trusted Advisor assegno
- La categoria dell' Trusted Advisor assegno
- 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	vioZmlba45kf2JWle_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	Llc4zRaUSiIGRSlmqMa5V	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-_TlMw-5Jc	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7lgTzjTYb	1xHq5ovV8bS0H1Z-t7Kbik	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 accadere quando gli utenti con un piano di supporto Basic o Developer accedono alla Trusted Advisor console per la prima volta. Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, può essere necessaria fino a una settimana dalla registrazione dell'account prima che gli utenti vedano i risultati del controllo. Per ulteriori informazioni, consulta [Aggiorna Trusted Advisor i controlli](#).
- 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 .csv 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, puoi utilizzare un'interfaccia SQL con un AWS servizio come Amazon Athena per eseguire query sui tuoi report. Puoi anche usare Amazon Quick per creare dashboard e visualizzare i tuoi dati. Per ulteriori informazioni, consulta [Utilizzo di altri AWS servizi per visualizzare Trusted Advisor i report](#).

Disattiva visualizzazione organizzativa

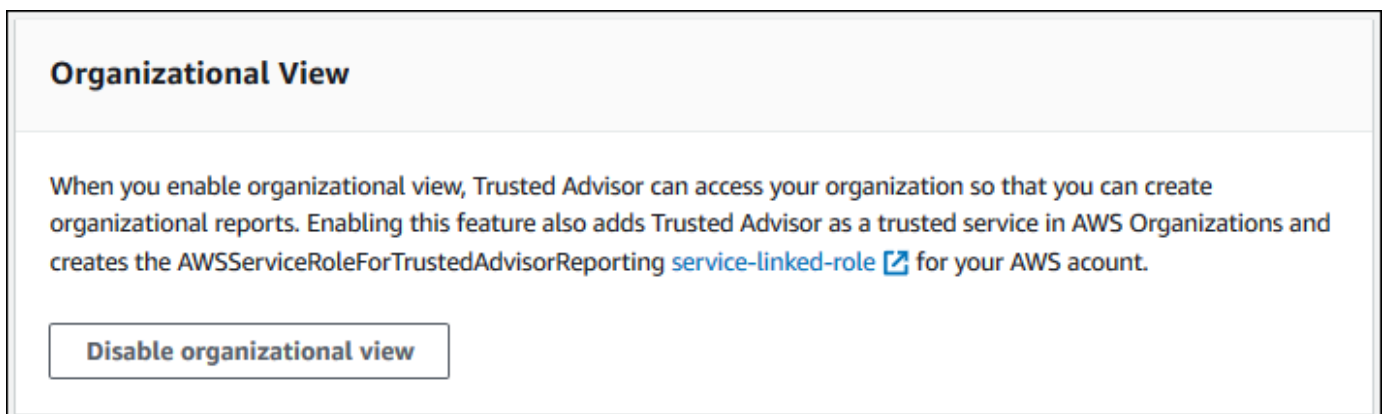
Segui questa procedura per disattivare la visualizzazione organizzativa. È necessario accedere all'account di gestione dell'organizzazione o assumere un ruolo con le autorizzazioni necessarie per disattivare questa funzionalità. Non è possibile disattivare questa funzionalità da un altro account nell'organizzazione.

Dopo aver disattivato questa funzionalità, si verifica quanto segue:

- Trusted Advisor viene rimosso come servizio affidabile 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, consulta [Abilita visualizzazione organizzativa](#).

Per disabilitare la visualizzazione organizzativa per Trusted Advisor

1. Accedi all'account di gestione dell'organizzazione e apri la AWS Trusted Advisor console 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 disabilitato la visualizzazione organizzativa, Trusted Advisor non aggrega più gli assegni provenienti da altri AWS account dell'organizzazione. Tuttavia, il ruolo `AWSServiceRoleForTrustedAdvisorReporting` collegato al servizio rimane nell'account di gestione dell'organizzazione finché non lo elimini tramite la console IAM, l'API IAM o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Note

Puoi utilizzare altri AWS servizi per interrogare e visualizzare i tuoi dati per i report di visualizzazione organizzativa. Per maggiori informazioni, consulta le seguenti risorse:

- [Visualizza suggerimenti di AWS Trusted Advisor su scala con AWS Organizations](#) nel Blog AWS Management & Governance
- [Utilizzo di altri AWS servizi per visualizzare Trusted Advisor i report](#)

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

Puoi utilizzare le seguenti policy AWS Identity and Access Management (IAM) per consentire agli utenti o ai ruoli del tuo 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

JSON

```
{
  "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 seguente policy 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.

JSON

```
{
  "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 abilitato il tuo account, AWS CloudTrail nelle voci di registro possono comparire i seguenti ruoli:

- `AWSServiceRoleForTrustedAdvisorReporting`— Il ruolo collegato al servizio Trusted Advisor utilizzato per accedere agli account dell'organizzazione.
- `AWSServiceRoleForTrustedAdvisor`— Il ruolo collegato ai servizi Trusted Advisor utilizzato per accedere ai servizi dell'organizzazione.

Per ulteriori informazioni sui ruoli collegati al servizio, consulta [Utilizzo di ruoli collegati ai servizi per Trusted Advisor](#).

Utilizzo di altri AWS servizi per visualizzare Trusted Advisor i report

Segui questo tutorial per caricare e visualizzare i tuoi dati utilizzando altri AWS servizi. In questo argomento, crei un bucket Amazon Simple Storage Service (Amazon S3) per archiviare il report e CloudFormation un modello per creare risorse nel tuo account. Quindi, puoi utilizzare Amazon Athena per analizzare o eseguire query per il tuo report o Quick per visualizzare quei dati in una dashboard.

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.
- Usa gli Stati Uniti orientali (Virginia settentrionale) Regione AWS per configurare rapidamente i tuoi AWS servizi e le tue risorse.
- Crea un account Quick. Per ulteriori informazioni, consulta [Getting Started with Data Analysis in Quick](#) nella Amazon Quick User Guide.

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 Console di gestione AWS a <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. Nella *bucket-name* pagina, scegli 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.

Crea le tue risorse utilizzando AWS CloudFormation

Dopo aver caricato il report su Amazon S3, carica il seguente modello YAML su CloudFormation. Questo modello indica CloudFormation quali risorse creare per il tuo 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 le tue risorse con CloudFormation

1. Scarica il [trusted-advisor-reports-templatefile.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. Salvare il file.
6. Apri la CloudFormation console 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. Nella parte inferiore della pagina, seleziona la casella di controllo Riconosco che CloudFormation potrebbe creare risorse IAM.
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.

Trusted-Advisor-reports				Delete	Update	Stack actions ▼
Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Resources (12)						
Search resources						
Logical ID ▲	Physical ID ▼	Type ▼	Status ▼			
AWSPutS3TANotification	2020/05/27/[\$LATEST]5bfd3cb8b29a4b85bc0f8d861EXAMPLE1	Custom::AWSPutS3TANotification	✔ CREATE_COMPLETE			
AWSS3TAEventLambdaPermission	Trusted-Advisor-reports-AWSS3TAEventLambdaPermission-10KT2EXAMPLE1	AWS::Lambda::Permission	✔ CREATE_COMPLETE			
AWSS3TALambdaExecutor	Trusted-Advisor-reports-AWSS3TALambdaExecutor-1BJ3KEXAMPLE1	AWS::IAM::Role	✔ CREATE_COMPLETE			
AWSS3TANotification	Trusted-Advisor-reports-AWSS3TANotification-15J3KEXAMPLE1	AWS::Lambda::Function	✔ CREATE_COMPLETE			
AWSS3TACrawler	2020/05/27/[\$LATEST]66726149d3d64a1f9242cdccEXAMPLE1	Custom::AWSS3TACrawler	✔ CREATE_COMPLETE			
AWSTACrawler	AWSTACrawler	AWS::Glue::Crawler	✔ CREATE_COMPLETE			

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.

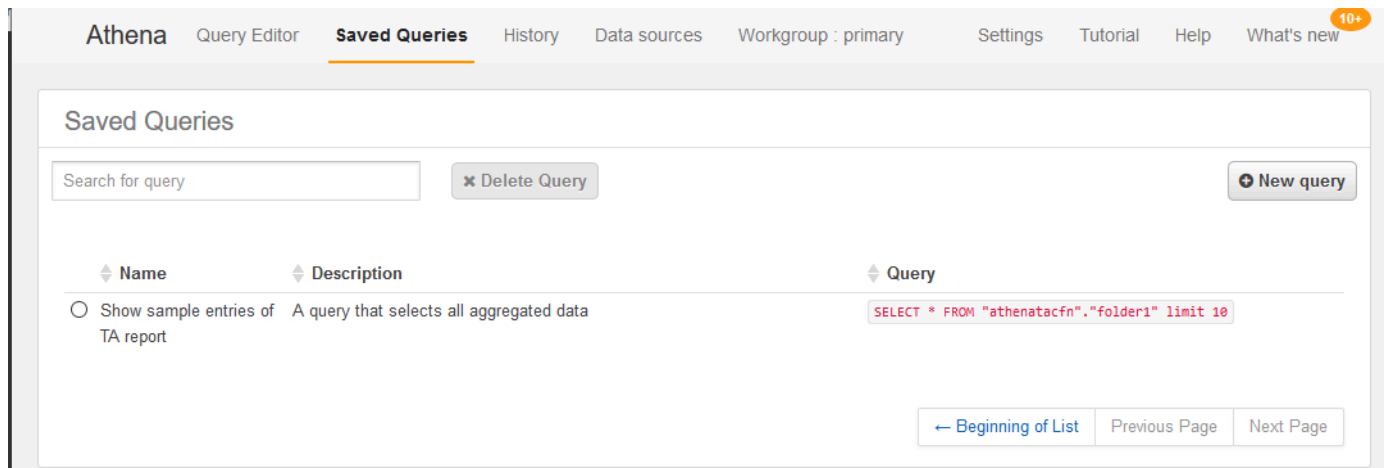
Note

- 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. Apri 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 Esegui query. Vengono visualizzati i risultati della query.

Example: Query Athena

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

New query 1

✔ Show sample ent... ✕ +

```
1 SELECT * FROM "athenatacfn"."folder1" limit 10
2
```

Run query

Save as

Create ▾

(Run time: 0.83 seconds, Data scanned: 94.75 KB)

Format query

Clear

Use Ctrl + Enter to run query, Ctrl + Space to autocomplete

Results

	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.

Crea una dashboard in Quick

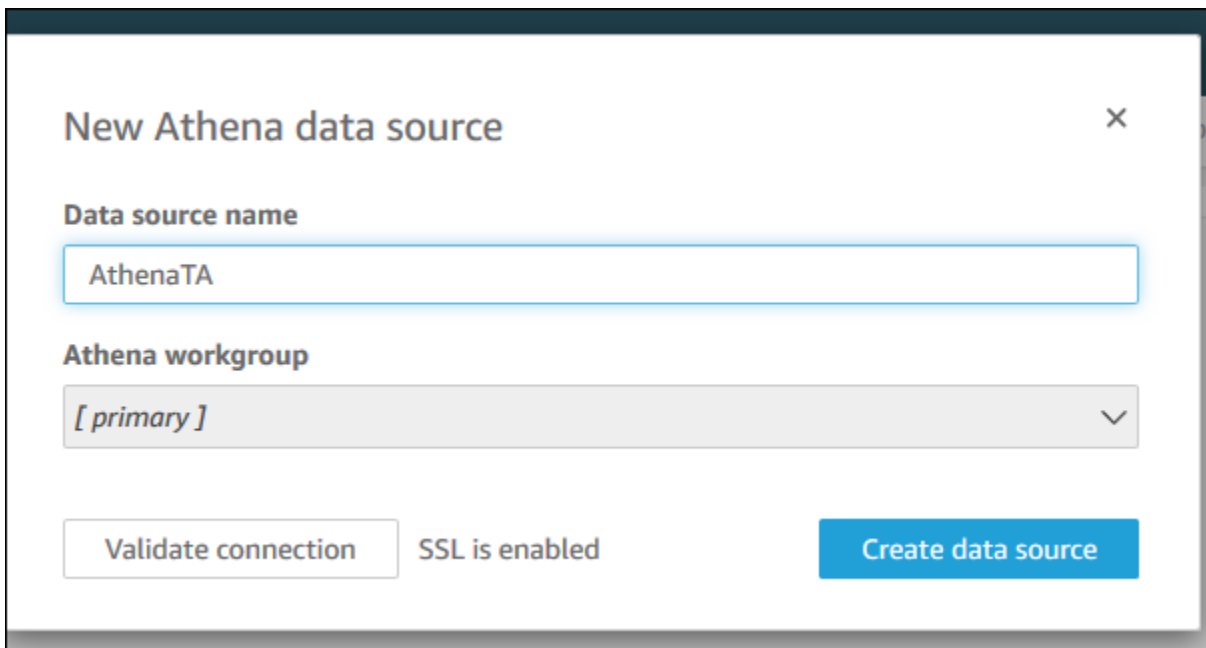
Puoi anche configurare Quick in modo da poter visualizzare i dati in una dashboard e visualizzare le informazioni del rapporto.

Note

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

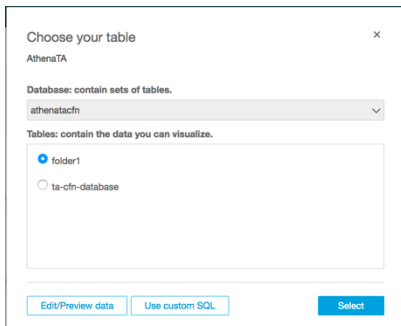
Per creare una dashboard in Quick

1. Vai alla console Quick 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.



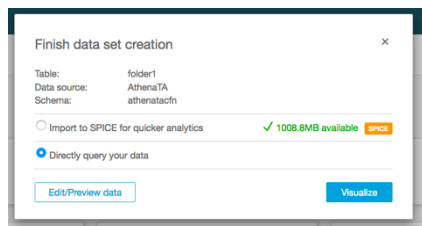
The screenshot shows a dialog box titled "New Athena data source". It has a close button (X) in the top right corner. Below the title, there is a "Data source name" label and a text input field containing "AthenaTA". Below that is an "Athena workgroup" label and a dropdown menu showing "[primary]" with a downward arrow. At the bottom, there are three buttons: "Validate connection", "SSL is enabled", and "Create data source".

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



The screenshot shows a dialog box titled "Choose your table". It has a close button (X) in the top right corner. Below the title, there is a "Database" dropdown menu showing "athenatacfn". Below that is a "Tables" section with a list of tables: "folder1" (selected with a radio button) and "ta-cfn-database" (unselected). At the bottom, there are three buttons: "Edit/Preview data", "Use custom SQL", and "Select".

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

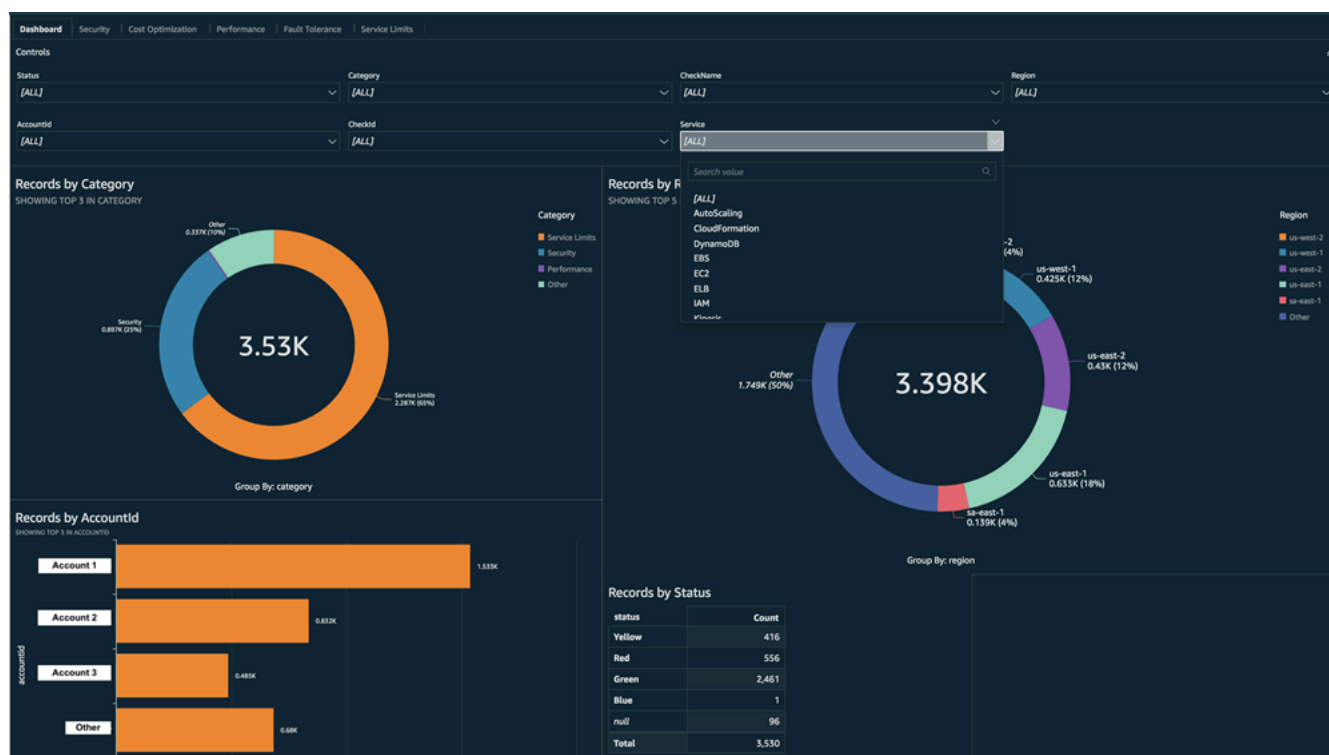


Ora puoi creare una dashboard in Quick. Per ulteriori informazioni, consulta [Working with Dashboards](#) nella Amazon Quick User Guide.

Example: Dashboard rapido

La dashboard di esempio seguente mostra informazioni sui Trusted Advisor controlli, come le seguenti:

- Account interessato IDs
- Riepilogo per AWS regioni
- Categorie di controllo
- Stati del controllo
- Numero di voci nel report per ciascun account



 Note

Se riscontri errori di autorizzazione durante la creazione della dashboard, assicurati che Quick possa utilizzare Athena. Per ulteriori informazioni, consulta [Non riesco a connettermi ad Amazon Athena](#) nella Amazon Quick User Guide.

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 crei un report, la funzionalità di visualizzazione organizzativa non aggiorna automaticamente i Trusted Advisor controlli all'interno dell'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 Trusted Advisor i controlli](#).

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 AWS Glue console per visualizzare lo schema e identificare rapidamente se nel rapporto sono presenti colonne duplicate.

Per trovare colonne duplicate

1. Apri la AWS Glue console 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 **folder1**, 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 già fatto, aggiorna gli Trusted Advisor assegni per gli account della tua organizzazione. Per informazioni, consulta [Aggiorna Trusted Advisor i controlli](#).
2. Crea e scarica un altro report JSON nella Trusted Advisor console. Per informazioni, consulta [Creazione di report di visualizzazione organizzativa](#). Per questo tutorial è necessario utilizzare un file JSON.
3. Accedi a Console di gestione AWS 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, consulta [Esegui query sui dati in Amazon Athena](#).

 Note

Se ci sono ancora problemi con questo tutorial, puoi creare una richiesta di supporto tecnico nel [Centro Supporto AWS](#).

Visualizza AWS Trusted Advisor i controlli forniti da AWS Config

 Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

AWS Config è un servizio che valuta, verifica e valuta continuamente le configurazioni delle risorse per le impostazioni desiderate. AWS Config fornisce regole gestite, che sono controlli di conformità predefiniti e personalizzabili AWS Config utilizzati per valutare se le AWS risorse sono conformi alle migliori pratiche comuni.

La AWS Config console guida l'utente nella configurazione e nell'attivazione delle regole gestite. Puoi anche utilizzare AWS Command Line Interface (AWS CLI) o l' AWS Config API 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 AWS Config, consulta la [Guida per gli AWS Config sviluppatori](#).

AWS Config le regole gestite forniscono una serie di Trusted Advisor controlli in tutte le categorie. Quando si abilitano determinate regole gestite, i Trusted Advisor controlli corrispondenti vengono abilitati automaticamente. Per vedere quali Trusted Advisor controlli sono basati su regole AWS Config gestite specifiche, consulta [AWS Trusted Advisor verifica riferimento](#).

I AWS Config power check sono disponibili per i clienti con un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations. Se attivi AWS Config e disponi di uno di questi Supporto AWS piani, visualizzerai automaticamente i consigli basati sulle corrispondenti regole gestite distribuite AWS Config .

Note

I risultati di questi controlli vengono aggiornati automaticamente in base agli aggiornamenti delle regole gestite attivati dalle modifiche. 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 la registrazione e le regole gestite per AWS Config, ma non vedo i controlli corrispondenti. Trusted Advisor](#)

- [Ho implementato la stessa regola AWS Config gestita due volte, cosa vedrò? Trusted Advisor](#)
- [Ho disattivato la registrazione per AWS Config In una AWS regione. Cosa vedrò Trusted Advisor?](#)

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

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

Ho implementato la stessa regola AWS Config gestita due volte, cosa vedrò? Trusted Advisor

Nei risultati del Trusted Advisor controllo vengono visualizzate voci separate per ogni regola gestita installata.

Ho disattivato la registrazione per AWS Config In una AWS regione. Cosa vedrò Trusted Advisor?

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

Visualizzazione AWS Security Hub CSPM dei controlli in AWS Trusted Advisor

Dopo averlo abilitato AWS Security Hub CSPM Account AWS, puoi visualizzare i controlli di sicurezza e i relativi risultati nella Trusted Advisor console. Puoi utilizzare i controlli CSPM di Security Hub per identificare le vulnerabilità di 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 consigli del Security Hub CSPM per risolvere i problemi di sicurezza. Puoi utilizzare questa funzione per trovare consigli di sicurezza da Trusted Advisor e Security Hub CSPM in un'unica comoda posizione.

Note

- Da Trusted Advisor, puoi visualizzare i controlli nello 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 CSPM .

Per ulteriori informazioni sulle categorie CSPM di Security Hub, vedere [Categorie di controllo](#).

- Trusted Advisor controlli CSPM Security Hub integrati fino al 26 settembre 2024. I controlli rilasciati dopo il 26 settembre 2024 non sono ancora stati integrati. Trusted Advisor Puoi trovare i controlli rilasciati dopo quella data nel registro [CSPM di Security Hub](#).

Argomenti

- [Prerequisiti](#)
- [Visualizza i risultati del Security Hub CSPM](#)
- [Aggiorna i risultati del Security Hub CSPM](#)
- [Disattiva Security Hub CSPM da Trusted Advisor](#)
- [Risoluzione dei problemi](#)

Prerequisiti

È necessario soddisfare i seguenti requisiti per abilitare l'integrazione CSPM di Security Hub con: Trusted Advisor

- È necessario disporre di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations per questa funzionalità. Puoi trovare il tuo piano di supporto dal [Centro Supporto AWS](#) o dalla pagina [Piani di supporto](#). Per ulteriori informazioni, [consulta Confronta Supporto AWS](#) i piani.
- È necessario abilitare la registrazione delle risorse AWS Config per Regioni AWS ciò che si desidera per i controlli CSPM di Security Hub. Per ulteriori informazioni, consulta [Abilitazione e configurazione di AWS Config](#).

- È necessario abilitare Security Hub CSPM 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 CSPM](#) nella Guida per l'utente di AWS Security Hub CSPM.

Note

Se i prerequisiti sono già stati completati, è possibile passare alla [Visualizza i risultati del Security Hub CSPM](#).

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. Non è necessario contattare gli account dei singoli membri Supporto per abilitare questa funzionalità. Tuttavia, gli account dei membri dell'organizzazione devono abilitare Security Hub CSPM se desiderano visualizzare i risultati. Trusted Advisor

Se vuoi disabilitare questa integrazione per un account membro specifico, consulta [Disattiva questa funzionalità per gli account AWS Organizations](#).

Visualizza i risultati del Security Hub CSPM

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

Per visualizzare i risultati del CSPM 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 Source, puoi scegliere di AWS Security Hub CSPM filtrare i controlli CSPM di Security Hub.

3. Scegli il nome del controllo CSPM di 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 CSPM. Per i controlli CSPM di Security Hub, puoi trovare l'ID del controllo.
- **Criteri di avviso:** lo stato del controllo. Ad esempio, se Security Hub CSPM rileva un problema importante, lo stato potrebbe essere Rosso: Critico o Alto.
- **Azione consigliata:** utilizza il link alla documentazione CSPM di Security Hub per trovare i passaggi consigliati per risolvere il problema.
- **Risorse CSPM di Security Hub:** puoi trovare le risorse nel tuo account in cui Security Hub CSPM ha rilevato un problema.

Note

- I risultati di questi controlli vengono aggiornati automaticamente almeno una volta al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. È possibile utilizzare la Trusted Advisor console per escludere le risorse dai controlli che si aggiornano automaticamente. È possibile utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per escludere risorse da qualsiasi controllo ad eccezione delle risorse di raccomandazione Trusted Advisor Priority.
- La funzionalità di visualizzazione organizzativa supporta questa integrazione con Security Hub CSPM. Puoi visualizzare i risultati dei controlli CSPM del Security Hub in tutta l'organizzazione, quindi creare e scaricare report. Per ulteriori informazioni, consulta [Visualizzazione organizzativa per AWS Trusted Advisor](#).

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

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

▼


IAM root user access key should not exist

Last updated: an hour ago  

Checks if the root user access key is available.

Source

[AWS Security Hub](#)
 Security Hub control ID: IAM.4

Alert Criteria

Red: Critical or High. Security Hub control failed.

Recommended Action

Follow the [Security Hub documentation](#) to fix the issue.

IAM root user access key should not exist (1)

Exclude & Refresh

Included items ▼

1 of 1 resources failed this Security Hub control.

<

1

>



☐	Status ▼	Region ▼	Resource ▼	Last Updated Time ▼
☐		us-east-1	AWS:::Account:123456789012	2021-12-12T19:56:26.305Z

Aggiorna i risultati del Security Hub CSPM

Dopo aver abilitato uno standard di sicurezza, possono essere necessarie fino a due ore prima che Security Hub CSPM riceva i risultati relativi alle tue risorse. Possono quindi essere necessarie fino a 24 ore prima che i dati vengano visualizzati nella Trusted Advisor console. Se di recente hai abilitato lo standard di sicurezza AWS Foundational Security Best Practices v1.0.0, ricontrolla la Trusted Advisor console più tardi.

Note

- La pianificazione di aggiornamento per ogni controllo CSPM di Security Hub è periodica o viene attivata una modifica. Al momento, non è possibile utilizzare la Trusted Advisor console o l' [Supporto AWS API](#) per aggiornare i controlli CSPM di Security Hub. Per ulteriori informazioni, consulta [Pianificazione dell'esecuzione dei controlli di sicurezza](#).
- I risultati di questi controlli vengono aggiornati automaticamente almeno una volta al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. È possibile utilizzare la Trusted Advisor console per escludere le risorse dai controlli che si aggiornano automaticamente. È possibile utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per escludere

risorse da qualsiasi controllo ad eccezione delle risorse di raccomandazione Trusted Advisor Priority.

Disattiva Security Hub CSPM da Trusted Advisor

Segui questa procedura se non desideri che le informazioni del CSPM di Security Hub vengano visualizzate nella Trusted Advisor console. Questa procedura disabilita solo l'integrazione CSPM di Security Hub con. Trusted Advisor Non influirà sulle configurazioni con Security Hub CSPM. Puoi continuare a utilizzare la console CSPM di Security Hub per visualizzare i controlli di sicurezza, le risorse e i consigli.

Per disabilitare l'integrazione CSPM di Security Hub

1. Contatta [Supporto AWS](#) se richiedi di disabilitare l'integrazione CSPM di Security Hub con. Trusted Advisor

Dopo aver Supporto AWS disabilitato questa funzione, Security Hub CSPM non invia più dati a. Trusted Advisor I dati CSPM del Security Hub verranno rimossi da. Trusted Advisor

2. Se desideri abilitare nuovamente questa integrazione, contatta [Supporto AWS](#).

Disattiva questa funzionalità per gli account AWS Organizations

Se hai già completato la procedura precedente per un account di gestione, l'integrazione CSPM di Security Hub viene automaticamente rimossa da tutti gli account dei membri dell'organizzazione. I singoli account membri dell'organizzazione non devono contattare Supporto AWS separatamente.

Se sei un account membro di un'organizzazione, puoi contattarci Supporto per rimuovere questa funzionalità solo dal tuo account.

Risoluzione dei problemi

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

Indice

- [Non vedo i risultati del CSPM di Security Hub nella console Trusted Advisor](#)

- [Ho configurato Security Hub CSPM e AWS Config correttamente, ma i risultati non sono ancora stati rilevati](#)
- [Desidero disabilitare controlli CSPM specifici di Security Hub](#)
- [Voglio trovare le mie risorse CSPM Security Hub escluse](#)
- [Voglio abilitare o disabilitare questa funzionalità per un account membro che appartiene a un'organizzazione AWS](#)
- [Ne vedo più di uno Regioni AWS per la stessa risorsa interessata per un controllo CSPM del Security Hub](#)
- [Ho disattivato Security Hub \(CSPM\) o AWS Config in una regione](#)
- [Il mio controllo è archiviato in Security Hub CSPM, ma vedo ancora i risultati in Trusted Advisor](#)
- [Non riesco ancora a visualizzare i risultati del CSPM di Security Hub](#)

Non vedo i risultati del CSPM di Security Hub nella console Trusted Advisor

Verifica di avere completato i seguenti passaggi:

- Hai un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations.
- È stata abilitata la registrazione delle risorse all' AWS Config interno della stessa regione del Security Hub CSPM.
- Hai abilitato Security Hub CSPM e selezionato lo standard di sicurezza AWS Foundational Security Best Practices v1.0.0.
- I nuovi controlli di Security Hub CSPM vengono aggiunti come check-in Trusted Advisor entro due o quattro settimane. Consulta la [nota](#).

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

Ho configurato Security Hub CSPM e AWS Config correttamente, ma i risultati non sono ancora stati rilevati

Possono essere necessarie fino a due ore prima che Security Hub CSPM riceva i risultati relativi alle tue risorse. Possono quindi essere necessarie fino a 24 ore prima che i dati vengano visualizzati nella Trusted Advisor console. Controlla di nuovo la console Trusted Advisor più tardi.

 Note

- Verranno visualizzati solo i risultati relativi ai controlli dello standard di sicurezza AWS Foundational Security Best Practices, ad Trusted Advisor eccezione dei controlli che hanno la categoria: Recover > Resilience.
- Se c'è un problema di servizio con Security Hub CSPM o Security Hub CSPM non è disponibile, possono essere necessarie fino a 24 ore prima che i risultati vengano visualizzati. Trusted Advisor Controlla di nuovo la console Trusted Advisor più tardi.

Desidero disabilitare controlli CSPM specifici di Security Hub

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

Puoi accedere alla [console CSPM di Security Hub](#) e verificare se il controllo è abilitato o disabilitato.

Se disabiliti un controllo CSPM di Security Hub o disabiliti 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 vengono 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](#)

Voglio trovare le mie risorse CSPM Security Hub escluse

Dalla Trusted Advisor console, puoi scegliere il nome del controllo CSPM di Security Hub, quindi scegliere l'opzione Elementi esclusi. Questa opzione visualizza tutte le risorse che sono soppresse in Security Hub CSPM.

Se lo stato del flusso di lavoro per una risorsa è impostato su SUPPRESSED, quella risorsa è un elemento escluso in Trusted Advisor. Non puoi sopprimere le risorse CSPM di Security Hub dalla console. Trusted Advisor Per farlo, usa la console [CSPM di Security Hub](#). Per ulteriori informazioni, consulta [Impostazione dello stato del flusso di lavoro per i risultati](#).

Voglio abilitare o disabilitare questa funzionalità per un account membro che appartiene 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 [Supporto AWS](#).

Ne vedo più di una Regione AWS per la stessa risorsa interessata per un controllo CSPM del 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 CSPM di Security Hub che valutano le risorse per i servizi globali, potresti visualizzare 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 CSPM 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 (CSPM) o AWS Config in una regione

Se interrompi la registrazione delle risorse con AWS Config o disabiliti Security Hub CSPM in un Regione AWS, Trusted Advisor non riceve più dati per alcun controllo in quella regione. Trusted Advisor rimuove i risultati del CSPM di Security Hub entro 7-9 giorni. Questo lasso di tempo è il risultato massimo e non è garantito. Per ulteriori informazioni, vedere [Disabilitazione del Security Hub CSPM](#).

Per disabilitare questa caratteristica per il tuo account, consulta [Disattiva Security Hub CSPM da Trusted Advisor](#).

Il mio controllo è archiviato in Security Hub CSPM, ma vedo ancora i risultati in Trusted Advisor

Quando lo `RecordState` stato cambia in `ARCHIVED` Per un risultato, Trusted Advisor elimina il risultato per quel controllo CSPM di Security Hub dal tuo account. Potresti continuare a visualizzare

il risultato Trusted Advisor per un massimo di 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 CSPM di Security Hub

Se ci sono ancora problemi con questa caratteristica, puoi creare una richiesta di supporto tecnico nel [Centro Supporto AWS](#).

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 almeno una volta al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. È possibile utilizzare la Trusted Advisor console per escludere le risorse dai controlli che si aggiornano automaticamente. È possibile utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per escludere risorse da qualsiasi controllo ad eccezione delle risorse di raccomandazione di Trusted Advisor Priority.
- Trusted Advisor dispone già dei controlli Amazon EBS Volumes sottoutilizzati e Amazon EBS Magnetic Volumes sovrautilizzati.

Dopo aver attivato Compute Optimizer, ti consigliamo di utilizzare invece i nuovi controlli dei volumi con provisioning eccessivo di Amazon EBS e dei volumi con provisioning insufficiente di Amazon EBS.

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

Inizia a usare AWS Trusted Advisor Priority

Trusted Advisor Priority ti aiuta a proteggere e ottimizzare Account AWS le tue AWS best practice da seguire. Con Trusted Advisor Priority, il tuo Account AWS team può monitorare in modo proattivo il tuo account e creare consigli prioritari quando individuano opportunità per te.

Ad esempio, il team addetto all'account può identificare se l'utente root dell' AWS account 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. La raccomandazione viene visualizzata come raccomandazione attiva con priorità nella pagina Trusted Advisor Priorità della console. Trusted Advisor Dopodiché, puoi seguire i suggerimenti per risolverlo.

Trusted Advisor I consigli prioritari provengono da queste due fonti:

- Servizi AWS — Servizi come Trusted Advisor AWS Security Hub CSPM, e AWS Well-Architected creano automaticamente consigli. Il team addetto all'account condivide questi consigli 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 consigli 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 consigli per tutti gli account membro della tua organizzazione.

Argomenti

- [Prerequisiti](#)
- [Abilita Trusted Advisor la priorità](#)
- [Visualizzare i suggerimenti prioritari](#)
- [Riconoscimento di un suggerimento](#)
- [Ignorare un suggerimento](#)
- [Risolvere un suggerimento](#)
- [Riapertura di un suggerimento](#)
- [Scarica i dettagli sul suggerimento](#)
- [Registrazione degli amministratori delegati](#)
- [Annullamento della registrazione di amministratori delegati](#)
- [Gestisci le notifiche Trusted Advisor prioritarie](#)
- [Disattiva Trusted Advisor la priorità](#)

Prerequisiti

È necessario soddisfare i seguenti requisiti per utilizzare Trusted Advisor Priority:

- È necessario disporre di un piano AWS Enterprise Support o AWS Unified Operations.
- 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 funzionalità nell'organizzazione](#) nella Guida per l'utente di AWS Organizations .
- L'organizzazione deve aver abilitato l'accesso affidabile a Trusted Advisor. Per abilitare l'accesso attendibile, accedi con l'account di gestione. Apri la pagina La [tua organizzazione](#) nella Trusted Advisor console.
- Devi aver effettuato l'accesso al tuo AWS account per visualizzare i consigli Trusted Advisor prioritari per il tuo account.
- 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](#).
- Devi disporre delle autorizzazioni AWS Identity and Access Management (IAM) per accedere a Trusted Advisor Priority. Per informazioni su come controllare l'accesso a Trusted Advisor Priority, consulta [Gestisci l'accesso a AWS Trusted Advisor](#) e [AWS politiche gestite per AWS Trusted Advisor](#).

Abilita Trusted Advisor la priorità

Chiedi al team del tuo account di abilitare automaticamente questa funzionalità. È necessario disporre di un piano AWS Unified Operations ed essere il proprietario dell'account di gestione dell'organizzazione. Se la pagina Trusted Advisor Priorità della console indica che è necessario un accesso affidabile con AWS Organizations, scegli Abilita accesso affidabile con AWS Organizations. Per ulteriori informazioni, consulta la sezione [Prerequisiti](#).

Visualizzare i suggerimenti prioritari

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

Come visualizzare i suggerimenti prioritari

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Sulla pagina Trusted Advisor Priority puoi visualizzare i seguenti elementi:

Se utilizzi un account di AWS Organizations gestione o amministratore delegato, 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. La raccomandazione può provenire dai Servizi AWS tuo Account AWS team o da un evento di servizio 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.

Per visualizzare i consigli con priorità per tutti gli account della tua organizzazione AWS

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

 Note

Gli account dei membri non hanno accesso ai suggerimenti aggregati.

1. [Accedi alla Trusted Advisor console da casa. https://console.aws.amazon.com/trustedadvisor/](https://console.aws.amazon.com/trustedadvisor/)
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. La raccomandazione può provenire dai Servizi AWS tuo Account AWS team o da un evento di servizio 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.

- 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: Raccomandazioni Trusted Advisor prioritarie

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.

The screenshot displays the 'Trusted Advisor Priority' console. At the top, there's a header with 'Trusted Advisor > Priority' and a sub-header 'Trusted Advisor Priority' with an 'Info' link. Below this is a navigation bar with 'My organization' (selected) and 'My account'. A dropdown menu shows 'Select an account from your organization' with 'All accounts' selected. The main content area is divided into two sections: 'Action needed' and 'Overview'. The 'Action needed' section shows 'Pending response' with a count of 15 and 'In progress' with a count of 27. The 'Overview' section shows 'Dismissed in the last 90 days' (5), 'Resolved in the last 90 days' (22), 'No update in 30+ days' (10), and 'Average time to resolve' (46 days). Below this is a tabbed interface with 'Active' (selected) and 'Closed'. The 'Active' tab shows 'Active prioritized recommendations (42)' with a search bar and a table of recommendations. The table has columns for Recommendations, Status, Source, Category, and Age (days). Two recommendations are visible: 'Low Utilization Amazon EC2 Instances test' (Pending response, AWS Trusted Advisor, Cost optimization, 33 days) and 'RDS DB instances should have deletion protection enabled' (Pending response, AWS Security Hub, Security, 20 days).

Recommendations	Status	Source	Category	Age (days)
Low Utilization Amazon EC2 Instances test	Pending response	AWS Trusted Advisor	Cost optimization	33 day(s) Shared on: Jun 20, 2023
RDS DB instances should have deletion protection enabled	Pending response	AWS Security Hub	Security	20 day(s) Shared on: Jul 3, 2023

Riconoscimento di un suggerimento

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

Riconoscere un suggerimento

- Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
- Se utilizzi un account di AWS Organizations gestione o amministratore delegato, passa alla scheda Il mio account.
- Nella pagina di Trusted Advisor Priority, nella scheda Active (Attivo), scegli il nome di un suggerimento.
- 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 consigli in corso o in attesa di risposta vengono visualizzati nella scheda Attivo della pagina Trusted Advisor Priorità.

8. Segui le azioni consigliate per risolvere il suggerimento. Per ulteriori informazioni, consulta [Risolvere un suggerimento](#).

Example: Raccomandazione manuale di Trusted Advisor Priority

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

The screenshot shows the AWS Trusted Advisor console interface. At the top, there's a navigation bar with 'Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts'. Below this, there are tabs for 'My organization' and 'My account'. The main heading is 'Low Utilization Amazon EC2 Instances - Production accounts'. To the right of the heading are buttons for 'Copy recommendation link', 'Download', 'Acknowledge', and 'Dismiss'. Below the heading, there are tabs for 'Details' and 'Affected resources'. The 'Overview' section shows a table with columns: Source (AWS Trusted Advisor), Category (Cost optimization), Age (33 day(s) Shared on: Jun 20, 2023), and Status (Pending response). The 'Details' section contains a description of the recommendation, alert criteria, recommended action, and additional resources.

Overview

Source	Category	Age	Status
AWS Trusted Advisor	Cost optimization	33 day(s) Shared on: Jun 20, 2023	Pending response

Details

Description

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What Is Auto Scaling?](#)

Additional Resources

- [Monitoring Amazon EC2](#)
- [Instance Metadata and User Data](#)
- [Amazon CloudWatch Developer Guide](#)
- [Auto Scaling Developer Guide](#)

Per confermare una raccomandazione per tutti gli account dell'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 Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
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: Raccomandazione manuale di 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.

Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts

My organization My account

Low Utilization Amazon EC2 Instances - Production accounts

Copy recommendation link Download Acknowledge Dismiss

Details Affected accounts Affected resources

Overview

Source AWS Trusted Advisor	Category Cost optimization	Age 0 day(s) Shared on: Jul 10, 2023	Status ⚠ Pending response
Shared by person@amazon.com			

Status Summary

This is a summary of the status of this recommendation across all your accounts

- 1 account Pending response
- 1 account In progress

Details

Description
Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria
Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action
Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

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 è necessario seguire le azioni consigliate.

Ignorare un suggerimento

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Se utilizzi un account di AWS Organizations gestione o amministratore delegato, 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 consiglio cambia in Ignorato e viene visualizzato nella scheda Chiuso della pagina Trusted Advisor Priorità.

Per ignorare una raccomandazione per tutti gli account dell'organizzazione AWS

L'account di gestione o l'amministratore delegato di Trusted Advisor Priority possono rifiutare una raccomandazione per tutti i propri account.

1. [Accedi alla Trusted Advisor console da casa. https://console.aws.amazon.com/trustedadvisor/](https://console.aws.amazon.com/trustedadvisor/)
2. Nella pagina Trusted Advisor Priorità, assicurati di essere nella 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. Il consiglio viene visualizzato nella scheda Chiuso della pagina Trusted Advisor Priorità.

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.

Trusted Advisor Priority comunica inoltre al team del tuo account che hai ignorato la raccomandazione.

Example: Ignora una raccomandazione di Priority Trusted Advisor

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

Dismiss recommendation ✕

 Please note: This action will apply to all accounts affected by this recommendation

Choose a reason for why you're dismissing this recommendation

The affected AWS account was temporarily created for an event ▼

Note - *optional*

These are test accounts that we will delete soon

Cancel Dismiss

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 Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Nella pagina Trusted Advisor Priorità, assicurati di essere nella 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 consigli risolti vengono visualizzati nella scheda Chiuso della pagina Trusted Advisor Priorità. Trusted Advisor Priority notifica al team del tuo account che hai risolto la raccomandazione.

Per risolvere una raccomandazione per tutti gli account della tua organizzazione AWS

L'account di gestione o gli amministratori delegati di Trusted Advisor Priority possono definire una raccomandazione per tutti i loro account.

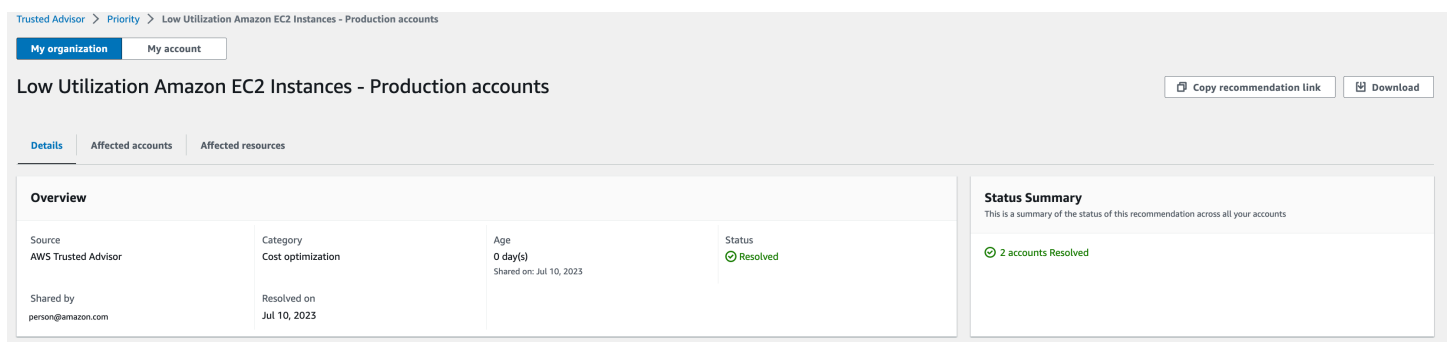
Note

Gli account dei membri non hanno accesso ai suggerimenti aggregati.

1. [Accedi alla Trusted Advisor console da casa](https://console.aws.amazon.com/trustedadvisor/)<https://console.aws.amazon.com/trustedadvisor/>.
2. Se utilizzi un account di AWS Organizations gestione o amministratore delegato, passa alla scheda Account personale.
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 consigli risolti vengono visualizzati nella scheda Chiuso della pagina Trusted Advisor Priorità. Trusted Advisor Priority notifica al team del tuo account che hai risolto la raccomandazione.

Example: Raccomandazione manuale di Trusted Advisor Priority

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



The screenshot shows the AWS Trusted Advisor console interface. At the top, there's a breadcrumb trail: "Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts". Below this, there are two tabs: "My organization" (selected) and "My account". The main heading is "Low Utilization Amazon EC2 Instances - Production accounts". To the right of the heading are two buttons: "Copy recommendation link" and "Download". Below the heading, there are three tabs: "Details" (selected), "Affected accounts", and "Affected resources". The "Details" tab is active, showing an "Overview" section with a table of recommendation details and a "Status Summary" section on the right.

Source	Category	Age	Status
AWS Trusted Advisor	Cost optimization	0 day(s) Shared on: Jul 10, 2023	Resolved

Shared by: person@amazon.com
Resolved on: Jul 10, 2023

Status Summary
This is a summary of the status of this recommendation across all your accounts
2 accounts Resolved

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 Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Se utilizzi un account di AWS Organizations gestione o amministratore delegato, 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.

Per riaprire una raccomandazione per tutti gli account della tua organizzazione AWS

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

Note

Gli account dei membri non hanno accesso ai suggerimenti aggregati.

1. [Accedi alla Trusted Advisor console da casa. https://console.aws.amazon.com/trustedadvisor/](https://console.aws.amazon.com/trustedadvisor/)
2. Nella pagina Trusted Advisor Priorità, assicurati di essere nella 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.

- Scegli Reopen (Riapri). Lo stato del suggerimento diventa In progress (In corso) e appare nella scheda Active (Attivo).

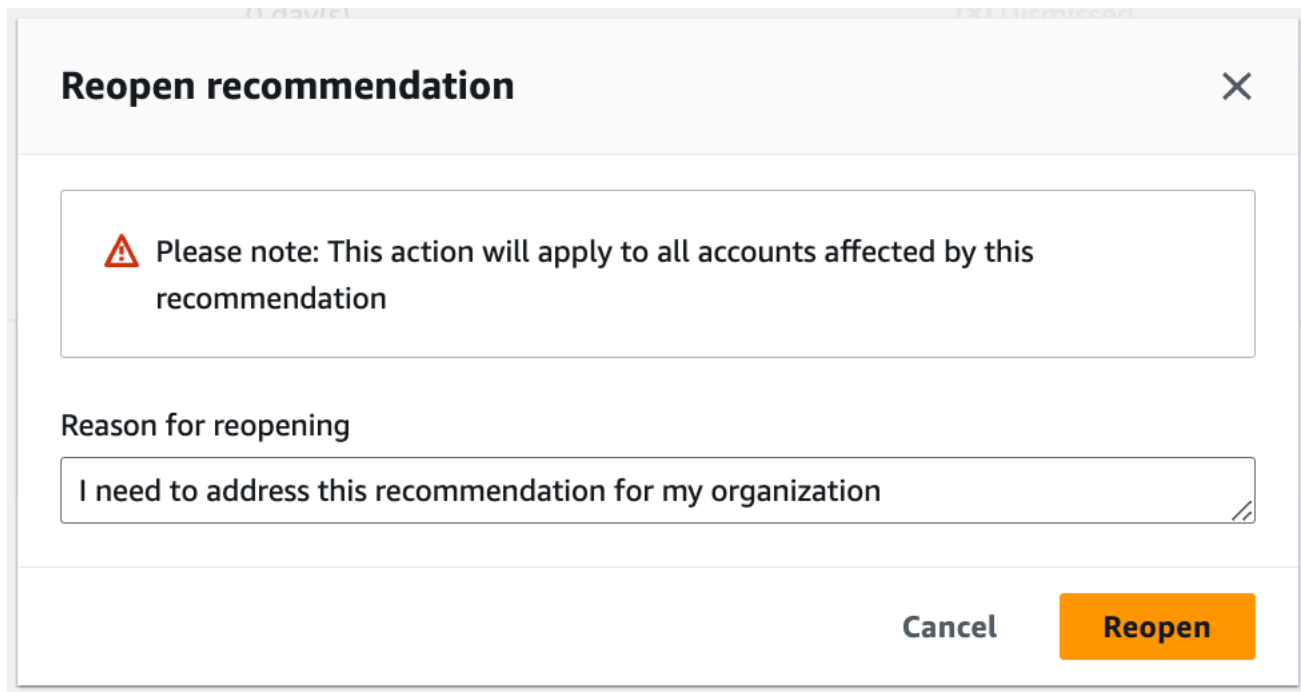
 Tip

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.

- Segui i passaggi riportati nei dettagli del suggerimento.

Example: riapre una raccomandazione da Priority Trusted Advisor

L'esempio seguente mostra un suggerimento che desideri riaprire.



Reopen recommendation ×

 Please note: This action will apply to all accounts affected by this recommendation

Reason for reopening

I need to address this recommendation for my organization

Cancel Reopen

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 Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa>.
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 di amministratore delegato possono esaminare, riconoscere, risolvere, ignorare e riaprire i consigli in Priority. Trusted Advisor

Dopo aver registrato un account, è necessario concedere all'amministratore delegato le autorizzazioni necessarie AWS Identity and Access Management per accedere a Priority. Trusted Advisor 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.

Per registrare un amministratore delegato per

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa> [come 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.

Per annullare la registrazione di un amministratore delegato di

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa> come 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).

Gestisci le notifiche Trusted Advisor prioritarie

Trusted Advisor Priority invia notifiche tramite 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. Puoi specificare la frequenza con cui ricevi gli aggiornamenti da Trusted Advisor Priority.

Se hai registrato account membri come amministratori delegati, questi possono anche configurare i propri account per ricevere notifiche e-mail Trusted Advisor prioritarie.

Trusted Advisor Le notifiche e-mail prioritarie non includono i risultati dei controlli per i singoli account e sono separate dalla notifica settimanale per Trusted Advisor Recommendations. 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 Trusted Advisor prioritarie.

Per gestire le notifiche Trusted Advisor prioritarie

1. Accedi alla Trusted Advisor console da <https://console.aws.amazon.com/trustedadvisor/casa> come account di gestione o 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. Puoi aggiungere e rimuovere contatti dalla pagina [Impostazioni account](#) della Gestione dei costi e fatturazione AWS console.
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'noreply@notifications.trustedadvisor.us-west-2.amazonaws.com indirizzo. Potrebbe essere necessario verificare che il tuo client di posta elettronica non contrassegni queste e-mail come spam.

Disattiva Trusted Advisor la priorità

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

Se disabiliti Trusted Advisor Priority e poi la riattivi in un secondo momento, puoi comunque visualizzare i consigli che il team del tuo account ha inviato prima di Trusted Advisor disabilitare Priority.

AWS Trusted Advisor verifica riferimento

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

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

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi anche utilizzare l'[AWS Trusted Advisor API](#) e il AWS Command Line Interface (AWS CLI) per accedere ai tuoi 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 disponi di un piano Basic Support o Developer Support, puoi utilizzare la Trusted Advisor console per accedere a tutti i controlli della [Limiti del servizio](#) categoria e ai seguenti controlli nelle categorie Security e Fault Tolerance:

- [Snapshot pubblici Amazon EBS](#)
- [Snapshot pubblici di Amazon RDS](#)
- [Autorizzazioni Bucket Amazon S3](#)
- [MFA sull'account root](#)
- [Gruppi di sicurezza — Porte specifiche senza restrizioni](#)
- [AWS STS utilizzo globale degli endpoint in tutto il mondo Regioni AWS](#)

Categorie di controllo

- [Ottimizzazione dei costi](#)
- [Performance](#)
- [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 non fa parte di AWS Organizations](#)
- [Consigli per l'ottimizzazione dei costi di Amazon Aurora per lo storage in cluster DB](#)
- [Endpoint Amazon Comprehend sottoutilizzati](#)
- [Consigli per l'acquisto di capacità riservata di Amazon DynamoDB](#)
- [Raccomandazioni per l'ottimizzazione dei costi di Amazon EBS per i volumi](#)
- [Volumi Amazon EBS con provisioning eccessivo](#)
- [Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per i gruppi Amazon EC2 Auto Scaling](#)
- [Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per le istanze](#)
- [Consolidamento di istanze Amazon EC2 per Microsoft SQL Server](#)
- [Istanze Amazon EC2 con provisioning eccessivo per Microsoft SQL Server](#)
- [Istanze Amazon EC2 interrotte](#)
- [Scadenza del lease di istanze riservate Amazon EC2](#)
- [Ottimizzazione delle istanze riservate Amazon EC2](#)
- [Amazon ECR Repository senza policy del ciclo di vita configurate](#)
- [Consigli per l'acquisto di nodi ElastiCache riservati Amazon](#)
- [AWS Fargate consigli per l'ottimizzazione dei costi per Amazon ECS](#)
- [Consigli per l'acquisto di nodi riservati Amazon MemoryDB](#)
- [Consigli per l'acquisto di istanze riservate di Amazon OpenSearch Service](#)
- [Consigli per l'ottimizzazione dei costi di Amazon RDS per le istanze DB](#)
- [Consigli per l'ottimizzazione dei costi di Amazon RDS per lo storage di istanze DB](#)
- [Istanze database inattive di Amazon RDS](#)
- [Consigli per l'acquisto di istanze riservate Amazon RDS](#)
- [Consigli per l'acquisto di nodi riservati Amazon Redshift](#)
- [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 raccomandazioni per l'ottimizzazione dei costi per le funzioni](#)
- [AWS Lambda funzioni con timeout eccessivi](#)
- [AWS Lambda funzioni con tassi di errore elevati](#)

- [AWS Lambda funzioni sovradimensionate per le dimensioni della memoria](#)
- [AWS Consigli per l'acquisto di Savings Plans per l'elaborazione](#)
- [AWS Consigli per l'acquisto di Savings Plans per Amazon SageMaker AI](#)
- [Problemi ad alto rischio di AWS Well-Architected per l'ottimizzazione dei costi](#)
- [Bilanciatori del carico inattivi](#)
- [Gateway NAT inattivi](#)
- [Inattivo AWS Network Firewall](#)
- [Endpoint di interfaccia VPC inattivi](#)
- [Endpoint Gateway Load Balancer inattivi](#)
- [Gateway NAT inattivi](#)
- [Istanze Amazon EC2 a basso utilizzo](#)
- [Indirizzi IP elastici non associati](#)
- [Volumi Amazon EBS sottoutilizzati](#)
- [Cluster Amazon Redshift sottoutilizzati](#)

Account AWS non fa parte di AWS Organizations

Description

Verifica se un Account AWS fa parte dell' AWS Organizations account di gestione appropriato.

AWS Organizations è un servizio di gestione degli account per il consolidamento di più AWS account in un'organizzazione gestita centralmente. 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 regole. AWS Config

Per ulteriori informazioni, consulta [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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz127

Origine

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

Criteri di avviso

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

Azione consigliata

Aggiungi questo AWS account come parte di AWS Organizations.

Per ulteriori informazioni, consulta il [Tutorial: creazione e configurazione di un'organizzazione](#).

Colonne del report

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

Consigli per l'ottimizzazione dei costi di Amazon Aurora per lo storage in cluster DB

Description

Controlla le configurazioni e i modelli di utilizzo dello storage del cluster Amazon Aurora DB per fornire consigli per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr17n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: uno storage cluster Aurora DB presenta un'azione di risparmio sui costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei consigli sui database Aurora e RDS](#)
- [Consigli di Amazon Aurora](#)
- [Impostazioni per Amazon Aurora](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Endpoint Amazon Comprehend sottoutilizzati

Description

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

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

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

Consigli per l'acquisto di capacità riservata di Amazon DynamoDB

Description

Verifica i modelli di utilizzo di Amazon DynamoDB e fornisce consigli per potenziali risparmi sui costi attraverso l'acquisto di capacità riservata.

Questo controllo genera raccomandazioni [nell'ambito del pagatore per il conto del pagatore e nell'ambito collegato per un conto collegato](#).

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr15n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account ha un'azione di risparmio sui costi identificata da Cost Optimization Hub per DynamoDB.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Capacità riservata DynamoDB](#)
- [Accesso ai consigli di prenotazione](#)
- [Capacità riservata di Amazon DynamoDB](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Raccomandazioni per l'ottimizzazione dei costi di Amazon EBS per i volumi

Description

Controlla le configurazioni dei volumi e i modelli di utilizzo di Amazon EBS per fornire suggerimenti per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr02n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: EBS Volume presenta un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei consigli sui volumi di Amazon EBS](#)
- [Parametri volume EBS](#)
- [Tipi di volume Amazon EBS](#)
- [Richiedi modifiche al volume di Amazon EBS](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Volumi Amazon EBS con provisioning eccessivo

Description

Note

Si tratta di un assegno precedente. Si consiglia di utilizzare il nuovo controllo (ID di controllo: [c1z7kmr02n](#)) che offre suggerimenti personalizzati aggiuntivi.

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

C016dfpM03

Criteri di avviso

Giallo: un volume EBS il cui approvvigionamento è stato eccessivo durante il periodo di lookback. Per determinare se un volume è sovra-fornito, prendiamo in considerazione tutte le metriche predefinite CloudWatch (inclusi IOPS e throughput). L'algoritmo utilizzato per identificare i volumi EBS sovradimensionati segue le best practice. AWS L'algoritmo viene aggiornato quando viene identificato un nuovo modello.

Azione 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
- Region
- 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

Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per i gruppi Amazon EC2 Auto Scaling

Description

Controlla le configurazioni e i modelli di utilizzo del gruppo Amazon EC2 Auto Scaling per fornire consigli per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione principale consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr01n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: il gruppo Amazon EC2 Auto Scaling dispone di un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei volumi consigliati di Amazon EC2 Auto Scaling](#)
- [Gruppi Amazon EC2 Auto Scaling](#)
- [Cos'è Amazon EC2 Auto Scaling](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per le istanze

Description

Controlla le configurazioni e i modelli di utilizzo delle istanze Amazon EC2 per fornire suggerimenti per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr00n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'istanza EC2 presenta un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di

questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei consigli per le istanze EC2](#)
- [Metriche delle istanze EC2](#)
- [Modifiche al tipo di istanza Amazon EC2](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Consolidamento di istanze Amazon EC2 per Microsoft SQL Server

Description

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. Secondo la Microsoft SQL Server Licensing Guide, stai pagando 4 licenze vCPU anche se un'istanza ha solo 1 o 2 v. CPUs È possibile consolidare le istanze di 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

Qsdfp3A4L2

Criteri di avviso

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

Operazione consigliata

Prendi in considerazione la possibilità di consolidare carichi di lavoro SQL Server più piccoli in istanze con almeno quattro v. CPUs

Risorse aggiuntive

- [Microsoft SQL Server in AWS](#)
- [Licenze Microsoft su AWS](#)
- [Guida alle licenze per Microsoft SQL Server](#)

Colonne del report

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

Istanze Amazon EC2 con provisioning eccessivo per Microsoft SQL Server

Description

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 vCPUs. Un'istanza con SQL Server Web può utilizzare fino a 32 vCPUs. 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 v CPUs utilizzabile da un'istanza di SQL Server e i prezzi 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

Qsdfp3A4L1

Criteri di avviso

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

Azione consigliata

Per l'edizione SQL Server Standard, valuta la possibilità di passare a un'istanza della stessa famiglia di istanze con 48 vCPUs. Per l'edizione Web di SQL Server, valuta la possibilità di passare a un'istanza della stessa famiglia di istanze con 32 vCPUs. Se richiede molta memoria, valuta la possibilità di passare a istanze R5 ottimizzate per la memoria.

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

Istanze Amazon EC2 interrotte

Description

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 AllowedDays. AWS 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

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

Scadenza del lease di istanze riservate Amazon EC2

Description

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.

Azione 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
- Platform (Piattaforma)
- Conteggio istanze
- Costo mensile corrente
- Risparmi mensili stimati
- Data di scadenza
- ID Istanza riservata
- Motivo

Ottimizzazione delle istanze riservate Amazon EC2

Description

Una parte importante dell'utilizzo AWS prevede il bilanciamento dell'acquisto di istanze riservate (RI) con l'utilizzo dell'istanza on demand. Questo controllo fornisce consigli in merito RIs ai quali contribuire a ridurre i costi derivanti 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 dell'anticipo parziale RIs può aiutare a ridurre i costi.

Azione consigliata

Consulta la pagina [Cost Explorer](#) per suggerimenti più dettagliati e personalizzati. Inoltre, consulta la [guida all'acquisto](#) per capire come effettuare l'acquisto RIs e le opzioni disponibili.

Risorse aggiuntive

- Informazioni su RIs come possono farti risparmiare denaro sono disponibili [qui](#).
- Per ulteriori informazioni su questo consiglio, consulta la sezione [Domande di controllo dell'ottimizzazione delle istanze riservate](#) nel Trusted Advisor FAQs.

Colonne del report

- Region
- Tipo di istanza
- Platform (Piattaforma)
- Numero consigliato RIs di acquisti
- Utilizzo medio previsto delle istanze riservate
- Risparmi stimati con i suggerimenti (mensile)
- Costo iniziale di RIs
- Costi stimati di RIs (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)

Amazon ECR Repository senza policy del ciclo di vita configurate

Description

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.

Azione 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
- Region

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

Consigli per l'acquisto di nodi ElastiCache riservati Amazon

Description

Controlla i tuoi modelli di ElastiCache utilizzo di Amazon per fornire consigli per potenziali risparmi sui costi attraverso gli acquisti di nodi riservati.

Questo controllo genera raccomandazioni relative all'[ambito del pagatore per l'account del pagatore e all'ambito collegato per un conto collegato](#).

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr13n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account ha un'azione di risparmio sui costi identificata da Cost Optimization Hub per Amazon ElastiCache.

Azione consigliata

Valuta [la possibilità di implementare la raccomandazione](#) Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Nodi riservati](#)
- [Accesso ai consigli di prenotazione](#)
- [Nodi ElastiCache riservati Amazon](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

AWS Fargate consigli per l'ottimizzazione dei costi per Amazon ECS

Description

Verifica le configurazioni e i modelli di utilizzo di Amazon ECS AWS Fargate per fornire suggerimenti per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr06n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: i servizi Amazon ECS attivi AWS Fargate prevedono un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei servizi Amazon ECS sui consigli di Fargate](#)
- [Metriche per i servizi Amazon ECS su Fargate](#)
- [AWS Fargate per Amazon ECS](#)
- [Aggiornamento di un servizio Amazon ECS tramite la console](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata

- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Consigli per l'acquisto di nodi riservati Amazon MemoryDB

Description

Controlla i tuoi modelli di utilizzo di Amazon MemoryDB per fornire consigli per potenziali risparmi sui costi attraverso l'acquisto di nodi riservati.

Questo controllo genera raccomandazioni [nell'ambito del pagatore per l'account del pagatore e nell'ambito collegato per un account collegato](#).

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr16n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account ha un'azione di risparmio sui costi identificata da Cost Optimization Hub for MemoryDB.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Nodi riservati di MemoryDB](#)
- [Accesso ai consigli di prenotazione](#)
- [Lavorare con nodi riservati](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Consigli per l'acquisto di istanze riservate di Amazon OpenSearch Service

Description

Verifica i tuoi modelli OpenSearch di utilizzo del servizio Amazon per fornire consigli per potenziali risparmi sui costi tramite acquisti di istanze riservate (RI).

Questo controllo genera raccomandazioni [nell'ambito del pagatore per l'account del pagatore e nell'ambito collegato per un account collegato](#).

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr14n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account ha un'azione di risparmio sui costi identificata da Cost Optimization Hub per Amazon OpenSearch Service.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Istanze riservate in Amazon Service OpenSearch](#)
- [Accesso ai consigli di prenotazione](#)
- [Acquisto di istanze riservate \(\)AWS CLI](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati

- Indicatore dell'ora dell'ultimo aggiornamento

Consigli per l'ottimizzazione dei costi di Amazon RDS per le istanze DB

Description

Controlla le configurazioni e i modelli di utilizzo delle tue istanze DB Amazon RDS per fornire consigli per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr03n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'istanza DB RDS presenta un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella

Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei consigli sul database RDS](#)
- [Metriche del database RDS](#)
- [Classi di istanza database](#)
- [Modifica di un'istanza database Amazon RDS](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Consigli per l'ottimizzazione dei costi di Amazon RDS per lo storage di istanze DB

Description

Controlla le configurazioni di storage e i modelli di utilizzo delle tue istanze database Amazon RDS per fornire suggerimenti per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr04n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: lo storage RDS DB prevede un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei consigli sul database RDS](#)
- [Archiviazione delle istanze database Amazon RDS](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)

- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Istanze database inattive di Amazon RDS

Description

Note

Si tratta di un assegno precedente. Si consiglia di utilizzare il nuovo controllo (ID di controllo: [c1z7kmr03n](#)) che offre suggerimenti personalizzati aggiuntivi.

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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

Ti39hal1fu8

Criteri di avviso

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

Azione 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

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

Consigli per l'acquisto di istanze riservate Amazon RDS

Description

Verifica i tuoi modelli di utilizzo di Amazon RDS per fornire consigli su potenziali risparmi sui costi tramite acquisti di istanze riservate (RI).

Questo controllo genera raccomandazioni [nell'ambito del pagatore per l'account del pagatore e nell'ambito collegato per un](#) account collegato.

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr11n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: EBS Volume presenta un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Istanza DB riservata per Amazon RDS](#)
- [Accesso ai consigli di prenotazione](#)
- [Acquisto di istanze DB riservate per Amazon RDS](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Consigli per l'acquisto di nodi riservati Amazon Redshift

Description

Verifica i tuoi modelli di utilizzo di Amazon Redshift per fornire consigli su potenziali risparmi sui costi attraverso l'acquisto di nodi riservati.

Questo controllo genera raccomandazioni relative all'[ambito del pagatore per l'account del pagatore e all'ambito collegato per un](#) account collegato.

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr12n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account ha un'azione di risparmio sui costi identificata da Cost Optimization Hub per Amazon Redshift.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Nodi riservati](#)
- [Accesso ai consigli di prenotazione](#)
- [Acquisto di un nodo riservato](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

Set di registri delle risorse di latenza Amazon Route 53

Description

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

Per consentire ad Amazon Route 53 di indirizzare le query verso la latenza di rete Regione AWS con la latenza di rete più bassa, è necessario creare set di record di risorse di latenza per un particolare nome di dominio (ad esempio example.com) in diverse regioni. 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 dai AWS servizi non verranno visualizzate nei risultati del controllo.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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 definisci set di record di risorse di latenza per ciascuna di esse; vedi Routing basato sulla latenza.](#)

Se non vuoi usarne più Regioni AWS, dovresti usare un semplice set di record di risorse. 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

Description

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 allo storage Amazon S3 Standard-IA 30 giorni dopo la creazione o ad Amazon 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 del controllo utilizzando i parametri delle 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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
- Region
- Risorsa
- AWS Config Regola
- Parametri di input

Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3

Description

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. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate. Per i clienti Business, Enterprise On-Ramp o Enterprise Support, puoi utilizzare l'`BatchUpdateRecommendationResourceExclusionAPI` per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione 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
- Region
- 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

Description

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 che desideri 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione consigliata

Configura le policy del ciclo di vita per i bucket di Amazon S3 per gestire gli oggetti in modo da archivarli 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
- Region
- Risorsa
- AWS Config Regola
- Parametri di input
- Ora ultimo aggiornamento

AWS Lambda raccomandazioni per l'ottimizzazione dei costi per le funzioni

Description

Verifica le AWS Lambda configurazioni e i modelli di utilizzo per fornire consigli per potenziali risparmi sui costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di Centrale ottimizzazione costi AWS.

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr05n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: la funzione Lambda presenta un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione. La raccomandazione è uno dei tipi di raccomandazione elencati in [Comprensione delle strategie di ottimizzazione dei costi](#) nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Utilizza i consigli dettagliati AWS Compute Optimizer per comprendere il potenziale impatto di queste modifiche su costi e prestazioni.

Risorse aggiuntive

- [Visualizzazione dei consigli sulle funzioni Lambda](#)
- [Parametri della funzione Lambda](#)
- [Configurazione delle funzioni AWS Lambda](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

AWS Lambda funzioni con timeout eccessivi

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione 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 con AWS LambdaAWS X-Ray](#)
- [Accesso ai CloudWatch log di Amazon per AWS Lambda](#)
- [Esempio di applicazione Error Processor per AWS Lambda](#)

Colonne del report

- Stato
- Region
- 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 tassi di errore elevati

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione 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](#)
- [Esempio di applicazione Error Processor per AWS Lambda](#)

Colonne del report

- Stato
- Region
- ARN della funzione
- Tasso di errore massimo giornaliero

- Data del tasso di errore massimo
- Tasso di errore medio giornaliero
- Costo di calcolo giornaliero perso
- Richiami per il giorno corrente
- Tasso di errore del giorno corrente
- *Richiamazioni giornaliere medie
- Ora ultimo aggiornamento

AWS Lambda funzioni sovradimensionate per le dimensioni della memoria

Description

Note

Si tratta di un assegno precedente. Si consiglia di utilizzare il nuovo controllo (ID di controllo: [c1z7kmr05n](#)) che offre suggerimenti personalizzati aggiuntivi.

Controlla le AWS Lambda funzioni che sono state richiamate almeno una volta durante il periodo di lookback. 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione 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
- Region
- 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

AWS Consigli per l'acquisto di Savings Plans per l'elaborazione

Description

Verifica i modelli di utilizzo dell' AWS elaborazione su Amazon EC2 AWS FargateAWS Lambda e fornisce consigli per l'acquisto di Savings Plans. Con questi consigli, puoi impegnarti a garantire un importo di utilizzo costante, misurato in dollari all'ora, in cambio di tariffe scontate.

Questo controllo genera raccomandazioni relative all'[ambito del pagatore per il conto pagante e all'ambito collegato per un](#) conto collegato.

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr09n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account dispone di un'azione di riduzione dei costi identificata da Cost Optimization Hub per le risorse di elaborazione.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Cosa sono i Savings Plans?](#)
- [Tipi di Savings Plans](#)
- [Acquisto di Savings Plans](#)

Colonne del report

- Stato

- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

AWS Consigli per l'acquisto di Savings Plans per Amazon SageMaker AI

Description

Verifica l'utilizzo di Amazon SageMaker AI e fornisce consigli per l'acquisto di Savings Plans. Con questi consigli, puoi impegnarti a garantire un importo di utilizzo costante, misurato in dollari all'ora, in cambio di tariffe scontate.

Questo controllo genera raccomandazioni relative all'[ambito del pagatore per il conto pagante e all'ambito collegato per un](#) conto collegato.

Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7kmr08n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: l'account ha un'azione di risparmio sui costi identificata da Cost Optimization Hub per Amazon SageMaker AI.

Azione consigliata

Valuta la possibilità [di implementare la raccomandazione](#). Per ulteriori informazioni sull'implementazione di questi consigli, consulta il AWS Cloud Financial Management (CFM) [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Cosa sono i Savings Plans?](#)
- [Tipi di Savings Plans](#)
- [Acquisto di Savings Plans](#)

Colonne del report

- Stato
- Region
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Indicatore dell'ora dell'ultimo aggiornamento

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

Description

Verifica la presenza di problemi ad alto rischio (HRIs) per i carichi di lavoro nell'ambito dell'ottimizzazione dei costi. 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

Wxdfp4B1L1

Criteri di avviso

- Rosso: almeno un problema attivo ad alto rischio è stato identificato nel pilastro di ottimizzazione dei costi per AWS Well-Architected.
- Verde: non sono stati rilevati problemi attivi ad alto rischio nel pilastro di 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
- Region
- 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 identificati per l'ottimizzazione dei costi HRIs
- Numero di HRIs problemi risolti per l'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

Description

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).

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Region
- Nome del load balancer
- Motivo
- Risparmi mensili stimati

Gateway NAT inattivi

Description

Controlla le configurazioni e i modelli di utilizzo del gateway NAT per identificare i gateway NAT inattivi o sottoutilizzati che potrebbero essere candidati all'ottimizzazione dei costi.

Per ogni risorsa, Trusted Advisor mostra solo l'azione più consigliata di. Centrale ottimizzazione costi AWS

Per utilizzare questo controllo, è necessario attivare [Cost Optimization Hub](#) e [AWS Compute Optimizer](#).

ID di controllo

c1z7kmr18n

Origine

Centrale ottimizzazione costi AWS

Criteri di avviso

Giallo: il gateway NAT prevede un'azione di riduzione dei costi identificata da Cost Optimization Hub.

Azione consigliata

Valuta la possibilità di implementare la raccomandazione per eliminare il gateway NAT inattivo. Per ulteriori informazioni sull'implementazione di questa raccomandazione, consulta il AWS Cloud Financial Management [Service Cost Optimization Playbook](#).

Risorse aggiuntive

- [Visualizzazione dei suggerimenti sulle risorse inattive](#)

- [Lavora con i gateway NAT](#)
- [Gateway NAT](#)

Colonne del report

- Stato
- Region
- Resource ID (ID risorsa)
- Operazione consigliata
- Riepilogo delle risorse attuali
- Riepilogo delle risorse consigliate
- Costo mensile stimato
- Risparmi mensili stimati
- Timestamp dell'ultimo aggiornamento

Inattivo AWS Network Firewall

Description

Controlla gli AWS Network Firewall endpoint e ti avvisa quando il Network Firewall sembra essere inattivo.

Un Network Firewall è considerato inattivo se su tutti i suoi endpoint non sono stati elaborati dati negli ultimi 30 giorni. Gli endpoint Network Firewall sono soggetti a tariffe orarie. Questo controllo segnala la presenza di Network Firewall senza dati elaborati negli ultimi 30 giorni. È consigliabile rimuovere i firewall di rete non utilizzati o aggiornare l'architettura.

ID di controllo

c2v1fg0bfw

Criteri di avviso

- Giallo: il Network Firewall ha elaborato 0 byte negli ultimi 30 giorni.
- Verde: il Network Firewall ha elaborato più di 0 byte negli ultimi 30 giorni.

Operazione consigliata

Se il Network Firewall non è stato utilizzato negli ultimi 30 giorni, valuta la possibilità di eliminarlo.

Se viene utilizzato un Transit Gateway per la comunicazione tra VPC, prendete in considerazione l'implementazione dei firewall di rete in architetture di ispezione della rete centralizzate. In questo modo è possibile ridurre i costi orari dei firewall di rete inattivi.

Risorse aggiuntive

[Prezzi di AWS Network Firewall](#)

[Modelli di implementazione delle ispezioni con AWS Network Firewall](#)

Colonne del report

- Stato
- Region
- Network Firewall Arn
- Id VPC
- Sottoreti
- TotalBytesProcessed
- Ora ultimo aggiornamento

Endpoint di interfaccia VPC inattivi

Description

Controlla gli endpoint dell'interfaccia VPC e ti avvisa quando gli endpoint sembrano inattivi. Un endpoint di interfaccia VPC è considerato inattivo se non contiene dati elaborati negli ultimi 30 giorni. Gli endpoint dell'interfaccia VPC hanno tariffe orarie e costi di elaborazione dei dati. Questo controllo ti avvisa sugli endpoint dell'interfaccia VPC con 0 dati elaborati negli ultimi 30 giorni. È consigliabile rimuovere gli endpoint dell'interfaccia VPC inutilizzati o aggiornare l'architettura.

ID di controllo

c2v1fg0jp6

Criteri di avviso

- Giallo: l'endpoint dell'interfaccia VPC ha elaborato 0 byte negli ultimi 30 giorni.
- Verde: l'endpoint dell'interfaccia VPC ha elaborato più di 0 byte negli ultimi 30 giorni

Operazione consigliata

Se l'endpoint dell'interfaccia VPC non è stato utilizzato negli ultimi 30 giorni, valuta la possibilità di eliminare l'endpoint dell'interfaccia VPC.

Se Transit Gateway viene utilizzato per la comunicazione tra VPC, prendi in considerazione l'implementazione degli endpoint dell'interfaccia VPC in un'architettura centralizzata per ridurre le tariffe orarie sugli endpoint di interfaccia VPC inattivi.

Risorse aggiuntive

- [AWS PrivateLink Prezzi](#)
- [Accesso centralizzato agli endpoint privati VPC](#)

Colonne del report

- Stato
- Region
- ID endpoint VPC
- Id VPC
- ID sottorete
- Nome del servizio
- TotalBytesProcessed
- Ora ultimo aggiornamento

Endpoint Gateway Load Balancer inattivi

Description

Controlla gli endpoint del Gateway Load Balancer e avvisa quando sembrano inattivi. Un endpoint Gateway Load Balancer è considerato sottoutilizzato se non contiene dati elaborati negli ultimi 30 giorni. Gli endpoint Gateway Load Balancer hanno tariffe orarie e tariffe per l'elaborazione dei dati. Questo controllo ti avvisa degli endpoint Gateway Load Balancer con 0 dati elaborati negli ultimi 30 giorni. Ti consigliamo di rimuovere gli endpoint Gateway Load Balancer non utilizzati o di aggiornare l'architettura.

ID di controllo

c2v1fg0k35

Criteri di avviso

- Giallo: l'endpoint Gateway Load Balancer ha elaborato 0 byte negli ultimi 30 giorni
- Verde: l'endpoint Gateway Load Balancer ha elaborato più di 0 byte negli ultimi 30 giorni

Operazione consigliata

Se l'endpoint Gateway Load Balancer non è stato utilizzato negli ultimi 30 giorni, valuta la possibilità di eliminare l'endpoint VPC.

Se si utilizza Transit Gateway per la comunicazione tra VPC, prendete in considerazione l'implementazione degli endpoint Gateway Load Balancer in un'architettura di ispezione della rete centralizzata per ridurre le tariffe orarie sugli endpoint Gateway Load Balancer inattivi.

Risorse aggiuntive

[Prezzi di AWS PrivateLink](#)

[Architettura di ispezione centralizzata con AWS Gateway Load Balancer e AWS Transit Gateway](#)

Colonne del report

- Stato
- Region
- ID endpoint VPC
- Id VPC
- ID sottorete
- Nome del servizio
- TotalBytesProcessed
- Ora ultimo aggiornamento

Gateway NAT inattivi

Description

Verifica la presenza di gateway non attivi nei gateway NAT. Un gateway NAT è considerato inattivo se nessun dato (0 byte) è stato elaborato negli ultimi 30 giorni. I gateway NAT prevedono tariffe orarie e tariffe per l'elaborazione dei dati.

ID di controllo

c2v1fg022t

Criteri di avviso

- Giallo: il gateway NAT ha elaborato 0 byte negli ultimi 30 giorni
- Verde: il gateway NAT ha elaborato più di 0 byte negli ultimi 30 giorni

Operazione consigliata

Prendi in considerazione l'eliminazione di tutti i gateway NAT che non sono stati utilizzati negli ultimi 30 giorni e che non sono necessari per l'accesso alla rete esterna al di fuori del VPC.

Se viene utilizzato un Transit Gateway per la comunicazione tra VPC, prendete in considerazione l'implementazione di un gateway NAT centralizzato per l'accesso all'architettura Internet. In questo modo è possibile ridurre il costo orario dei gateway NAT inattivi.

Risorse aggiuntive

[Prezzi di NAT Gateway](#)

[Accesso centralizzato a Internet](#)

Colonne del report

- Stato
- Region
- ID gateway NAT
- ID sottorete
- Id VPC
- TotalBytesFromDest
- TotalBytesFromSrc
- TotalBytes
- Ora ultimo aggiornamento

Istanze Amazon EC2 a basso utilizzo

Description

Note

Si tratta di un assegno obsoleto. Si consiglia di utilizzare il nuovo controllo (ID di controllo: [c1z7kmr00n](#)) che offre suggerimenti personalizzati aggiuntivi.

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

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

Qch7DwouX1

Criteri di avviso

Giallo: un'istanza ha registrato un utilizzo medio giornaliero della CPU pari o inferiore al 10% e una quantità di rete pari o inferiore a 5 MB I/O in 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 di I/O 14 giorni in rete
- Numero di giorni con utilizzo ridotto

Indirizzi IP elastici non associati

Description

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

EIPs sono indirizzi IP statici progettati per il cloud computing dinamico. A differenza degli indirizzi IP statici tradizionali, EIPs maschera l'errore di un'istanza o di una zona di disponibilità rimappando un indirizzo IP pubblico su un'altra istanza del tuo account. Un addebito nominale viene imposto per un EIP non associato a un'istanza in esecuzione.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Region
- Indirizzo IP

Volumi Amazon EBS sottoutilizzati

Description

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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, risorse incluse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

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

Note

Se hai attivato il tuo account per AWS Compute Optimizer, ti consigliamo di utilizzare invece il controllo dei volumi over-provisioned di Amazon EBS. Per ulteriori informazioni, consulta [Attiva AWS Compute Optimizer i Trusted Advisor controlli](#).

Cluster Amazon Redshift sottoutilizzati

Description

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
- Region
- Cluster
- Tipo di istanza
- Motivo
- Risparmi mensili stimati

Performance

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 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](#)
- [AWS Lambda funzioni non sufficientemente fornite per quanto riguarda le dimensioni 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 ad alto utilizzo della CPU](#)

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

Description

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 database al cluster e indirizzando il carico di lavoro di lettura all'endpoint di sola lettura del cluster di database.

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

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

Dimensionamento automatico di Amazon DynamoDB non abilitato

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz136

Origine

AWS Config Regola gestita: dynamodb-autoscaling-enabled

Criteri di avviso

Giallo: la scalabilità automatica non è abilitata per gli indici secondari globali delle tabelle DynamoDB and/or .

Operazione consigliata

A meno che non disponga già di un meccanismo per scalare automaticamente il throughput assegnato della tabella DynamoDB (gli indici secondari globali) in base ai requisiti and/or del carico di lavoro, valuta la possibilità di attivare la scalabilità automatica per le tabelle Amazon DynamoDB.

Per ulteriori informazioni, consulta [Using the Console di gestione AWS with DynamoDB auto scalingp](#).

Risorse aggiuntive

[Gestione automatica della capacità effettiva di trasmissione con il dimensionamento automatico di DynamoDB](#)

Colonne del report

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

Ottimizzazione Amazon EBS non abilitata

Description

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 fornisce capacità aggiuntiva dedicata per Amazon EBS I/O. This optimization provides the best performance for your Amazon EBS volumes by minimizing contention between Amazon EBS I/O e 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa

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

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

Description

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

- Status
- Regione/AZ
- ID volume
- Nome volume
- Allegato volume

- ID istanza
- Tipo di istanza
- Ottimizzazione per EBS

Volumi Amazon EBS con provisioning insufficiente

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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 consigliato (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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- AWS Config Regola

- Parametri di input
- Ora ultimo aggiornamento

Ottimizzazione della velocità effettiva da Amazon EC2 a EBS

Description

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

- Status
- Region
- ID istanza
- Tipo di istanza
- Tempo vicino al limite massimo

Il tipo di virtualizzazione EC2 è paravirtuale

Description

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. Ciò è dovuto ai miglioramenti apportati alla virtualizzazione HVM e alla disponibilità di driver fotovoltai per HVM AMIs, che hanno colmato il divario prestazionale che storicamente esisteva tra i guest PV e HVM. È importante notare che i tipi di istanza della generazione attuale non supportano PV. AMIs 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Limite massimo di memoria di Amazon ECS

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz176

Origine

AWS Config Regola gestita: -hard-limit ecs-task-definition-memory

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

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

Ottimizzazione della modalità di velocità di trasmissione effettiva di Amazon EFS

Description

Verifica se il file system Amazon EFS è attualmente configurato per utilizzare la modalità throughput Bursting. Il throughput di Amazon EFS Bursting utilizza i «crediti» per prestazioni superiori al throughput di base (50 per KiB/s GiB). Una volta esauriti i crediti, le prestazioni rallentano fino a raggiungere il throughput di base, il che può causare rallentamenti, guasti delle applicazioni e timeout per gli utenti. Per ulteriori informazioni sulla modalità bursting, consulta la modalità [Throughput](#) nella Amazon EFS User Guide

ID di controllo

c1dfprch02

Criteri di avviso

- Giallo: il file system utilizza la modalità Bursting throughput (velocità di trasmissione effettiva).

Operazione consigliata

Se i crediti di throughput Bursting sono bassi o esauriti, valuta la possibilità di passare alla modalità Provisioned o Elastic throughput per fornire agli utenti e alle applicazioni il throughput desiderato. Con il throughput Provisioned, è possibile impostare la velocità effettiva richiesta per il carico di lavoro e pagare in base alla quantità di throughput abilitata per il file system. Se non sei sicuro dei tuoi requisiti di throughput, puoi utilizzare la modalità Elastic Throughput, in cui la velocità di trasmissione si adatta elasticamente al carico di lavoro e paghi solo in base all'uso effettivo, misurato in base al totale dei dati trasferiti. Puoi aggiornare la configurazione del file system per passare da una modalità di throughput all'altra in qualsiasi momento. Per ulteriori informazioni sui prezzi di throughput, consulta la pagina dei prezzi di [Amazon EFS](#). Puoi anche stimare i costi utilizzando il [Calcolatore dei prezzi AWS](#).

Risorse aggiuntive

- [Produttività vertiginosa](#)
- [Prezzi di Amazon EFS](#)
- [Calcolatore dei prezzi AWS](#)

Colonne del report

- Status
- Region
- ID dei file system EFS

- Modalità di velocità di trasmissione effettiva
- Ora ultimo aggiornamento

Il parametro Amazon RDS autovacuum è disattivato

Description

Il parametro autovacuum è disattivato per le tue istanze DB. La disattivazione del parametro autovacuum aumenta le dimensioni della tabella e dell'indice e influisce sulle prestazioni.

È consigliabile attivare il parametro 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

I cluster Amazon RDS DB supportano solo volumi fino a 64 TiB

Description

I cluster di database in uso supportano solo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Aggiornare la versione del motore dei cluster di database 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

- Status
- Region
- Risorsa
- Nome del motore

- Versione del motore attuale
- Valore consigliato
- Ora ultimo aggiornamento

Istanze database Amazon RDS nei cluster con classi di istanze eterogenee

Description

È consigliabile utilizzare la stessa classe e le stesse dimensioni di istanza database per tutte le istanze database nel 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Utilizzare la stessa classe e le stesse dimensioni di istanza database per tutte le istanze database nel 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 delle 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

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Istanze database Amazon RDS nei cluster con dimensioni di istanze eterogenee

Description

È consigliabile utilizzare la stessa classe e le stesse dimensioni di istanza database per tutte le istanze database nel 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Utilizzare la stessa classe e le stesse dimensioni di istanza database per tutte le istanze database nel 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 delle 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

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

I parametri di memoria DB di Amazon RDS sono diversi da quelli predefiniti

Description

I parametri di memoria delle istanze database sono significativamente diversi dai valori predefiniti. Queste impostazioni possono influire sulle prestazioni e causare errori.

È consigliabile reimpostare i parametri di memoria personalizzati per l'istanza database sui valori predefiniti nel gruppo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Reimpostare i parametri di memoria sui valori predefiniti.

Risorse aggiuntive

Per ulteriori informazioni, consultare [Best practice per la configurazione dei parametri per Amazon RDS per MySQL, parte 1: Parametri relativi alle prestazioni](#).

Colonne del report

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro Amazon RDS `enable_indexonlyscan` è disattivato

Description

Il pianificatore o lo strumento di ottimizzazione di query non può utilizzare il tipo di piano di scansione del solo indice se è disabilitato.

Ti consigliamo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro Amazon RDS `enable_indexscan` è disattivato

Description

Il pianificatore o lo strumento di ottimizzazione di query non può utilizzare il tipo di piano di scansione del solo indice quando il parametro è disattivato.

Ti consigliamo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro `general_logging` di Amazon RDS è attivato

Description

La registrazione di log generali dell'istanza database è attivata. Questa impostazione è utile per la risoluzione dei problemi dei database. Tuttavia, l'attivazione della registrazione generale aumenta la quantità di I/O operazioni e lo spazio di archiviazione allocato, il che potrebbe causare conflitti e un peggioramento delle prestazioni.

Controllare i requisiti per l'utilizzo della registrazione di log generali. Si consiglia 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Controllare i requisiti per l'utilizzo della registrazione di log generali. 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato

- Ora ultimo aggiornamento

Parametro Amazon RDS Innodb_change_buffering che utilizza un valore inferiore a quello ottimale

Description

Il buffering delle modifiche consente a un'istanza database MySQL di rinviare alcune scritture necessarie per mantenere gli indici secondari. Questa funzionalità è utile in ambienti con dischi lenti. La modifica della configurazione del buffering ha migliorato leggermente le prestazioni del database, ma ha causato un ritardo nel ripristino in caso di arresto anomalo e tempi di shutdown prolungati 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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, consultare [Best practice per la configurazione dei parametri per Amazon RDS per MySQL, parte 1: Parametri relativi alle prestazioni](#).

Colonne del report

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro `innodb_open_files` di Amazon RDS è basso

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

- Status

- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro `innodb_stats_persistent` di Amazon RDS è disattivato

Description

L'istanza database non è configurata per memorizzare le statistiche InnoDB sul disco. Quando le statistiche non vengono archiviate, vengono ricalcolate ogni volta che si riavvia l'istanza e si accede alla tabella. Questo comporta 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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, consultare [Best practice per la configurazione dei parametri per Amazon RDS per MySQL, parte 1: Parametri relativi alle prestazioni](#).

Colonne del report

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Istanza Amazon RDS con capacità di sistema insufficiente

Description

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:

O ut-of-memory uccide: quando un processo sull'host del database viene interrotto a causa della riduzione della memoria a livello del sistema operativo, il contatore di uccisioni (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 per 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

Out-of-memory sono state rilevate interruzioni: 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

- Status
- Region
- Risorsa
- Out-of-memory uccisioni (contare)
- Scambio eccessivo (numero)
- Ultimo periodo di rilevamento
- Ora ultimo aggiornamento

Il volume magnetico Amazon RDS è in uso

Description

L'istanza database sta utilizzando l'archiviazione magnetica. L'archiviazione magnetica non è consigliabile per la maggior parte delle istanze database. Scegliere un tipo di archiviazione diverso: per uso generico (SSD) o capacità di IOPS allocata.

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Scegliere un tipo di archiviazione diverso: per uso generico (SSD) o capacità di IOPS allocata.

Risorse aggiuntive

Lo storage magnetico è un tipo di storage 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

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

I gruppi di parametri Amazon RDS non utilizzano pagine enormi

Description

Le pagine di grandi dimensioni possono aumentare la scalabilità del database, ma l'istanza database in uso non le utilizza. 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro della cache delle query di Amazon RDS è attivato

Description

Quando le modifiche richiedono l'eliminazione della cache delle query, l'istanza database 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. È consigliabile 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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, consultare [Best practice per la configurazione dei parametri per Amazon RDS per MySQL, parte 1: Parametri relativi alle prestazioni](#).

Colonne del report

- Status

- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

È richiesto l'aggiornamento della classe di istanza delle risorse Amazon RDS

Description

Il tuo 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. È consigliabile eseguire l'istanza database con una classe di istanza database di generazione 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Classe di istanza database
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Risorse Amazon RDS: è richiesto l'aggiornamento delle versioni principali

Description

I database con la versione principale corrente per il motore di database non saranno supportati. Si consiglia 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Eseguire l'aggiornamento alla versione principale più recente per il motore di database.

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. blue/green

Per maggiori informazioni, consulta le seguenti risorse:

- [Aggiornamento di una versione del motore di istanze DB](#)
- [Aggiornamenti Amazon Aurora](#)
- [Utilizzo di Amazon RDS Blue/Green Deployments per gli aggiornamenti del database](#)

Colonne del report

- Status
- Region
- 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

Description

Si consiglia di aggiornare la versione principale all'ultima versione del motore supportata da Amazon RDS per procedere 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

È consigliabile 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

- Status
- Region
- 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

Description

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.

 Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, risorse incluse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Status
- 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

AWS Lambda funzioni non sufficientemente fornite per quanto riguarda le dimensioni della memoria

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

C016dfpM06

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

- Status
- Region
- 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

Description

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 riservato minimo e massimo utilizzando `ConcurrencyLimitHigh` parametri `concurrencyLimitLow` 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Problemi ad alto rischio di AWS Well-Architected per le prestazioni

Description

Verifica la presenza di problemi ad alto rischio (HRIs) per i carichi di lavoro nel pilastro delle prestazioni. 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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 identificati per le prestazioni HRIs
- Numero di HRIs risolti per le prestazioni
- Numero di domande risposte per Prestazioni
- Numero totale di domande nel pilastro Prestazioni
- Ora ultimo aggiornamento

CloudFront Nomi di dominio alternativi

Description

Note

Questo controllo si applica alle CloudFront distribuzioni Amazon classiche.

Verifica che il DNS sia configurato correttamente nelle CloudFront distribuzioni Amazon classiche che utilizzano nomi di dominio alternativi (). CNAMEs

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

- Status
- ID distribuzione
- Nome di dominio della distribuzione
- Nome di dominio alternativo
- Motivo

CloudFront Ottimizzazione della distribuzione dei contenuti

Description

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.

 Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, risorse incluse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Status
- Region
- 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

Description

Note

Questo controllo si applica alle CloudFront distribuzioni Amazon classiche.

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 eseguite dalle edge cache CloudFront](#)
- [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 ad alto utilizzo della CPU

Description

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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, risorse incluse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

ZRxQ1Psb6c

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 CSPM per il tuo Account AWS, puoi visualizzare i risultati nella Trusted Advisor console. Per informazioni, consulta [Visualizzazione AWS Security Hub CSPM dei controlli 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 CSPM .

Controlla i nomi

- [Gruppo di sicurezza per Application Load Balancer](#)
- [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](#)
- [Connessioni peering VPC di Amazon con risoluzione DNS disabilitata](#)
- [Protocollo crittografato per gruppi target di Application Load Balancer](#)
- [AWS Backup Vault senza una politica basata sulle risorse per impedire l'eliminazione dei punti di ripristino](#)
- [AWS CloudTrail Registrazione degli eventi di gestione](#)
- [AWS Lambda Funzioni che utilizzano runtime obsoleti](#)
- [AWS Well-Architected Problemi ad alto rischio di per la sicurezza](#)
- [CloudFront Certificati SSL personalizzati nell'IAM Certificate Store](#)
- [CloudFront Certificato SSL sul server di origine](#)
- [Sicurezza del Listener ELB](#)
- [Gruppi di sicurezza Classic Load Balancer](#)
- [Exposed Access Keys](#)
- [Rotazione delle chiavi di accesso IAM](#)
- [Accesso esterno a IAM Access Analyzer](#)
- [Policy delle Password IAM](#)
- [Provider di identità IAM SAML 2.0](#)
- [MFA sull'account root](#)
- [Chiave di accesso utente root](#)
- [Gruppi di sicurezza — Porte specifiche senza restrizioni](#)

- [Gruppi di sicurezza — Accesso illimitato](#)

Gruppo di sicurezza per Application Load Balancer

Description

Verifica i gruppi di sicurezza collegati all'Application Load Balancer e ai relativi target Amazon EC2. I gruppi di sicurezza Application Load Balancer devono consentire solo le porte in ingresso configurate in un listener. I gruppi di sicurezza di una destinazione non devono accettare connessioni dirette da Internet nella stessa porta sulla quale la destinazione riceve il traffico dal sistema di bilanciamento del carico.

Se un gruppo di sicurezza consente l'accesso a porte non configurate per il bilanciamento del carico o consente l'accesso diretto agli obiettivi, aumenta il rischio di perdita di dati o di attacchi dannosi.

Questo controllo esclude i seguenti gruppi:

- Gruppi target non associati a indirizzi IP o istanze EC2.
- Regole dei gruppi di sicurezza per il traffico IPv6 .

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

8604e947f2

Criteri di avviso

- Rosso: Target ha un IP pubblico e un gruppo di sicurezza che consente connessioni in entrata sulla porta di controllo di destinazione da qualsiasi luogo (0.0.0.0/0).
- Rosso: Target ha un IP pubblico e un gruppo di sicurezza che consente connessioni in entrata sulla porta di traffico da qualsiasi luogo (0.0.0.0/0).

- Rosso: Application Load Balancer ha l'autenticazione abilitata e target consente le connessioni in entrata sulla porta di traffico da qualsiasi luogo (0.0.0.0/0).
- Giallo: il gruppo di sicurezza di Target consente le connessioni in entrata sulla porta di traffico da qualsiasi luogo (0.0.0.0/0).
- Giallo: il gruppo di sicurezza di Target consente le connessioni in entrata sulla porta di controllo di Target da qualsiasi luogo (0.0.0.0/0).
- Giallo: il gruppo di sicurezza Application Load Balancer consente le connessioni in entrata su porte che non dispongono di un listener corrispondente.
- Giallo: il gruppo di sicurezza di Target consente le connessioni in entrata sulla porta di controllo di destinazione da un gruppo di sicurezza non collegato ad Application Load Balancer.
- Verde: il gruppo di sicurezza Application Load Balancer consente solo connessioni in entrata su porte che corrispondono a un listener.

Operazione consigliata

Per una maggiore sicurezza, assicurati che i tuoi gruppi di sicurezza consentano solo i flussi di traffico necessari:

- I gruppi di sicurezza di Application Load Balancer dovrebbero consentire le connessioni in entrata solo per le stesse porte configurate nei relativi listener.
- Utilizza gruppi di sicurezza esclusivi per i sistemi di bilanciamento del carico e le destinazioni.
- I gruppi di sicurezza Target devono consentire le connessioni nella porta di traffico solo dai sistemi di bilanciamento del carico a cui sono associati.
- I gruppi di sicurezza target devono consentire le connessioni nella porta di controllo di destinazione solo dai sistemi di bilanciamento del carico a cui sono associati.

Risorse aggiuntive

- [Controlla il traffico verso le tue risorse AWS utilizzando gruppi di sicurezza](#)
- [Gruppi di sicurezza per l'Application Load Balancer](#)

Colonne del report

- Status
- Region
- Gruppo di destinazione
- Nome ALB
- ALB SG ID

- ID SG di destinazione
- Autenticazione abilitata
- Ora ultimo aggiornamento

Periodo di conservazione di Amazon CloudWatch Log Group

Description

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 i `MinRetentionTime` parametri `LogGroupName` 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Fine del supporto per le istanze Amazon EC2 con Microsoft SQL Server

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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, prendi in considerazione il programma di End-of-Support migrazione (EMP) per Windows Server. Per ulteriori informazioni, consulta il [sito Web di EMP](#).

Risorse aggiuntive

- [Preparati per la fine del supporto per SQL Server con AWS](#)
- [Microsoft SQL Server in AWS](#)

Colonne del report

- Status
- Region
- 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

Description

Questo controllo ti avvisa se le versioni di Microsoft Windows Server sono prossime o hanno raggiunto la fine del supporto. Ogni versione di Windows 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 Windows Server non riceverà aggiornamenti di sicurezza regolari. L'esecuzione di applicazioni con versioni di Windows Server non supportate può comportare rischi per la sicurezza o la conformità.

Note

Questo controllo genera risultati in base all'AMI utilizzata per avviare l'istanza EC2. È possibile che il sistema operativo dell'istanza corrente sia diverso dall'AMI di avvio. Ad esempio, se hai avviato un'istanza da un'AMI di Windows Server 2016 e successivamente esegui l'aggiornamento a Windows Server 2019, l'AMI di avvio non cambia.

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

Qsdfp3A4L4

Criteri di avviso

- Rosso: un'istanza EC2 viene eseguita su 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 viene eseguita su una versione di Windows Server che raggiungerà la fine del supporto in meno di 18 mesi (Windows Server 2012 e 2012 R2).

Azione 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](#).

Completa questa procedura:

- Aggiorna la versione di Windows Server
- Arresto difficile e avvio al momento dell'aggiornamento
- Se usi EC2 Config, esegui la migrazione a Launch EC2

Colonne del report

- Status
- Region
- 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

Description

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 almeno una volta al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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. [Supporto](#)

Colonne del report

- Status
- Region

- 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

Description

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 Linux non includono una versione di stunnel che supporta le funzionalità TLS per impostazione predefinita. Se utilizzi una distribuzione Linux non supportata (consulta [Distribuzioni supportate](#) nella Amazon Elastic File System User

Guide), è consigliabile aggiornarla prima di rimontarla con l'impostazione di montaggio consigliata.

Risorse aggiuntive

- [Crittografia dei dati in transito](#)

Colonne del report

- Status
- Region
- ID dei file system EFS
- AZs con connessioni non crittografate
- Ora ultimo aggiornamento

Snapshot pubblici Amazon EBS

Description

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'istananea, consenti a tutti Account AWS e agli utenti l'accesso a tutti i dati in essa contenuti. Per condividere un'istananea solo con utenti o account specifici, contrassegna l'istananea come privata. Quindi, specifica l'utente o gli account con cui desideri condividere i dati dell'istananea. 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 [AWS Support - ModifyEBSSnapshotPermission](#).

Risorse aggiuntive

[Snapshot Amazon EBS](#)

Colonne del report

- Status
- Region
- ID volume
- ID snapshot
- Description

La crittografia dello storage Amazon RDS Aurora è disattivata

Description

Amazon RDS supporta la crittografia a riposo per tutti i motori di database utilizzando le chiavi da te gestite. AWS Key Management Service In un'istanza database attiva con crittografia Amazon RDS, i dati a riposo memorizzati vengono crittografati, in modo simile ai backup automatici, alle repliche di lettura e agli snapshot.

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Attivare la crittografia dei dati a riposo per il cluster di database.

Risorse aggiuntive

Puoi 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

- Status
- Region
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

È richiesto l'aggiornamento di una versione secondaria del motore Amazon RDS

Description

Le risorse del database non eseguono la versione secondaria del motore di database più recente. L'ultima versione secondaria include le correzioni più recenti per la 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Giallo: 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

- Status
- Region
- Risorsa
- Nome del motore
- Versione del motore attuale
- Valore consigliato
- Ora ultimo aggiornamento

Snapshot pubblici di Amazon RDS

Description

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 [AWS Support - ModifyRDSSnapshotPermission](#).

Risorse aggiuntive

[Backup e ripristino di istanze DB di Amazon RDS](#)

Colonne del report

- Status
- Region
- Istanza DB o ID cluster
- ID snapshot

Rischio accesso gruppo di sicurezza Amazon RDS

Description

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.

Note

[Questo controllo valuta solo i gruppi di sicurezza collegati alle istanze Amazon RDS in esecuzione all'esterno su un Amazon VPC.](#)

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.
- Rosso: una regola del gruppo di sicurezza DB concede l'accesso globale (il suffisso della regola CIDR è /0).
- Verde: un gruppo di sicurezza DB non include regole permissive.

Operazione consigliata

EC2-Classical è stato ritirato il 15 agosto 2022. Si consiglia di spostare le istanze Amazon RDS su un VPC e utilizzare i gruppi di sicurezza Amazon EC2. Per ulteriori informazioni sullo spostamento dell'istanza DB su un VPC, consulta [Spostare un'istanza DB non contenuta in un VPC in un VPC](#).

Se non riesci a migrare le istanze Amazon RDS su un VPC, 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, utilizza l'API [Authorize o DBSecurity GroupIngress](#) il. Console di gestione AWS 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

- Status
- Region
- Nome del gruppo di sicurezza RDS
- Regola in ingresso
- Motivo

La crittografia dello storage Amazon RDS è disattivata

Description

Amazon RDS supporta la crittografia a riposo per tutti i motori di database utilizzando le chiavi da te gestite. AWS Key Management Service In un'istanza database attiva con crittografia Amazon RDS, i dati a riposo memorizzati vengono crittografati, in modo simile ai backup automatici, alle repliche di lettura e agli snapshot.

Se la crittografia non è attivata durante la creazione di un'istanza DB, devi 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Attivare la crittografia dei dati a riposo per l'istanza database.

Risorse aggiuntive

Puoi crittografare un'istanza DB solo quando crei 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 maggiori informazioni, consulta le seguenti risorse:

- [Crittografia delle risorse di Amazon RDS](#)
- [Copia di un'istantanea del DB](#)

Colonne del report

- Status
- Region
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Record CNAME di Amazon Route 53 non corrispondenti che puntano direttamente ai bucket S3

Description

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, impedisce 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 di [Amazon](#) S3 con record CNAME. URLs

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

- Status
- 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

Description

Per ogni record MX, verifica la presenza di un record TXT associato che contiene un valore SPF valido. Il valore del record TXT deve iniziare con «v=spf1». I tipi di record SPF sono obsoleti dall'Internet Engineering Task Force (IETF). Con Route 53, è consigliabile utilizzare un record TXT anziché un record SPF. Trusted Advisor riporta questo controllo come verde quando a un record MX è associato almeno un record TXT con un valore SPF valido.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

c9D319e7sG

Criteri di avviso

- Verde: un set di record di risorse MX ha un record di risorse TXT che contiene un valore SPF valido.
- Giallo: un set di record di risorse MX ha un record di risorse TXT o SPF che contiene un valore SPF valido.
- Rosso: un set di record di risorse MX non ha un record di risorse TXT o SPF che contenga 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

- [Tipo di record MX](#)
- [Tipo di record SPF](#)
- [Guida Re:POST](#)
- [RFC 7208](#)

Colonne del report

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

Autorizzazioni Bucket Amazon S3

Description

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

Pfx0RwqB1i

Criteri di avviso

- Rosso: l'ACL del bucket consente l'accesso alla lista o l' Upload/Delete accesso per tutti o qualsiasi AWS utente autenticato e le impostazioni di blocco dell'accesso pubblico non sono abilitate.
- Rosso: una policy bucket consente l'accesso pubblico e le impostazioni Block Public Access non sono abilitate.
- Rosso: Trusted Advisor non dispone dell'autorizzazione per verificare la politica oppure la politica non può essere valutata per altri motivi.

- Giallo: una policy bucket consente l'accesso pubblico, ma l'impostazione Restrict Public Buckets è attivata e limita l'accesso solo agli utenti autorizzati di quell'account.
- Giallo: il bucket è conforme ma non ha la protezione completa Block Public Access abilitata.
- Verde: il bucket è conforme e ha la protezione completa di Block Public Access abilitata.

 Note

Le concessioni ACL pubbliche non vengono valutate quando è abilitata l'opzione Block Public Access Ignore Public. ACLs

Azione consigliata

Se un bucket consente l'accesso aperto, determina se è veramente necessario. Ad esempio, per ospitare un sito Web statico, puoi utilizzare Amazon CloudFront per fornire i contenuti ospitati su Amazon S3. Consulta [Limitazione dell'accesso a un'origine Amazon S3](#) nella CloudFront Amazon Developer Guide. Quando possibile, 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](#)

[Configurazione delle impostazioni di blocco dell'accesso pubblico per i bucket Amazon S3](#)

Colonne del report

- Status
- 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

Connessioni peering VPC di Amazon con risoluzione DNS disabilitata

Description

Verifica se le connessioni peering VPC hanno la risoluzione DNS attivata sia per l'accettatore che per il richiedente. VPCs

La risoluzione DNS per una connessione peering VPC consente la risoluzione di nomi host DNS pubblici in indirizzi IPv4 privati quando vengono richieste dal tuo VPC. Ciò consente l'uso di nomi DNS per la comunicazione tra risorse in modalità peer-to-peer. VPCs 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 il VPC IDs, 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 l'accettatore che per il richiedente in VPCs 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

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

Protocollo crittografato per gruppi target di Application Load Balancer

Description

Verifica che i gruppi target di Application Load Balancer (ALB) utilizzino il protocollo HTTPS per crittografare le comunicazioni in transito per tipi di istanze o IP di destinazione back-end. Le richieste HTTPS tra ALB e target di back-end aiutano a mantenere la riservatezza dei dati per i dati in transito.

ID di controllo

c2v1fg0p1w

Criteri di avviso

- Giallo: gruppo target Application Load Balancer che utilizza HTTP.
- Verde: gruppo target Application Load Balancer che utilizza HTTPS.

Operazione consigliata

Configura i tipi di istanza o IP di destinazione di back-end per supportare l'accesso HTTPS e modifica il gruppo di destinazione per utilizzare il protocollo HTTPS per crittografare la comunicazione tra ALB e i tipi di istanza o IP di destinazione di back-end.

Risorse aggiuntive

[Applica la crittografia in transito](#)

[Tipi di target di Application Load Balancer](#)

[Configurazione del routing dell'Application Load Balancer](#)

[Protezione dei dati in Elastic Load Balancing](#)

Colonne del report

- Status
- Region
- ALB Arn
- Nome ALB
- ID VPC ALB
- Gruppo target Arn
- Nome del gruppo target
- Protocollo gruppo di destinazione
- Ora ultimo aggiornamento

AWS Backup Vault senza una politica basata sulle risorse per impedire l'eliminazione dei punti di ripristino

Description

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 che non desideri AWS Identity and Access Management ARNs che la regola controlli nel `principalArnList` parametro 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 autorizzazioni di backup:DeleteRecoveryPoint, backup: e backup:UpdateRecoveryPointLifecycle. PutBackupVaultAccessPolicy

Per ulteriori informazioni, consulta [Impostazione delle policy di accesso su vault di backup](#).

Colonne del report

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

AWS CloudTrail Registrazione degli eventi di gestione

Description

Verifica l'utilizzo di. AWS CloudTrail CloudTrail offre una maggiore visibilità sulle attività del tuo Account AWS. Lo fa 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 percorso si applica a tutti Regioni AWS (impostazione predefinita quando si crea un nuovo percorso), il percorso viene visualizzato più volte nel rapporto. Trusted Advisor

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c25hn9x03v

Criteri di avviso

- Rosso: non viene creato alcun percorso per un percorso oppure Regione AWS la registrazione non è abilitata per nessun percorso.
- Giallo: CloudTrail è abilitato ma tutti i percorsi segnalano errori di consegna dei log.
- Verde: CloudTrail è abilitato e non vengono segnalati errori di consegna dei log.

Operazione consigliata

Per creare un percorso e avviare la registrazione dalla console, apri la [AWS CloudTrail console](#).

Per avviare la registrazione, consulta [Interruzione e avvio della registrazione per un percorso](#).

Se ricevi errori di recapito dei log, assicurati che il bucket esista e che al bucket sia allegata la policy necessaria. Consulta [Policy del bucket Amazon S3](#).

Risorse aggiuntive

- [AWS CloudTrail Guida per l'utente](#)
- [Regioni supportate](#)
- [Servizi supportati](#)
- [Creazione di un percorso per un'organizzazione](#)

Colonne del report

- Status
- Region
- Registrazione abilitata
- Errore di consegna segnalato
- Ora ultimo aggiornamento

AWS Lambda Funzioni che utilizzano runtime obsoleti

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 sta per diventare obsoleto. Le funzioni sono incluse almeno 180 giorni prima della data di deprecazione del runtime.

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

- Status
- Region
- 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

Description

Verifica la presenza di problemi ad alto rischio (HRIs) 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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 identificati per la sicurezza HRIs

- Numero di HRIs risolti per la sicurezza
- Numero di domande per Sicurezza
- Numero totale di domande nel pilastro Sicurezza
- Ora ultimo aggiornamento

CloudFront Certificati SSL personalizzati nell'IAM Certificate Store

Description

Note

Questo controllo si applica alle CloudFront distribuzioni Amazon classiche.

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 sono obsoleti dalla maggior parte dei 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 errato). Per ulteriori informazioni, consulta [Utilizzo di HTTPS e di nomi di dominio alternativi](#).

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

Si consiglia di AWS Certificate Manager utilizzarla per fornire, gestire e distribuire i certificati del server. Con ACM, puoi richiedere un nuovo certificato o distribuire un certificato ACM o esterno esistente alle risorse. AWS I certificati forniti da ACM sono gratuiti e possono essere rinnovati automaticamente. Per ulteriori informazioni sull'utilizzo di ACM, consulta la [AWS Certificate Manager Guida per l'utente di](#). Per verificare i supporti Regioni AWS ACM, consulta gli [AWS Certificate Manager endpoint](#) e le quote nel. Riferimenti generali di AWS

Rinnova i certificati scaduti o i certificati che stanno per scadere. Per ulteriori informazioni sul rinnovo di un certificato, consulta [Gestione dei certificati del server](#) in IAM.

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](#)

[Importazione di certificati](#)

[AWS Certificate Manager Guida per l'utente](#)

Colonne del report

- Status
- ID distribuzione
- Nome di dominio della distribuzione

- Nome del certificato
- Motivo

CloudFront Certificato SSL sul server di origine

Description

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

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Status
- ID distribuzione
- Nome di dominio della distribuzione
- Origin
- Motivo

Sicurezza del Listener ELB

Description

Verifica la presenza di sistemi di bilanciamento del carico classici 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 e cifrari e protocolli sicuri. Quando si utilizza un protocollo sicuro per una connessione front-end (da client a load balancer), le richieste vengono crittografate tra i client e il sistema di bilanciamento del carico. Questo crea un ambiente più sicuro. Elastic Load Balancing fornisce policy di sicurezza predefinite con crittografia e protocolli che aderiscono alle best practice 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

- Rosso: un load balancer non ha listener configurati con un protocollo sicuro (HTTPS).

- Giallo: un listener HTTPS di load balancer è configurato con una politica di sicurezza che contiene un codice debole.
- Giallo: un listener HTTPS di load balancer non è configurato con la politica di sicurezza consigliata.
- Verde: un sistema di bilanciamento del carico ha almeno un listener HTTPS E tutti i listener HTTPS sono configurati con la policy consigliata.

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

- Status
- Region
- Nome del load balancer
- Porta del load balancer
- Motivo

Gruppi di sicurezza Classic Load Balancer

Description

Verifica la presenza di sistemi di bilanciamento del carico configurati con un gruppo di sicurezza che consente l'accesso a porte non configurate per il bilanciamento del carico.

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.
- Verde: le regole in entrata di un gruppo di sicurezza Amazon VPC associato a un sistema di bilanciamento del carico non consentono l'accesso a porte non definite nella configurazione del listener di load balancers.

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](#)
- [Effettua la migrazione del tuo Classic Load Balancer](#)
- [Configurazione di un Classic Load Balancer](#)

Colonne del report

- Status
- Region
- Nome del load balancer
- Gruppo di sicurezza IDs
- Motivo

Exposed Access Keys

Description

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 AWS risorse. 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.

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

Se viene indicata una scadenza per una chiave di accesso, AWS può sospendere l'utilizzo non autorizzato Account AWS se l'utilizzo non autorizzato non viene interrotto entro tale data. Se ritieni che un avviso sia errato, [contatta Supporto AWS](#).

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

12Fnkp18Y5

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 [Console di gestione AWS](#) 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

- Location (Ubicazione)
- Scadenza
- Utilizzo (USD al giorno)

Rotazione delle chiavi di accesso IAM

Description

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

- Status
- Utente IAM
- Chiave di accesso
- Ultima chiave ruotata
- Motivo

Accesso esterno a IAM Access Analyzer

Description

Verifica se è presente l'accesso esterno di IAM Access Analyzer a livello di account.

Gli analizzatori di accesso esterni IAM Access Analyzer aiutano a identificare le risorse negli account condivise con un'entità esterna. L'analizzatore crea quindi una dashboard centralizzata con i risultati. Dopo l'attivazione del nuovo analizzatore nella console IAM, i team di sicurezza possono quindi dare priorità agli account da esaminare in base alle autorizzazioni eccessive. Un analizzatore di accesso esterno crea risultati di accesso pubblici e interaccount alle risorse e viene fornito senza costi aggiuntivi.

ID di controllo

07602fcad6

Criteri di avviso

- Rosso: l'accesso esterno all'analizzatore non è attivato a livello di account.
- Verde: l'accesso esterno all'analizzatore è attivato a livello di account.

Operazione consigliata

La creazione di un analizzatore di accesso esterno per account aiuta i team di sicurezza a dare priorità agli account da esaminare in base alle autorizzazioni eccessive. Per ulteriori informazioni, consulta [Guida introduttiva](#) ai risultati. AWS Identity and Access Management Access Analyzer

Inoltre, è consigliabile utilizzare l'Unused Access Analyzer, una funzionalità a pagamento che semplifica l'ispezione degli accessi inutilizzati per orientare l'utente verso il privilegio minimo. Per ulteriori informazioni, consulta [Identificazione dell'accesso non utilizzato](#) concesso a utenti e ruoli IAM.

Risorse aggiuntive

- [Uso di AWS Identity and Access Management Access Analyzer](#)
- [Aggiornamenti di IAM Access Analyzer: trova gli accessi non utilizzati, controlla le politiche prima della distribuzione](#)

Colonne del report

- Status
- Region
- Account External Access Analyzer Arn
- Organizzazione External Access Analyzer Arns
- Ora ultimo aggiornamento

Policy delle Password IAM

Description

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

Yw2K9puPz1

Criteri di avviso

- Verde: è abilitata una politica di password con i requisiti di contenuto consigliati abilitati.
- Giallo: una policy sulle password è abilitata, ma almeno un requisito relativo al contenuto non è abilitato.

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](#).

Per accedere a Console di gestione AWS, gli utenti IAM necessitano di password. Come best practice, consigliamo AWS vivamente di utilizzare la federazione anziché creare utenti IAM. La federazione consente agli utenti di utilizzare le proprie credenziali aziendali esistenti per accedere a Console di gestione AWS. Utilizza IAM Identity Center per creare o federare l'utente e quindi assumere un ruolo IAM in un account.

Per saperne di più sui provider di identità e la federazione, consulta [Provider di identità e federazione](#) nella Guida per l'utente IAM. Per ulteriori informazioni su IAM Identity Center, consulta la [Guida per l'utente di IAM Identity Center](#).

Risorse aggiuntive

[La gestione delle password](#)

Colonne del report

- Policy sulle password
- Maiuscolo
- Minuscolo
- Numero
- Non alfanumerico

Provider di identità IAM SAML 2.0

Description

Verifica se Account AWS è configurato per l'accesso tramite un provider di identità (IdP) che supporta SAML 2.0. Assicurati di seguire le migliori pratiche quando centralizzi le identità e configuri gli utenti in un provider di identità [esterno](#) o [AWS IAM Identity Center](#).

ID di controllo

c2v1fg0p86

Criteri di avviso

- Giallo: questo account non è configurato per l'accesso tramite un provider di identità (IdP) che supporta SAML 2.0.
- Verde: questo account è configurato per l'accesso tramite un provider di identità (IdP) che supporta SAML 2.0.

Operazione consigliata

Attiva IAM Identity Center per. Account AWS Per ulteriori informazioni, consulta [Enabling IAM Identity Center](#). Dopo aver attivato IAM Identity Center, puoi eseguire attività comuni come la creazione di un set di autorizzazioni e l'assegnazione dell'accesso ai gruppi di Identity Center. Per ulteriori informazioni, consulta [Attività comuni](#).

Gestire gli utenti umani in IAM Identity Center è una best practice. Ma puoi attivare l'accesso federato degli utenti con IAM per utenti umani a breve termine per implementazioni su piccola scala. Per ulteriori informazioni, consulta la federazione [SAML 2.0](#).

Risorse aggiuntive

[Cos'è il Centro identità IAM?](#)

[Che cos'è IAM?](#)

Colonne del report

- Status
- Account AWS Id
- Ora ultimo aggiornamento

MFA sull'account root

Description

Verifica le credenziali utente root di un account e avvisa 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. Console di gestione AWS

Note

Per il tuo account di AWS Organizations gestione, AWS richiede l'autenticazione a più fattori (MFA) per l'utente root quando accede a. Console di gestione AWS

Per i tuoi account AWS Organizations membro, ti consigliamo di gestire centralmente le credenziali root utilizzando. AWS Identity and Access Management Le credenziali utente

root dell'account membro possono essere eliminate centralmente, eliminando la necessità di gestire l'MFA sulle credenziali dell'utente root. Per ulteriori informazioni, consulta le [migliori pratiche per gli account dei membri nella Guida](#) per l'AWS Organizations utente.

ID di controllo

7DAFEemoDos

Criteri di avviso

- Rosso: l'MFA non è abilitata sull'account root.
- Verde: non esistono credenziali utente root (password root) o l'MFA è abilitata per l'account.

Azione consigliata

Se si tratta di un account membro in AWS Organizations: accedi al tuo account di gestione, abilita la funzionalità di gestione degli accessi root in IAM e rimuovi le credenziali dell'utente root da questo account membro. Vedi [Centralizzare l'accesso root per gli account dei membri](#).

Se si tratta di un account autonomo o di gestione, accedi al tuo account root e attiva un dispositivo MFA. AWS Organizations Per ulteriori informazioni, consulta [Verifica dello stato dell'MFA](#) e dell'autenticazione a [AWS più fattori](#) in IAM

Risorse aggiuntive

- [Gestire centralmente l'accesso root per gli account membri](#)
- [AWS Autenticazione a più fattori in IAM](#)
- [Autenticazione a più fattori per utente root Account AWS](#)

Chiave di accesso utente root

Description

Verifica se è presente la chiave di accesso dell'utente root. Si consiglia vivamente di non creare coppie di chiavi di accesso per l'utente root. Poiché [solo alcune attività richiedono l'utilizzo dell'utente root](#) e in genere tali operazioni vengono eseguite raramente, è consigliabile accedere al sito per Console di gestione AWS eseguire le attività dell'utente root. Prima di creare le chiavi di accesso, esamina le [alternative alle chiavi di accesso a lungo termine](#).

ID di controllo

c2v1fg0f4h

Criteri di avviso

- Rosso: è presente la chiave di accesso dell'utente root
- Verde: la chiave di accesso dell'utente root non è presente

Operazione consigliata

Elimina le chiavi di accesso per l'utente root. Vedere [Eliminazione delle chiavi di accesso per l'utente root](#). Questa operazione deve essere eseguita dall'utente root. Non è possibile eseguire questi passaggi come utente o ruolo IAM.

Risorse aggiuntive

- [Attività che richiedono le credenziali dell'utente root](#)
- [Reimpostazione di una password utente root persa o dimenticata](#)

Colonne del report

- Status
- ID account
- Ora ultimo aggiornamento

Gruppi di sicurezza — Porte specifiche senza restrizioni

Description

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 dall'utente e le relative regole in entrata per gli indirizzi. IPv4 I gruppi di sicurezza creati da AWS Directory Service

sono contrassegnati in rosso o giallo, ma non rappresentano un rischio per la sicurezza e possono essere esclusi. Per ulteriori informazioni, consultare la pagina relativa alle [domande frequenti su Trusted Advisor](#).

 Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

HCP4007jGY

Criteri di avviso

- Verde: Security Group fornisce un accesso illimitato alle porte 80, 25, 443 o 465.
- Rosso: Security Group è collegato a una risorsa e fornisce accesso illimitato alle porte 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432 o 5500.
- Giallo: Security Group fornisce un accesso illimitato a qualsiasi altra porta.
- Giallo: Security Group non è collegato a nessuna risorsa e fornisce un accesso 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.

Rivedi ed elimina i gruppi di sicurezza non utilizzati. Puoi utilizzarlo AWS Firewall Manager per configurare e gestire centralmente i gruppi di sicurezza su Account AWS larga scala. Per ulteriori informazioni, consulta la [AWS Firewall Manager documentazione](#).

Prendi in considerazione l'utilizzo di Systems Manager Sessions Manager per l'accesso SSH (porta 22) e RDP (porta 3389) alle istanze EC2. Con il gestore delle sessioni, puoi accedere alle tue istanze EC2 senza abilitare le porte 22 e 3389 nel gruppo di sicurezza.

Risorse aggiuntive

- [Gruppi di sicurezza Amazon EC2](#)

[Elenco dei numeri di porta TCP e UDP](#)

- [Classless Inter-Domain Routing](#)
- [Lavorare con Session Manager](#)
- [AWS Firewall Manager](#)

Colonne del report

- Status
- Region
- Nome del gruppo di sicurezza
- ID gruppo di sicurezza
- Protocollo
- Dalla porta
- Alla porta
- Associazione

Gruppi di sicurezza — Accesso illimitato

Description

Controlla i gruppi di sicurezza per le regole che consentono l'accesso illimitato a una risorsa.

L'accesso illimitato aumenta le opportunità di attività dannose (pirateria informatica, denial-of-service attacchi, perdita di dati).

Note

Questo controllo valuta solo i gruppi di sicurezza creati dall'utente e le relative regole in entrata per gli indirizzi. IPv4 I gruppi di sicurezza creati da AWS Directory Service sono contrassegnati in rosso o giallo, ma non rappresentano un rischio per la sicurezza e possono essere esclusi. Per ulteriori informazioni, consultare la pagina relativa alle [domande frequenti su Trusted Advisor](#).

 Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

1iG5NDGVre

Criteri di avviso

- Verde: una regola del gruppo di sicurezza ha un indirizzo IP di origine con un suffisso /0 per le porte 25, 80 o 443.
- Giallo: una regola del gruppo di sicurezza ha un indirizzo IP di origine con un suffisso /0 per porte diverse da 25, 80 o 443 e il gruppo di sicurezza è collegato a una risorsa.
- 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 e il gruppo di sicurezza non è collegato a una risorsa.

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.

Rivedi ed elimina i gruppi di sicurezza non utilizzati. Puoi utilizzarlo AWS Firewall Manager per configurare e gestire centralmente i gruppi di sicurezza su Account AWS larga scala. Per ulteriori informazioni, consulta la [AWS Firewall Manager documentazione](#).

Prendi in considerazione l'utilizzo di Systems Manager Sessions Manager per l'accesso SSH (porta 22) e RDP (porta 3389) alle istanze EC2. Con il gestore delle sessioni, puoi accedere alle tue istanze EC2 senza abilitare le porte 22 e 3389 nel gruppo di sicurezza.

Risorse aggiuntive

- [Gruppi di sicurezza Amazon EC2](#)
- [Classless Inter-Domain Routing](#)
- [Lavorare con Session Manager](#)
- [AWS Firewall Manager](#)

Colonne del report

- Status
- Region
- Nome del gruppo di sicurezza
- ID gruppo di sicurezza
- Protocollo
- Dalla porta
- Alla porta
- Intervallo IP
- Associazione

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 di Amazon CloudFront Origin](#)
- [Rischio di accesso agli endpoint Amazon Comprehend](#)
- [Cluster Amazon DocumentDB Single AZ](#)
- [Ripristino con Amazon DynamoDB Point-in-time](#)
- [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](#)
- [Amazon EC2 Auto Scaling non è distribuito AZs in più o non soddisfa il numero minimo di AZs](#)
- [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: nessuna ridondanza del target di montaggio](#)
- [Amazon EFS non è AWS Backup previsto](#)
- [Cluster Amazon ElastiCache Multi-AZ](#)
- [ElastiCache Backup automatico dei cluster \(Redis OSS\)](#)
- [Cluster Multi-AZ Amazon MemoryDB](#)
- [Broker Amazon MSK che ospitano un numero eccessivo di partizioni](#)
- [Cluster Amazon MSK Multi-AZ](#)
- [Domini Amazon OpenSearch Service con meno di tre nodi di dati](#)
- [Backup Amazon RDS](#)
- [Backup continuo di Amazon RDS non abilitato](#)
- [I cluster di database Amazon RDS dispongono di un'istanza database](#)
- [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](#)
- [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](#)
- [Auto Scaling disponibile nelle sottoreti IPs](#)
- [Controllo dell'integrità del gruppo Auto Scaling](#)
- [Risorse dei gruppi Auto Scaling](#)
- [AWS CloudHSM cluster che eseguono istanze HSM in un'unica AZ](#)
- [Direct Connect Resilienza della posizione](#)
- [AWS Lambda funzioni senza una coda di lettere non scritte configurata](#)
- [AWS Lambda Sulle destinazioni degli eventi di fallimento](#)
- [AWS Lambda Funzioni abilitate per VPC senza ridondanza Multi-AZ](#)
- [AWS Outposts Implementazione a rack singolo](#)
- [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 STS utilizzo globale degli endpoint in tutto il mondo Regioni AWS](#)
- [AWS Well-ArchitectedProblemi ad alto rischio di per l'affidabilità](#)
- [Classic Load Balancer non ha configurazioni multiple AZs](#)

- [Connection Draining CLB](#)
- [Elb Target Squilibrio](#)
- [GWLb: indipendenza dall'endpoint AZ](#)
- [Ottimizzazione del load balancer](#)
- [Indipendenza dell'AZ disponibilità dal Gateway NAT](#)
- [Network Firewall endpoint AZ Independence](#)
- [Network Firewall Multi-AZ](#)
- [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 \(interfacce di rete endpoint multiple\) AZs](#)
- [Ridondanza del Tunnel VPN](#)
- [Ridondanza della zona di disponibilità ActiveMQ](#)
- [Ridondanza della zona di disponibilità RabbitMQ](#)

ALB Multi-AZ

Description

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 parti AZs 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1dfprch08

Criteri di avviso

Giallo: ALB si trova in una sola AZ.

Verde: ALB ne ha due o più. AZs

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

- Status
- Region
- Nome ALB
- Regola ALB
- ARN BIANCO
- Numero di AZs
- Ora ultimo aggiornamento

Backtracking del cluster MySQL di Amazon Aurora non abilitato

Description

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 `BacktrackWindowInHours` parametro delle AWS Config regole.

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa

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

Accessibilità dell'istanza DB Amazon Aurora

Description

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

xuy7H1avt1

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

- Status
- Region
- Cluster
- Istanze DB pubbliche
- Istanze DB private
- Motivo

Failover di Amazon CloudFront Origin

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region

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

Rischio di accesso agli endpoint Amazon Comprehend

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 aggiornarla. AWS KMS Per ulteriori informazioni, vedere [Modifica di una policy delle chiavi](#).

Risorse aggiuntive

[AWS KMS Autorizzazioni](#)

Colonne del report

- Status
- Region
- ARN endpoint
- ARN modello
- KMS KeyId
- Ora ultimo aggiornamento

Cluster Amazon DocumentDB Single AZ

Description

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 più volte al giorno e le richieste di aggiornamento non sono consentite. Potrebbero essere necessarie alcune ore prima che le modifiche vengano visualizzate.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Zona di disponibilità
- DB Cluster Identifier (Identificatore cluster database)
- ARN del cluster DB
- Ora ultimo aggiornamento

Ripristino con Amazon DynamoDB Point-in-time

Description

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 [Point-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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz138

Origine

AWS Config Managed Rule: dynamodb-pitr-enabled

Criteri di avviso

Giallo: Point-in-time il ripristino 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 [Point-in-time Recovery: How it Works.](#)

Risorse aggiuntive

[Point-in-time ripristino per DynamoDB](#)

Colonne del report

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

Tabella di Amazon DynamoDB non inclusa nel piano di backup

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Amazon EBS non incluso nel piano AWS Backup

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Snapshot Amazon EBS

Description

Verifica l'età degli snapshot per i tuoi volumi Amazon EBS (disponibili o in uso). I guasti possono verificarsi anche se i volumi Amazon EBS vengono replicati. Le istantanee vengono salvate in 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](#).

Per automatizzare la creazione di snapshot EBS, puoi prendere in considerazione l'utilizzo di [Amazon Data AWS BackupLifecycle Manager](#).

Risorse aggiuntive

[Amazon Elastic Block Store \(Amazon EBS\)](#)

[Snapshot Amazon EBS](#)

[AWS Backup](#)

[Amazon Data Lifecycle Manager](#)

Colonne del report

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Per il gruppo con dimensionamento automatico Amazon EC2 è abilitato il ribilanciamento della capacità

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Amazon EC2 Auto Scaling non è distribuito AZs in più o non soddisfa il numero minimo di AZs

Description

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 minAvailabilityZonesparametro nelle tue regole. AWS Config

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: il gruppo Amazon EC2 Auto Scaling non AZs ha configurazioni multiple o non soddisfa il numero minimo AZs 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

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

Bilanciamento della zona di disponibilità Amazon EC2

Description

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](#)
- [Gruppi di posizionamento per le tue istanze Amazon EC2](#)
- [Tipi di istanza Amazon EC2](#)

Colonne del report

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione 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

- Status
- Region
- Risorsa
- AWS Config Regola

- Parametri di input
- Ora ultimo aggiornamento

Driver Amazon ECS AWS Logs in modalità di blocco

Description

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.

Questo controllo non prende in considerazione le impostazioni di configurazione del driver a livello di 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1dvkm4z6b

Criteri di avviso

Giallo: la modalità dei parametri di configurazione della registrazione del driver awslogs è impostata su blocco.

Verde: la definizione delle attività di Amazon ECS non utilizza il driver awslogs o il driver awslogs è configurato in modalità non bloccante.

Azione 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 [Prevenzione della perdita di log con la modalità non bloccante nel driver di registro del contenitore AWS 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

- Status
- Region
- ARN di definizione dell'attività
- Nomi di definizione dei contenitori
- Ora ultimo aggiornamento

Servizio Amazon ECS con un'unica AZ

Description

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 economica e a bassa latenza tra AZs di loro. Regione AWS Avviando più istanze AZs nella stessa regione, puoi contribuire a proteggere le tue applicazioni da un singolo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1z7dfpz01

Criteri di avviso

- Giallo: un servizio di Amazon ECS esegue tutte le attività in un'unica AZ.
- Verde: un servizio Amazon ECS esegue attività in almeno due aree diverse AZs.

Azione consigliata

Crea almeno un'altra attività per il servizio in un'AZ diversa.

Risorse aggiuntive

[Capacità e disponibilità di Amazon ECS](#)

Colonne del report

- Status
- Region
- Nome del servizio del cluster Name/ECS ECS
- Numero delle zone di disponibilità
- Ora ultimo aggiornamento

Strategia di collocazione Multi-AZ di Amazon ECS

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione consigliata

Abilita la strategia Spread Task Placement per distribuire le attività tra più attività AZs. 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

- Status
- Region
- Nome del Name/ECS servizio cluster ECS
- Strategia di collocazione distribuita delle attività abilitata e applicata correttamente
- Ora ultimo aggiornamento

Amazon EFS: nessuna ridondanza del target di montaggio

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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.

Azione 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 destinazioni di montaggio utilizzando la console di Amazon EFS](#)
- [Quote e limiti di Amazon EFS](#)

Colonne del report

- Status
- Region
- ID dei file system EFS
- Numero di destinazioni di montaggio
- Numero di AZs
- Ora ultimo aggiornamento

Amazon EFS non è AWS Backup previsto

Description

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: i file system Amazon EFS non sono inclusi nel AWS Backup piano.

Azione 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

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

Cluster Amazon ElastiCache Multi-AZ

Description

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 multiple AZs migliorano la disponibilità dei ElastiCache cluster mediante la replica asincrona su repliche di sola lettura in una zona di disponibilità diversa. Se si verifica una manutenzione pianificata del cluster o se un nodo primario non è disponibile, ElastiCache 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

ECHdfsQ402

Criteri di avviso

- Verde: Multi-AZ è attivo nel cluster.
- Giallo: Multi-AZ non è attivo nel cluster.

Azione consigliata

Crea almeno una replica per partizione, in una zona di disponibilità diversa da quella primaria.

Risorse aggiuntive

Per ulteriori informazioni, consulta [Riduzione al minimo dei tempi di inattività in ElastiCache \(Redis OSS\)](#) con Multi-AZ.

Colonne del report

- Status
- Region
- Nome del cluster
- Ora ultimo aggiornamento

ElastiCache Backup automatico dei cluster (Redis OSS)

Description

Verifica se i cluster Amazon ElastiCache (Redis OSS) 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 `snapshotRetentionPeriod` parametri delle regole. AWS Config

Per ulteriori informazioni, consulta [Backup e ripristino per ElastiCache \(Redis OSS\)](#).

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz178

Origine

AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check

Criteri di avviso

Rosso: nei cluster Amazon ElastiCache (Redis OSS) 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 (Redis OSS) 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 per ElastiCache \(Redis OSS\)](#).

Risorse aggiuntive

Per ulteriori informazioni, consulta [Pianificazione di backup automatici](#).

Colonne del report

- Status
- Region
- Nome del cluster
- Ora ultimo aggiornamento

Cluster Multi-AZ Amazon MemoryDB

Description

Controlla cluster MemoryDB implementati in una singola zona di disponibilità (AZ). Questo controllo avvisa quando Multi-AZ è inattivo in un cluster.

Le distribuzioni multiple AZs migliorano la disponibilità del cluster MemoryDB mediante la replica asincrona su repliche di sola lettura in una zona di disponibilità 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region

- Nome del cluster
- Ora ultimo aggiornamento

Broker Amazon MSK che ospitano un numero eccessivo di partizioni

Description

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

- Status
- Region
- ARN del cluster
- ID del broker
- Conteggio partizioni

Cluster Amazon MSK Multi-AZ

Description

Verifica il numero di zone di disponibilità (AZs) per il cluster fornito da Amazon MSK. Il cluster Amazon MSK è composto da diversi broker che collaborano e distribuiscono i dati e il carico. La

produzione potrebbe essere interrotta durante la manutenzione o problemi di intermediazione in un cluster 2-AZ.

ID di controllo

90046ff5b5

Criteri di avviso

- Giallo: il cluster Amazon MSK è dotato di broker solo in due AZs
- Verde: il cluster Amazon MSK è dotato di broker distribuiti su tre o più AZs

Operazione consigliata

Per aumentare la disponibilità del cluster, puoi creare un altro cluster in una configurazione a 3. AZs Quindi migra il cluster esistente nel nuovo cluster che hai creato. Puoi utilizzare la replica Amazon MSK per questa migrazione.

Risorse aggiuntive

[Disponibilità elevata di Amazon MSK](#)

[Migrazione Amazon MSK](#)

Colonne del report

- Status
- Region
- ARN del cluster MSK
- Numero di AZs
- Ora ultimo aggiornamento

Domini Amazon OpenSearch Service con meno di tre nodi di dati

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- AWS Config Regola

- Parametri di input
- Ora ultimo aggiornamento

Backup Amazon RDS

Description

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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Status
- Regione/AZ
- Istanza database
- ID VPC
- Backup retention period (Periodo di retention dei backup)

Backup continuo di Amazon RDS non abilitato

Description

Verifica se un'istanza Amazon RDS è abilitata con backup automatici utilizzando Amazon RDS o con backup continui di. AWS Backup I backup continui riducono il rischio di perdita imprevista dei dati e consentono il ripristino. point-in-time

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

44fde09ab5

Criteri di avviso

- Rosso: l'istanza non ha il backup automatico abilitato in Amazon RDS o il backup continuo in AWS Backup.
- Rosso: le versioni di MySQL precedenti alla 5.6 non supportano il backup automatico o continuo. Per garantire la resilienza, aggiorna prima la versione del database e poi abilita il backup automatico o continuo.
- Verde: l'istanza ha il backup automatico abilitato in Amazon RDS.
- Verde: l'istanza ha il backup continuo abilitato. AWS Backup

Operazione consigliata

Assicurati che le istanze di Amazon RDS abbiano configurato il backup automatico impostando un periodo di conservazione superiore a 0 in Amazon RDS o creando un piano di backup continuo utilizzando. AWS Backup

Risorse aggiuntive

- [Nozioni di base su Amazon RDS](#)

- [Gestione dei backup automatici](#)
- [Introduzione ai backup](#)
- [Backup e point-in-time ripristino continui \(PITR\)](#)
- [AWS Backup disponibilità delle funzionalità](#)

Colonne del report

- Status
- Region
- DB Instance Identifier (Identificatore istanza database)
- ARN dell'istanza DB
- Tipo di distribuzione
- Tipo di backup
- Motivo
- Ora ultimo aggiornamento

I cluster di database Amazon RDS dispongono di un'istanza database

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Nome del motore
- Classe di istanza database
- Ora ultimo aggiornamento

Cluster Amazon RDS DB con tutte le istanze nella stessa zona di disponibilità

Description

I cluster di database si trovano attualmente in un'unica zona di disponibilità. Utilizzare 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Aggiungere le istanze database a più zone di disponibilità nel cluster di database.

Risorse aggiuntive

Si consiglia 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

- Status

- Region
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Cluster Amazon RDS DB con tutte le istanze di lettura nella stessa zona di disponibilità

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 (AZs) sono località distinte l'una dall'altra per garantire l'isolamento in caso di interruzioni all'interno di ciascuna AWS regione. Si consiglia di distribuire l'istanza principale e le istanze di lettura nel cluster DB su più istanze AZs per migliorare la disponibilità del cluster DB. Puoi creare un cluster Multi-AZ utilizzando Console di gestione AWS, AWS CLI, o l'API Amazon RDS al momento della creazione del cluster. È inoltre possibile modificare il cluster Aurora esistente in un cluster Multi-AZ aggiungendo una nuova istanza di lettura e specificando una zona di disponibilità diversa.

Per ulteriori informazioni, consulta [Alta disponibilità per Amazon Aurora](#).

Colonne del report

- Status
- Region
- Risorsa
- Nome del motore
- Ora ultimo aggiornamento

Monitoraggio avanzato delle istanze DB Amazon RDS non abilitato

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa

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

La scalabilità automatica dello storage sulle istanze DB di Amazon RDS è disattivata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Istanze database Amazon RDS che non utilizzano la distribuzione Multi-AZ

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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, consultare [Prezzi](#).

Colonne del report

- Status
- Region
- Risorsa
- Nome del motore

- Ora ultimo aggiornamento

Amazon RDS DiskQueueDepth

Description

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 la possibilità di passare a istanze e volumi di storage che supportano queste caratteristiche. read/write

Colonne del report

- Status
- Region
- ARN dell'istanza DB
- DiskQueueDepth Parametro

Amazon RDS FreeStorageSpace

Description

Verifica se la FreeStorageSpace CloudWatch metrica per un'istanza di database RDS è scesa al di sotto di una soglia ragionevole dal punto di vista operativo.

ID di controllo

Cmsvnj8db2

Criteri di avviso

- Rosso: FreeStorageSpace ha meno del 10% della capacità totale
- Giallo: FreeStorageSpace è compreso tra il 10% e il 20% della capacità totale
- Verde: FreeStorageSpace rappresenta più del 20% 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

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

L'impostazione del parametro innodb_default_row_format di Amazon RDS non è sicura

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro `innodb_flush_log_at_trx_commit` di Amazon RDS non è 1

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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, consultare [Best practice per la configurazione dei parametri per Amazon RDS per MySQL, parte 1: Parametri relativi alle prestazioni](#).

Colonne del report

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Il parametro max_user_connections di Amazon RDS è basso

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Amazon RDS Multi-AZ

Description

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.

 Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

- Status
- Regione/AZ
- Istanza database
- ID VPC
- Multi-AZ

Amazon RDS non è previsto AWS Backup

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- AWS Config Regola

- Parametri di input
- Ora ultimo aggiornamento

Le repliche di lettura di Amazon RDS sono aperte in modalità scrivibile

Description

L'istanza database ha la replica di lettura in modalità scrivibile e consente gli aggiornamenti dei client.

Ti consigliamo di impostare il parametro `read_only` su `in` nel `TrustedAdvisor` modo che le repliche 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 `TrueIfReplica`

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 `TrueIfReplica`. Per un'istanza di replica, `TrueIfReplica` imposta il valore `read_only` su `ON (1)` e disabilita qualsiasi attività di scrittura da parte dei client. master/writer. Ad esempio, `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, causando 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

I backup automatici delle risorse Amazon RDS sono disattivati

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Attivare i backup automatizzati 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 maggiori informazioni, consulta le seguenti risorse:

- [Abilitazione dei backup automatici](#)
- [Demistificazione dei costi dello storage di backup di Amazon RDS](#)

Colonne del report

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Il parametro sync_binlog di Amazon RDS è disattivato

Description

La sincronizzazione del log binario sul disco non viene applicata prima della conferma del commit delle transazioni nell'istanza database.

Ti consigliamo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Per il cluster DB RDS non è abilitata la replica Multi-AZ

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Istanza di standby RDS Multi-AZ non abilitata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Amazon RDS ReplicaLag

Description

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. Ad esempio, può essere causato da istanze di replaced/launched replica recenti da backup precedenti e tali repliche richiedono molto tempo per «recuperare» l'istanza del database principale e le transazioni live. 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 durante diversi periodi del day/month/etc... con conseguente occasionale ReplicaLag ritardo. 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

- Status
- Region
- ARN dell'istanza DB
- ReplicaLag Parametro

Il parametro Amazon RDS `synchronous_commit` è disattivato

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 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

- Status
- Region
- Risorsa
- Nome parametro
- Valore consigliato
- Ora ultimo aggiornamento

Snapshot automatiche del cluster di Amazon Redshift

Description

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 disabilitare le istantanee automatiche per i tipi di RA3 nodi.

Puoi specificare il periodo di conservazione minimo e massimo desiderato utilizzando il `MaxRetentionPeriod` parametro `MinRetentionPeriod` 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Amazon Route 53 ha eliminato i Controlli dell'integrità

Description

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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

Description

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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

Description

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 impiegano più tempo a richiedere record DNS aggiornati, il che può causare inutili ritardi nel reindirizzamento del traffico (ad esempio, quando il failover DNS rileva e risponde a un guasto di uno degli endpoint). Questo controllo esamina solo i record con una politica di failover o se è presente un controllo dello stato associato.

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

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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.
- Verde: un record di risorse non ha una politica di failover o ha una politica di failover con un TTL inferiore a 60.

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

- Status
- 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

Description

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, dove ### 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.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

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

Description

Verifica se la configurazione del servizio prevede indirizzi IP specificati in almeno due zone di disponibilità (AZs) per la ridondanza. Un'AZ è una posizione distinta che è isolata da errori presenti in altre zone. Specificando più indirizzi IP AZs nella stessa regione, è possibile proteggere le applicazioni da un singolo punto di errore.

ID di controllo

Chr231ch1

Criteri di avviso

- Giallo: gli indirizzi IP sono specificati in una sola AZ
- Verde: gli indirizzi IP sono specificati in almeno due AZs

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

- Status
- Region
- ARN risorsa
- Numero di AZs

Replica di bucket Amazon S3 non abilitata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status

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

Amazon S3 Bucket Versioning

Description

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.
- Giallo: Trusted Advisor non ha accesso alla convalida del controllo delle versioni.

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

- Status
- Region
- 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

Description

Controlla se i tuoi sistemi di bilanciamento del carico (Application, Network e Gateway Load Balancer) sono configurati con sottoreti su più zone di disponibilità.

Puoi specificare le zone di disponibilità minima desiderate nei `minAvailabilityZones` parametri delle tue 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status

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

Auto Scaling disponibile nelle sottoreti IPs

Description

Verifica che IPs rimanga sufficiente disponibilità tra le sottoreti di destinazione. Avere una IPs disponibilità sufficiente per l'uso sarebbe utile quando il gruppo Auto Scaling 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

- Status
- Region
- ARN risorsa
- Numero massimo di istanze che è possibile creare
- Numero di istanze disponibili

Controllo dell'integrità del gruppo Auto Scaling

Description

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

CLOG40CD08

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

- Status
- Region
- Nome del gruppo con scalabilità automatica

- Load balancer associato
- Controllo dello stato

Risorse dei gruppi Auto Scaling

Description

Verifica la disponibilità delle risorse associate alle configurazioni di avvio, ai modelli di avvio e ai gruppi di 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 di Auto Scaling e i configurations/launch modelli di avvio che puntano a risorse non disponibili non funzionano come previsto.

Note

Questo controllo riporta le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.

ID di controllo

8CNsS11I5v

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.
- Rosso: un modello di avvio è associato a un'Amazon Machine Image (AMI) eliminata.

Operazione consigliata

Se il load balancer è stato eliminato, crea un nuovo load balancer o un nuovo gruppo target e poi associalo al gruppo Auto Scaling. Oppure crea un nuovo gruppo Auto Scaling senza il load balancer. 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 stato eliminato, crea una nuova configurazione di avvio o una versione del modello di avvio utilizzando un AMI valido e associalo a un gruppo Auto Scaling. Per informazioni su come creare una nuova configurazione di avvio, consulta [Create a launch configuration](#) nella Amazon EC2 Auto Scaling User Guide. Per informazioni su come creare un modello di lancio, consulta [Create a launch template for an Auto Scaling group](#) nella Amazon EC2 Auto Scaling User Guide.

 Note

Per motivi di sicurezza, i risultati del controllo non includono alcuna risorsa a cui si fa riferimento utilizzando AWS Systems Manager i parametri nel modello di lancio.

Se i tuoi modelli di lancio includono un AWS Systems Manager parametro che include un ID Amazon Machine Image (AMI), esamina il modello di avvio per assicurarti che i parametri facciano riferimento a un ID AMI valido o apporta le modifiche appropriate nell'archivio AWS Systems Manager dei parametri. Per ulteriori informazioni, consulta [Usa AWS Systems Manager parametri anziché AMI IDs](#) nella Amazon EC2 Auto Scaling User Guide.

Risorse aggiuntive

- [Risoluzione dei problemi di Auto Scaling: Amazon EC2 AMIs](#)
- [Risoluzione dei problemi di Auto Scaling: configurazione del load balancer](#)
- [Guida per l'utente di Dimensionamento automatico Amazon EC2](#)
- [Usa AWS Systems Manager i parametri invece dell'AMI IDs](#)

Colonne del report

- Status
- Region
- Nome del gruppo con scalabilità automatica
- Tipo di lancio
- Tipo di risorsa
- Nome risorsa

AWS CloudHSM cluster che eseguono istanze HSM in un'unica AZ

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- ID cluster

- Numero di istanze HSM
- Ora ultimo aggiornamento

Direct Connect Resilienza della posizione

Description

Verifica la resilienza dell'utente 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 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 [Direct Connect resilienza](#).

Risorse aggiuntive

[Direct Connect Raccomandazioni sulla resilienza](#)

[Direct Connect Test di failover](#)

Colonne del report

- Status
- Region
- Ora ultimo aggiornamento
- Stato di resilienza
- Location (Ubicazione)
- ID connessione
- ID Gateway

AWS Lambda funzioni senza una coda di lettere non scritte configurata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz182

Origine

AWS Config Managed Rule: lambda-dlq-check

Criteri di avviso

Giallo: AWS Lambda la 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

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

AWS Lambda Sulle destinazioni degli eventi di fallimento

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 On Failure Event Destinations](#)

Colonne del report

- Status
- Region
- 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

AWS Lambda Funzioni abilitate per VPC senza ridondanza Multi-AZ

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- ARN della funzione
- ID VPC
- Media richiami giornalieri
- Ora ultimo aggiornamento

AWS Outposts Implementazione a rack singolo

Description

Controlla il saldo degli Outposts Racks. Questo valuta se le istanze Outposts di un cliente sono distribuite su più rack Outposts o su un singolo Outpost Rack. Un singolo rack Outposts crea un singolo punto di errore per problemi che coinvolgono un singolo rack (ad esempio, guasti ambientali). Questi scenari possono essere mitigati installando avamposti su più rack.

ID di controllo

c243hjzrhn

Criteri di avviso

- Giallo: il tuo Outpost è installato su un singolo rack
- Verde: il tuo Outpost è distribuito su più rack.

Operazione consigliata

Se esegui carichi di lavoro di produzione AWS Outposts, è consigliabile utilizzare la seguente architettura resiliente. Un singolo AWS Outposts rack crea un singolo punto di errore. Prendi in considerazione l'aggiunta di un secondo AWS Outposts rack a quella posizione con una capacità sufficiente per un evento di failover, quindi distribuisce i carichi di lavoro tra i rack.

Risorse aggiuntive

[Modalità di guasto 4: rack o data center](#)

Colonne del report

- Status
- ARN risorsa

- AZ
- Numero di rack
- Ora ultimo aggiornamento

AWS Resilience Hub Controllo dei componenti dell'applicazione

Description

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

- Status

- Region
- Nome applicazione
- AppComponent Nome
- Ora ultimo aggiornamento

AWS Resilience Hub politica violata

Description

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

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Nome applicazione
- Ora ultimo aggiornamento

AWS Resilience Hub punteggi di resilienza

Description

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

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Nome applicazione
- Punteggio di resilienza dell'applicazione
- Ora ultimo aggiornamento

AWS Resilience Hub età di valutazione

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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

Description

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 [Cos'è la AWS Site-to-Site VPN?](#)

 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz123

Origine

AWS Config Managed Rule: vpc-vpn-2-tunnels-up

Criteri di avviso

Giallo: una Site-to-Site VPN ha almeno un tunnel inattivo.

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

- Status
- Region
- Risorsa
- AWS Config Regola
- Parametri di input

- Ora ultimo aggiornamento

AWS STS utilizzo globale degli endpoint in tutto il mondo Regioni AWS

Description

Questo controllo identifica un rischio di resilienza quando i AWS carichi di lavoro effettuano chiamate interregionali all'endpoint globale STS nella regione Stati Uniti orientali (Virginia settentrionale). AWS i carichi di lavoro che effettuano richieste interregionali all'endpoint globale STS negli Stati Uniti orientali (Virginia settentrionale) potrebbero risentire negativamente dell'impatto sulla connettività all'endpoint STS degli Stati Uniti orientali (Virginia settentrionale).

Nell'aprile 2025, abbiamo AWS migliorato l'endpoint globale per servire automaticamente le chiamate agli endpoint globali STS nella stessa regione in cui sono in esecuzione i carichi di lavoro, per tutte le chiamate abilitate per impostazione predefinita. AWS Regioni AWS Tuttavia, alcuni carichi di lavoro, come quelli in esecuzione in regioni opt-in o quelli che non utilizzano server Amazon DNS, non traggono vantaggio dalla latenza ridotta e dall'[isolamento degli errori](#) offerti come parte di questo miglioramento. Per questi carichi di lavoro, le richieste di endpoint globali STS vengono gestite nella regione Stati Uniti orientali (Virginia settentrionale), il che comporta un rischio di resilienza per l'applicazione e un aumento della latenza delle richieste STS.

Note

I risultati di questo controllo vengono aggiornati automaticamente più volte al giorno, ogni volta negli ultimi 15 giorni. Le richieste di aggiornamento non sono consentite. Pertanto, potrebbero essere necessari fino a 15 giorni prima che le modifiche vengano visualizzate nei risultati del Trusted Advisor controllo.

Per i clienti Business, Enterprise On-Ramp o Enterprise Support, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c15m0mg1d3

Criteri di avviso

Rosso: i carichi di lavoro effettuano chiamate interregionali verso l'endpoint AWS STS globale nella regione Stati Uniti orientali (Virginia settentrionale).

Azione consigliata

Per migliorare la resilienza e le prestazioni dei carichi di lavoro, ti consigliamo di migrare dall'endpoint globale STS all'endpoint regionale STS. Utilizzando un endpoint regionale, puoi utilizzarlo AWS STS nella stessa regione dei tuoi carichi di lavoro.

Di seguito è riportato un elenco di principali AWS Identity and Access Management (IAM) che effettuano chiamate interregionali verso l'endpoint AWS STS globale nella regione Stati Uniti orientali (Virginia settentrionale). Seguendo i passaggi riportati nel post del blog [Come utilizzare gli AWS STS endpoint regionali, puoi riconfigurare](#) i tuoi carichi di lavoro per utilizzare l'endpoint STS regionale.

Status	ARN principale	Tipo principale IAM	Azione	Ora ultimo aggiornamento	Regione di origine
Rosso	arn:aws:iam::999999999:ruolo/esempio	Ruolo	AssumeRole	01/01/2025 ALLE 08:00.000 Z	ca-west-1
Rosso	arn:aws:iam::123456789012:user/JohnDoe	Utente	GetCallerIdentity	01/01/2025 ALLE 08:00.000 Z	ca-west-1
Rosso	arn:aws:sts::123456789012:federated-user/<Name>	Utente federato	GetCallerIdentity	01/01/2025 ALLE 08:00.000 Z	eu-west-2
Rosso	arn:aws:iam::123456789012:root	Radice	AssumeRole	2025-01-01T 08:00.000 Z	il-central-1
Rosso	arn:aws:sts::0123456789012:	Ruolo di identità	GetCallerIdentity	2025-01-01T 08:00.000 HZ	us-west-1

Status	ARN principale	Tipo principale e IAM	Azione	Ora ultimo aggiornamento	Regione di origine
	presupposto - -01234567 89 esempio role/aws:ec2- instance/i	dell'istanza EC2			

Risorse aggiuntive

- [Gestisci in un AWS STS Regione AWS](#)
- [AWS STS Endpoint regionali](#)

Colonne del report

- Status
- Preside Arn
- Azione
- Tipo di principale
- Regione di origine
- Ora ultimo aggiornamento

AWS Well-Architected Problemi ad alto rischio di per l'affidabilità

Description

Verifica la presenza di problemi ad alto rischio (HRIs) per i carichi di lavoro nel pilastro dell'affidabilità. 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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 identificati per l'affidabilità HRIs
- Numero di risposte HRIs risolte per l'affidabilità
- Numero di domande risposte per Affidabilità
- Numero totale di domande nel pilastro Affidabilità
- Ora ultimo aggiornamento

Classic Load Balancer non ha configurazioni multiple AZs

Description

Verifica se Classic Load Balancer si estende su più zone di disponibilità (). AZs

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.

È possibile modificare il numero minimo di zone di disponibilità utilizzando il `minAvailabilityZones` parametro nelle 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

`c18d2gz154`

Origine

AWS Config Managed Rule: `clb-multiple-az`

Criteri di avviso

Giallo: Classic Load Balancer non dispone di Multi-AZ configurato o non soddisfa il numero minimo specificato. AZs

Operazione consigliata

Assicurati che per i Classic Load Balancer siano configurate più zone di disponibilità. Distribuisci il tuo sistema di bilanciamento del carico su più livelli AZs per assicurarti un'elevata disponibilità dell'applicazione.

Per ulteriori informazioni, consulta [Tutorial: creazione di un Classic Load Balancer](#).

Colonne del report

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

Connection Draining CLB

Description

Verifica la presenza di sistemi di bilanciamento del carico Classic che non dispongono del drenaggio della connessione abilitato.

Quando il drenaggio della connessione non è abilitato e annulli la registrazione di un'istanza Amazon EC2 da un sistema di bilanciamento del carico Classic, il sistema di bilanciamento del carico Classic interrompe l'instradamento del traffico verso quell'istanza e chiude la connessione. Quando il drenaggio della connessione è abilitato, il sistema di bilanciamento del carico Classic interrompe l'invio di nuove richieste all'istanza annullata ma mantiene la connessione aperta per soddisfare le richieste attive.

ID di controllo

7qGXsKIUw

Criteri di avviso

- Giallo: il drenaggio della connessione non è abilitato per un sistema di bilanciamento del carico Classic.
- Verde: il drenaggio della connessione è abilitato per il sistema di bilanciamento del carico Classic.

Operazione consigliata

Abilita il drenaggio della connessione per il sistema di bilanciamento del carico Classic. 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

- Status
- Region
- Nome del load balancer
- Motivo

Elb Target Squilibrio

Description

Verifica la distribuzione dei target dei gruppi target tra le zone di disponibilità (AZs) per Application Load Balancer (ALB), Network Load Balancer (NLB) e Gateway Load Balancer (GWLB).

Questo controllo esclude quanto segue:

- Bilanciatori di carico configurati con un'unica zona di disponibilità (AZ).
- Bilanciatori del carico in cui la differenza nel numero di destinazioni tra quelle più popolate e quelle meno popolate AZs è uguale o inferiore a 1.
- Gruppi target con obiettivi basati su IP in cui l' AvailabilityZone attributo è impostato su «tutto».

ID di controllo

b92b83d667

Criteri di avviso

- Rosso: una singola AZ rappresenta oltre il 66% della capacità del load balancer.
- Giallo: una singola AZ rappresenta più del 50% della capacità del load balancer.
- Verde: No AZs rappresenta più del 50% della capacità del load balancer.

Operazione consigliata

Per una migliore resilienza, assicurati che i tuoi gruppi target abbiano lo stesso numero di obiettivi.
AZs

Risorse aggiuntive

[Gruppi target per i tuoi Application Load Balancer](#)

[Registra gli obiettivi con il tuo gruppo target di Application Load Balancer](#)

Colonne del report

- Status
- Region
- Nome del load balancer
- Tipo di Load Balancer
- ARN del gruppo target (arn)
- Differenza tra gli obiettivi registrati AZs
- Ora ultimo aggiornamento

GWLB: indipendenza dall'endpoint AZ

Description

Verifica se gli endpoint Gateway Load Balancer (GWLB) sono configurati come destinazione di routing da un'altra zona di disponibilità (AZ).

Gli endpoint Gateway Load Balancer inoltrano il traffico di rete alle appliance firewall protette da un Gateway Load Balancer per l'ispezione. Ogni endpoint Gateway Load Balancer opera all'interno di una zona specifica ed è costruito con ridondanza solo in quella zona. Pertanto, tutte le risorse in una particolare AZ devono utilizzare un endpoint Gateway Load Balancer nella stessa AZ. Ciò garantisce che qualsiasi potenziale interruzione di un endpoint Gateway Load Balancer o della relativa zona di disponibilità non influisca sulle risorse in un'altra zona.

ID di controllo

528d6f5ee7

Criteri di avviso

- Giallo: il traffico proveniente dalla sottorete in una AZ viene instradato attraverso un endpoint Gateway Load Balancer in un'altra AZ.

- Verde: il traffico proveniente dalla sottorete in una AZ viene instradato attraverso un endpoint Gateway Load Balancer nella stessa AZ.

Operazione consigliata

Controlla la zona di disponibilità della sottorete e configurane la tabella di routing per indirizzare il traffico attraverso un endpoint Gateway Load Balancer nella stessa AZ.

Se non è presente alcun endpoint Gateway Load Balancer nell'AZ, creane uno nuovo e quindi instrada il traffico della sottorete attraverso di esso.

Se hai la stessa tabella di routing associata a sottoreti diverse AZs, mantieni questa tabella di routing associata alle sottoreti che risiedono nella stessa AZ dell'endpoint Gateway Load Balancer. Per le sottoreti nell'altra AZ, è quindi possibile associare una tabella di routing separata a una route verso un endpoint Gateway Load Balancer in questa AZ.

È consigliabile scegliere una finestra di manutenzione per le modifiche all'architettura nel tuo Amazon VPC.

Risorse aggiuntive

- [Indipendenza dalla zona di disponibilità](#)
- [Configurazione del routing per l'endpoint Gateway Load Balancer](#)
- [AWS Well-Architected Tool - Utilizza architetture bulkhead per limitare l'ambito di impatto](#)

Colonne del report

- Status
- Region
- Elenco ID di sottorete Cross AZ
- ID dell'endpoint Gateway Load Balancer
- ID della sottorete dell'endpoint Gateway Load Balancer
- Subnet AZ di endpoint VPC
- Ora ultimo aggiornamento

Ottimizzazione del load balancer

Description

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

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 hai la stessa tabella di routing associata a sottoreti diverse AZs, mantieni questa tabella di routing associata alle sottoreti che risiedono nella stessa AZ del gateway NAT e per le sottoreti nell'altra AZ, associa una tabella di route separata a una route verso un gateway NAT in 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

- Status
- Region
- 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

Network Firewall endpoint AZ Independence

Description

Verifica se gli AWS Network Firewall endpoint sono configurati come destinazione del percorso da un'altra zona di disponibilità (AZ).

Gli endpoint Network Firewall inoltrano il traffico di rete a un Network Firewall per l'ispezione. Ogni endpoint Network Firewall opera all'interno di una zona di attività designata ed è costruito con ridondanza solo in quella zona. Le tue risorse in una particolare AZ devono utilizzare un endpoint Network Firewall nella stessa AZ. In questo modo si garantisce che qualsiasi potenziale interruzione di un endpoint Network Firewall o della relativa zona di disponibilità non influisca sulle risorse in un'altra zona. Il traffico di rete che ha origine in una zona diversa per l'ispezione del traffico comporta costi di trasferimento dati tra le AZ. È consigliabile assicurarsi che tutte le risorse di una zona specifica utilizzino un Network Firewall nella stessa zona per evitare addebiti sui dati tra diverse AZ.

ID di controllo

7040ea389a

Criteri di avviso

- Giallo: il traffico proveniente da una sottorete in una AZ viene instradato attraverso un endpoint Network Firewall in un'altra AZ.
- Verde: il traffico proveniente da una sottorete in una zona di disponibilità viene instradato attraverso un endpoint Network Firewall nella stessa zona di distribuzione.

Operazione consigliata

Controlla la zona di disponibilità della sottorete e indirizzate il traffico attraverso un endpoint Network Firewall nella stessa zona.

Se nella zona AZ non è presente alcun endpoint Network Firewall, crea un nuovo Network Firewall e instrada il traffico della sottorete attraverso di esso.

Se la stessa tabella di routing è associata a più sottoreti diverse AZs, mantieni questa tabella di routing associata alle sottoreti che risiedono nella stessa AZ dell'endpoint Network Firewall. Per le sottoreti in altre aree AZs, associa una tabella di routing separata a una route verso un endpoint Network Firewall in quella zona.

È consigliabile scegliere una finestra di manutenzione per le modifiche all'architettura nel tuo Amazon VPC.

Risorse aggiuntive

[Trasferimento dati all'interno dello stesso Regione AWS](#)

[Comprensione dei costi di trasferimento dei dati](#)

[Indipendenza dalla zona di disponibilità](#)

[Procedure di alto livello per l'implementazione di un firewall](#)

[Creazione di un firewall](#)

[AWS Well-Architected Tool - Utilizza architetture bulkhead per limitare l'ambito di impatto](#)

Colonne del report

- Status
- Region
- ID dell'endpoint del Network Firewall
- Network Firewall Arn
- Subnet Network Firewall Endpoint
- Network Firewall Endpoint AZ
- Elenco di sottoreti Cross AZ
- Ora ultimo aggiornamento

Network Firewall Multi-AZ

Description

Verifica se i firewall di rete sono configurati per utilizzare più di una zona di disponibilità (AZ) per gli endpoint del firewall.

Una AZ è una posizione distinta isolata dai guasti in altre zone. Se l'endpoint Network Firewall viene distribuito solo in 1 zona di disponibilità, può costituire un singolo punto di errore e compromettere i carichi di lavoro di altri utenti che utilizzano il AZs Network Firewall per l'ispezione del traffico. È consigliabile configurare più firewall di rete nella stessa regione per migliorare la AZs disponibilità dei carichi di lavoro.

ID di controllo

c2v1fg0gqd

Criteri di avviso

- Giallo: l'endpoint Network Firewall è distribuito in 1 zona.

- Verde: gli endpoint Network Firewall sono distribuiti in almeno due. AZs

Operazione consigliata

Assicurati che il tuo Network Firewall sia configurato con almeno due AZs per i carichi di lavoro di produzione.

Risorse aggiuntive

[Configurazione della sottorete VPC per AWS Network Firewall](#)

[Creazione di un firewall](#)

[Zona di disponibilità](#)

[AWS Well-Architected Tool - Distribuisci il carico di lavoro in più posizioni](#)

[Appliance in un VPC con servizi condivisi](#)

Colonne del report

- Status
- Region
- Network Firewall Arn
- Id VPC
- Sottoreti Network Firewall
- Sottoreti Network Firewall AZs
- Ora ultimo aggiornamento

Bilanciamento del carico tra zone di Network Load Balancer

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- AWS Config Regola
- Parametri di input

- Ora ultimo aggiornamento

NLB: risorsa rivolta a Internet in sottorete privata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 sistema di bilanciamento del carico 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

- Status
- Region
- NLB Arn
- Nome NLB
- ID sottorete
- Schema NLB
- Tipo di sottorete
- Ora ultimo aggiornamento

NLB Multi-AZ

Description

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 parti AZs 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c1dfprch09

Criteri di avviso

Giallo: NLB si trova in una sola AZ.

Verde: NLB ne ha due o più. AZs

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: distribuisce il carico di lavoro in più sedi](#)
- [Regioni e zone di disponibilità](#)

Colonne del report

- Status
- Region
- Numero di AZs
- NLB ARN
- Nome NLB
- Ora ultimo aggiornamento

Numero di componenti Regioni AWS in un set di repliche di Incident Manager

Description

Verifica che la configurazione di un set di repliche di Incident Manager ne utilizzi più di una 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Multi-regione
- Set di repliche
- Ora ultimo aggiornamento

Controllo dell'applicazione in una singola AZ

Description

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. Distribuendo il servizio su più piattaforme AZs, si limita il raggio di esplosione di un guasto 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- ID VPC
- Ora ultimo aggiornamento

Interfaccia VPC (interfacce di rete endpoint multiple) AZs

Description

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 i paesi della stessa AZs regione. AWS Seleziona più sottoreti AZs 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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. AZs

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 e Servizio AWS utilizzare 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

- Status
- Region
- ID dell'endpoint VPC
- È Multi AZ
- Ora ultimo aggiornamento

Ridondanza del Tunnel VPN

Description

Controlla il numero di tunnel attivi per ciascuno dei tuoi. Site-to-Site VPNs

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 l'utente di AWS Site-to-Site 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 [Il dispositivo gateway del cliente](#) o [Eliminazione di una connessione Site-to-Site VPN](#).

Risorse aggiuntive

- [AWS Site-to-Site Guida per l'utente della VPN](#)
- [Crea un gateway di destinazione](#)

Colonne del report

- Status
- Region
- ID VPN
- VPC
- Gateway virtuale privato
- Gateway del cliente
- Tunnel attivi
- Motivo

Ridondanza della zona di disponibilità ActiveMQ

Description

Verifica che i broker Amazon MQ for ActiveMQ siano configurati per l'alta disponibilità con active/standby un broker 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 active/standby implementazione.

Risorse aggiuntive

- [Creazione di un broker ActiveMQ](#)

Colonne del report

- Status
- Region
- ID del broker ActiveMQ
- Tipo di motore del broker
- Modalità di implementazione
- Ora ultimo aggiornamento

Ridondanza della zona di disponibilità RabbitMQ

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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: non Trusted Advisor è stato possibile 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 aprire una richiesta di assistenza in Support Center.](#)

Colonne del report

- Status
- 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 di volume EBS Provisioned IOPS SSD \(io1\)](#)
- [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-Classical](#)
- [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

fw7HH017J9

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

aw7HH017J9

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

gW7HH017J9

Risorse aggiuntive

[CloudFormation quote](#)

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

eI7KK017J9

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

dH7RR016J9

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

dH7RR016J3

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

cG7HH017J9

Risorse aggiuntive

[Limiti di Amazon EBS](#)

IOPS aggregati di volume EBS Provisioned IOPS SSD (io1)

Description

Verifica che l'utilizzo sia superiore all'80% della quota IOPS aggregata di volume EBS Provisioned IOPS SSD (io1).

ID di controllo

tV7YY017J9

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

gI7MM017J9

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

gI7MM017J2

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

wH7DD013J9

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

iH7PP017J9

Risorse aggiuntive

[Quote di Amazon EC2](#)

Indirizzi IP elastici EC2-Classical

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota degli indirizzi IP elastici EC2-Classical.

ID di controllo

aW9HH018J6

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

1N7RR017J9

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

EM8b3yLRTx

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

iK700017J9

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

sU7XX017J9

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

n07SS017J9

Risorse aggiuntive

[Quote di IAM](#)

Policy IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota delle policy IAM.

ID di controllo

pR7UU017J9

Risorse aggiuntive

[Quote di IAM](#)

Ruoli IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota dei ruoli IAM.

ID di controllo

oQ7TT017J9

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

rT7WW017J9

Risorse aggiuntive

[Quote di IAM](#)

Utenti IAM

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota degli utenti IAM.

ID di controllo

qS7VV017J9

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

bw7HH017J9

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 aprire una richiesta di assistenza in Support Center.

Risorse aggiuntive

- [Utilizzo dell'archiviazione di codice Lambda](#)

Colonne del report

- Status
- Region
- L'ARN della funzione qualificata per tale risorsa.
- L'utilizzo della memorizzazione del codice funzionale 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

jt1IM03qZM

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

gfZAn3W7w1

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

3Njm0DJQ09

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

hJ7NN017J9

Risorse aggiuntive

[Quote di Amazon SES](#)

VPC

Description

Verifica eventuali occorrenze di utilizzo superiore all'80% della quota VPC.

ID di controllo

jL7PP017J9

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

kM7QQ017J9

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](#)
- [Amazon API Gateway REST APIs senza tracciamento a raggi X 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](#)
- [La registrazione OpenSearch di Amazon Service CloudWatch non è 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](#)
- [Registri di accesso Amazon S3 abilitati](#)
- [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](#)
- [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

Description

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 dal tuo. APIs 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 il tuo Amazon API Gateway [REST APIs](#) o [WebSocket APIs](#) con il livello di registrazione appropriato (ERROR, INFO).

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

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

Amazon API Gateway REST APIs senza tracciamento a raggi X abilitato

Description

Verifica se Amazon API Gateway REST APIs ha il AWS X-Ray tracciamento attivato.

Attiva il tracciamento X-Ray per il tuo REST per consentire APIs ad API Gateway di campionare le richieste di chiamata API con informazioni di tracciamento. In questo modo puoi trarre vantaggio dal tracciamento e dall'analisi delle AWS X-Ray richieste mentre viaggiano attraverso il tuo API Gateway REST APIs verso i servizi downstream.

Per ulteriori informazioni, vedere [Tracciamento delle richieste degli utenti su REST APIs 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 il tuo API Gateway REST. APIs

Per ulteriori informazioni, consulta [Configurazione AWS X-Ray con API Gateway REST APIs](#).

Risorse aggiuntive

- [Tracciamento delle richieste degli utenti su REST APIs utilizzando X-Ray](#)
- [Che cos'è? AWS X-Ray](#)

Colonne del report

- Status

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

Amazon CloudFront Access Log configurato

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

L'azione CloudWatch di Amazon Alarm è disabilitata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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](#) AWS CLI Command Reference e [func \(*CloudWatch\) EnableAlarmActions](#) nell' AWS SDK for Go API Reference.

Colonne del report

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

Istanza Amazon EC2 non gestita da AWS Systems Manager

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Repository di Amazon ECR con immutabilità dei tag disabilitata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Cluster di Amazon ECS con approfondimenti sui container disabilitati

Description

Verifica se Amazon CloudWatch Container Insights è attivato per i tuoi cluster Amazon ECS.

CloudWatch Container Insights raccoglie, aggrega e riepiloga metriche e 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

La registrazione dei log delle attività di Amazon ECS non è abilitata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 CloudWatch Logs o a un altro driver di registrazione.

Per ulteriori informazioni, consulta [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

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

La registrazione OpenSearch di Amazon Service CloudWatch non è configurata

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Istanze database Amazon RDS nei cluster con gruppi di parametri eterogenei

Description

È consigliabile che tutte le istanze database nel cluster di database utilizzino lo stesso gruppo di parametri 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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

Associare l'istanza database al gruppo di parametri database associato all'istanza di scrittura nel cluster di database.

Risorse aggiuntive

Quando le istanze DB del cluster di database utilizzano diversi gruppi di parametri DB, può verificarsi un comportamento incoerente durante un failover o problemi di compatibilità tra le istanze DB del cluster di database.

Per ulteriori informazioni, consulta la sezione [Uso di gruppi di parametri](#).

Colonne del report

- Status
- Region
- Risorsa

- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Amazon RDS Enhanced Monitoring è disattivato

Description

Il monitoraggio avanzato non è attivato per le risorse del database. Il monitoraggio avanzato offre le metriche 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

Attivare 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

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Amazon RDS Performance Insights è disattivato

Description

Amazon RDS Performance Insights monitora il carico dell'istanza DB per aiutarti ad analizzare e risolvere i problemi di prestazioni del database. È consigliabile attivare Approfondimenti sulle 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

 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 DB con Performance Insights su Amazon Aurora](#).

Colonne del report

- Status
- Region
- Risorsa
- Valore consigliato
- Nome del motore
- Ora ultimo aggiornamento

Il parametro Amazon RDS track_counts è disattivato

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- Risorsa
- Valore del parametro
- Valore consigliato
- Ora ultimo aggiornamento

Registrazione dei log di controllo del cluster di Amazon Redshift

Description

Controlla se la registrazione dei log di controllo del database è attivata per i cluster di Amazon Redshift. Amazon Redshift registra le informazioni sulle connessioni e le attività degli utenti nel tuo 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Registri di accesso Amazon S3 abilitati

Description

Verifica la configurazione di registrazione dei bucket di Amazon Simple Storage Service.

L'attivazione della registrazione degli accessi al server fornisce log di accesso orari dettagliati a un bucket Amazon S3 specifico. I log di accesso contengono i dettagli della richiesta, tra cui tipo, risorse specificate e data/ora di elaborazione. La registrazione è disattivata per impostazione

predefinita. I clienti devono attivare la registrazione degli accessi per eseguire controlli di sicurezza o analizzare il comportamento e i modelli di utilizzo degli utenti.

Quando la registrazione viene inizialmente attivata, la configurazione viene convalidata automaticamente. Tuttavia, le modifiche future possono causare errori di registrazione. Tieni presente che attualmente questo controllo non esamina le autorizzazioni di scrittura del bucket Amazon S3.

ID di controllo

c1fd6b9614

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.
- Verde: Bucket ha la registrazione degli accessi al server abilitata, la destinazione esiste ed esistono le autorizzazioni per scrivere sulla destinazione

Operazione consigliata

Attiva la registrazione degli accessi al server per tutti i bucket Amazon S3 pertinenti. I log di accesso al server forniscono una pista di controllo che può essere utilizzata per comprendere i modelli di accesso ai bucket e indagare su attività sospette. L'attivazione della registrazione su tutti i bucket applicabili migliorerà la visibilità degli eventi di accesso nel tuo ambiente Amazon S3. 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](#).

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

- Status
- Region
- ARN risorsa
- Bucket Name (Nome bucket)
- Nome destinazione
- Destinazione esistente
- Stesso proprietario
- Scrittura abilitata
- Motivo
- Ora ultimo aggiornamento

Per Amazon S3 non sono abilitate le Notifiche di eventi

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz163

Origine

AWS Config Managed Rule: s3-event-notifications-enabled

Criteri di avviso

Giallo: Amazon S3 non ha le notifiche degli eventi abilitate o non è configurato 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

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Amazon VPC senza log di flusso

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz122

Origine

AWS Config Managed Rule: vpc-flow-logs-enabled

Criteri di avviso

Giallo: VPCs non dispongono di Amazon VPC Flow Logs.

Operazione consigliata

Crea log di flusso VPC per ognuno dei tuoi VPCs

Per ulteriori informazioni, consulta [Creazione di un log di flusso](#)

Colonne del report

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

Application Load Balancer e Classic Load Balancer senza log di accesso abilitati

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

CloudFormation Notifica Stack

Description

Verifica se tutti i tuoi CloudFormation stack utilizzano Amazon SNS per ricevere notifiche quando si verifica un evento.

Puoi configurare questo controllo per cercare argomenti specifici di Amazon SNS ARNs utilizzando i parametri nelle tue AWS Config regole.

Per ulteriori informazioni, consulta [Impostazione delle opzioni 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 CloudFormation stack non sono attivate.

Operazione consigliata

Assicurati che i tuoi 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

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

AWS CodeBuild Registrazione del progetto

Description

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 cloudWatchGroup 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

ID di controllo

c18d2gz113

Origine

AWS Config Managed Rule: codebuild-project-logging-enabled

Criteri di avviso

Giallo: la registrazione AWS CodeBuild del 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

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

AWS CodeDeploy Rollback e monitoraggio automatici abilitati

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

AWS CodeDeploy Lambda utilizza all-at-once la configurazione di distribuzione

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 dell'implementazione](#)

Colonne del report

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

AWS Elastic Beanstalk Enhanced Health Reporting non è configurato

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

AWS Elastic Beanstalk con gli aggiornamenti gestiti della piattaforma disattivati

Description

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 `UpdateLevel` parametri 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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 affatto configurati, 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

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

AWS Fargate la versione della piattaforma non è la più recente

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

AWS Systems Manager State Manager Association in stato di non conformità

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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 State Manager](#)

Colonne del report

- Status
- Region

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

CloudTrail i trail non sono configurati con Amazon CloudWatch Logs

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

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

Controllo della protezione dall'eliminazione del cluster DB di RDS

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

Risorse aggiuntive

[Protezione dall'eliminazione per i cluster di Aurora](#)

Colonne del report

- Status

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

Controllo automatico dell'aggiornamento delle versioni secondarie di istanze DB di RDS

Description

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.

Per i clienti del piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi utilizzare l'[BatchUpdateRecommendationResourceExclusion](#) API per includere o escludere una o più risorse dai risultati. Trusted Advisor

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

- Status
- Region
- 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' API Supporto AWS, i controlli obsoleti non verranno visualizzati nei risultati dei controlli. Se utilizzi un controllo obsoleto, ad esempio specificando l'ID di controllo in un'operazione Supporto AWS API o il tuo codice, ricevi errori di chiamata API. Rimuovi questi controlli per evitare errori.

Per ulteriori informazioni sulle operazioni API disponibili, consulta la sezione [AWS Trusted Advisor verifica riferimento](#).

Modifica data	Nome di controllo	Descrizione della modifica
19 febbraio 2026	Nuovi gateway NAT inattivi	È stato aggiunto un nuovo controllo per identificare i gateway NAT inattivi o sottoutilizzati che potrebbero essere candidati all'ottimizzazione dei costi.
9 gennaio 2026	5 controlli di ottimizzazione dei costi obsoleti Trusted Advisor	I seguenti controlli erano obsoleti: • Savings Plan - VZ2C2W1SRF • Ottimizzazione delle istanze riservate di Amazon Relational Database Service (RDS) - 1QaZXsw23E • Ottimizzazione dei nodi riservati Amazon Redshift - 1qw23er45t • Ottimizzazione dei nodi ElastiCache riservati Amazon - H3L1oTH3RE • Ottimizzazione delle istanze riservate OpenSearch di Amazon Service - 7ujm6yhn5t
18 dicembre 2025	Versioni aggiornate per Amazon S3 Bucket	È stato aggiunto un nuovo criterio di avviso: • Giallo: Trusted Advisor non ha accesso per convalidare il controllo delle versioni

Modifica data	Nome di controllo	Descrizione della modifica
17 dicembre 2025	Autorizzazioni Amazon S3 Bucket aggiornate	È stata aggiornata la sezione Criteri di avviso.
21 novembre 2025	Gruppo di sicurezza Applicati on Load Balancer aggiornato	Sono stati aggiornati gli avvisi e i consigli del gruppo di sicurezza Application Load Balancer.
17 novembre 2025	Utilizzo AWS STS globale degli endpoint aggiornato nella descrizione del controllo Regioni AWS	È stato aggiornato l'utilizzo o AWS STS globale degli endpoint nella descrizione del Regioni AWS controllo per chiarire quando i risultati del controllo vengono aggiornati.
15 ottobre 2025	Descrizioni di controllo multiple aggiornate	È stata aggiunta una nota a più descrizioni di controllo per indicare che il controllo riporta tutte le risorse contrassegnate in base ai criteri e il numero totale di risorse valutate, comprese le risorse. OK La tabella delle risorse elenca solo le risorse contrassegnate.
10 ottobre 2025	Riferimento di controllo aggiornato	Aggiornato il riferimento del controllo per mostrare tutti i controlli disponibili.
11 settembre 2025	L4DFS2Q4C5: funzioni che utilizzano runtime obsoleti AWS Lambda	Criterio di avviso giallo aggiornato per indicare che sono inclusi i runtime obsoleti entro almeno 180.

Modifica data	Nome di controllo	Descrizione della modifica
19 agosto 2025	Pfx0RwqBli: autorizzazioni per i bucket Amazon S3	Criteri di avviso aggiornati: Trusted Advisor non dispone dell'autorizzazione per verificar e la policy o l'ACL, oppure la policy o l'ACL non possono essere valutati per altri motivi cambiati da giallo a rosso.
22 luglio 2025	- vjaf H0: UGJ9 Registrazione AWS CloudTrail - BueAdj7nRP: registrazione dei bucket Amazon S3	Questi controlli sono obsoleti.
03 luglio 2025	Pfx0RwqBli: autorizzazioni per i bucket Amazon S3	I criteri di avviso vengono aggiornati per riflettere tutti i criteri gialli e rossi.
03 luglio 2025	c1dfprch15: Fine del supporto standard per le istanze Amazon EC2 con Ubuntu LTS	È stata aggiornata la nota per indicare che questo controllo viene aggiornato almeno una volta al giorno.
02 luglio 2025	c1dvkm4z6b: driver Amazon ECS in modalità di blocco AWSLogs	Amazon ECS ha modificato l'impostazione predefinita per la modalità dei parametri di configurazione della registrazione dei driver awslogs da a. blocking non-blocking. La descrizione dello stato in giallo è stata aggiornata per riflettere questa modifica.

Modifica data	Nome di controllo	Descrizione della modifica
02 luglio 2025	7 DAFEmo cose da fare: MFA sull'account root	Sono state aggiunte informazioni che indicano che le credenziali utente root dell'account membro possono essere eliminate centralmente, eliminando la necessità di gestire l'MFA sulle credenziali dell'utente root.
9 giugno 2025	c1z7kmr17n: raccomandazioni per l'ottimizzazione dei costi di Amazon Aurora per lo storage in cluster DB	Nuovo assegno
9 giugno 2025	c15m0mgld3: utilizzo globale degli endpoint in tutto AWS STSRegioni AWS	Controllo aggiornato: questo controllo è ora disponibile per tutti i piani. Supporto AWS
02 giugno 2025	c15m0mgld3: utilizzo globale degli endpoint in tutto AWS STSRegioni AWS	Nuovo controllo

Modifica data	Nome di controllo	Descrizione della modifica
30 maggio 2025	- c1z7kmr15n: Consigli per l'acquisto di capacità riservata di Amazon DynamoDB - c1z7kmr02n: Raccomandazioni per l'ottimizzazione dei costi di Amazon EBS per i volumi - c1z7kmr01n: Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per i gruppi Amazon EC2 Auto Scaling - c1z7kmr00n: Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per le istanze - c1z7kmr13n: Consigli per l'acquisto di nodi ElastiCache riservati Amazon - c1z7kmr16n: Consigli per l'acquisto di nodi riservati Amazon MemoryDB - c1z7kmr14n: Consigli per l'acquisto di istanze riservate di Amazon OpenSearch Service - c1z7kmr04n: Consigli per l'ottimizzazione dei costi di Amazon RDS per lo storage di istanze DB - c1z7kmr03n: Consigli per l'ottimizzazione dei costi di	Nuovi controlli dell'hub di ottimizzazione dei costi

Modifica data	Nome di controllo	Descrizione della modifica
	Amazon RDS per le istanze DB • c1z7kmr11n: Consigli per l'acquisto di istanze riservate Amazon RDS • c1z7kmr12n: Consigli per l'acquisto di nodi riservati Amazon Redshift • c1z7kmr06n: AWS Fargate consigli per l'ottimizzazione dei costi per Amazon ECS • c1z7kmr05n: AWS Lambda raccomandazioni per l'ottimizzazione dei costi per le funzioni • c1z7kmr08n: AWS Consigli per l'acquisto di Savings Plans per Amazon SageMaker AI • c1z7kmr09n: AWS Consigli per l'acquisto di Savings Plans per l'elaborazione	
30 aprile 2025	• N420c450f2: nomi di dominio alternativi CloudFront • N425c450f2: certificati SSL personalizzati nell'archivio certificati IAM CloudFront	È stata aggiunta una nota che indica che questo controllo si applica alle CloudFront distribuzioni Amazon classiche .

Modifica data	Nome di controllo	Descrizione della modifica
30 aprile 2025	N415c450f2: CloudFront header forwarding e cache hit ratio	È stata aggiunta una nota che indica che questo controllo si applica alle CloudFront distribuzioni Amazon classiche.
02 aprile 2025	c1dfprch02: Ottimizzazione della modalità di throughput di Amazon EFS	La descrizione di questo controllo è cambiata. Per ulteriori informazioni, consulta la pagina Istanze Amazon EC2 con fine del supporto per Microsoft Windows Server .
02 aprile 2025	Qsdfp3A4L4: fine del supporto per istanze Amazon EC2 con Microsoft Windows Server	La descrizione di questo controllo è cambiata. Per ulteriori informazioni, consulta Amazon EFS Throughput Mode Optimization .

Aggiornamenti precedenti

I seguenti AWS Security Hub CSPM controlli sono obsoleti:

Nome di controllo	ID di controllo
S3.10 - I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	Hs4Ma3G211
S3.11 - I bucket S3 per uso generico devono avere le notifiche degli eventi abilitate	Hs4Ma3G212
CodeBuild.5 - gli ambienti di CodeBuild progetto non dovrebbero avere la modalità privilegiata abilitata	Hs4Ma3G218

Nome di controllo	ID di controllo
CloudFormation.1 - gli CloudFormation stack devono essere integrati con Amazon Simple Notification Service (SNS)	Hs4Ma3G245
SNS.2 - La registrazione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento	Hs4Ma3G263
Athena.1 - I gruppi di lavoro Athena devono essere crittografati quando sono inattivi	Hs4Ma3G294

Nuovo controllo: Amazon RDS Continuous Backup non abilitato

Trusted Advisor ha aggiunto il seguente controllo il 23 dicembre 2024.

Nome di controllo	Categoria di controllo	ID di controllo
Backup continuo Amazon RDS non abilitato	Tolleranza ai guasti	44fde09ab5

Verifica se un'istanza Amazon RDS è abilitata con backup automatici utilizzando Amazon RDS o con backup continui di AWS Backup. I backup continui riducono il rischio di perdita imprevista dei dati e consentono il ripristino point-in-time.

Per ulteriori informazioni, consulta [Backup continuo di Amazon RDS non abilitato](#).

Nuovo controllo: registrazione AWS CloudTrail degli eventi di gestione

Trusted Advisor ha aggiunto il seguente controllo il 23 dicembre 2024.

Nome di controllo	Categoria di controllo	ID di controllo
AWS CloudTrail Registrazione degli eventi di gestione	Sicurezza	c25hn9x03v

Verifica l'utilizzo di AWS CloudTrail

Per ulteriori informazioni, consulta [AWS CloudTrail Registrazione degli eventi di gestione](#).

Aggiornato il controllo Auto Scaling Group Resources

Trusted Advisor ha aggiornato il seguente controllo il 23 dicembre 2024.

Nome di controllo	Categoria di controllo	ID di controllo
Risorse dei gruppi Auto Scaling	Tolleranza ai guasti	8CNsS11I5v

La descrizione di questo controllo è stata aggiornata per includere le configurazioni di avvio e i modelli di avvio.

È Red: A launch template is associated with a deleted Amazon Machine Image (AMI) . stato aggiunto un nuovo criterio di avviso.

Per ulteriori informazioni, consulta [Risorse dei gruppi Auto Scaling](#).

È stato aggiornato il controllo degli accessi esterni di IAM Access Analyzer

Trusted Advisor ha aggiornato il seguente controllo il 23 dicembre 2024.

Nome di controllo	Categoria di controllo	ID di controllo
Accesso esterno a IAM Access Analyzer	Sicurezza	07602fcad6

La descrizione di questo controllo viene aggiornata per indicare che analizza l'accesso IAM a livello di account. Per ulteriori informazioni, consulta [Accesso esterno a IAM Access Analyzer](#).

Aggiunto 1 nuovo controllo

Trusted Advisor aggiunto 1 nuovo assegno il 22 novembre 2024:

- [8604e947f2 - Gruppi di sicurezza Application Load Balancer](#)

3 controlli aggiornati

Trusted Advisor 3 controlli aggiornati il 7 novembre 2024:

- [b92b83d667 - Elb Target Squilibrio](#)
- [8 CNs SLLi5v - Risorse del gruppo Auto Scaling](#)
- [WUY7G1zxQI - Bilanciamento della zona di disponibilità di Amazon EC2](#)

Aggiunti 4 controlli

Trusted Advisor ha aggiunto 4 nuovi assegni l'11 ottobre 2024:

- 07602fcad6 - IAM Access Analyzer - accesso esterno
- 528d6f5ee7 - GWLB - Endpoint A
- c2vlf0jp6 - Endpoint di interfaccia VPC inattivi
- c2vlf0k35 - Endpoint Gateway Load Balancer inattivi

3 controlli aggiornati

Trusted Advisor 3 controlli aggiornati il 2 ottobre 2024:

- Check ID 7040ea389a è passato dal pilastro Ottimizzazione dei costi al pilastro Fault Tolerance
- Check ID DAFEmo 7 Dos aggiornato
- ID di controllo aggiornato CMSvnj8db2

Aggiunti 9 nuovi controlli

Trusted Advisor ha aggiunto 9 nuovi controlli il 23 agosto 2024:

- c2vlf0p86 - [IAM] - Provider di identità SAML 2.0
- 7040ea389a - Trasferimento dati Cross-AZ dall'endpoint del Network Firewall
- c2vlf0bfbw - Network Firewall a basso utilizzo
- c2vlf0gqgd - Network Firewall Multi-AZ
- c2vlf0p1w - Protocollo crittografato Application Load Balancer Target Groups

- c2vlf022t - [NAT Gateway] - Risorsa sottoutilizzata
- c243hjzrh - AWS Outposts Implementazione Single Rack
- b92b83d667 - Squilibrio dell'obiettivo ELB
- 90046ff5b5 - La disponibilità di MSK è limitata a due zone

Per ulteriori informazioni, consulta [AWS Trusted Advisor verifica riferimento](#).

Aggiornato 1 controllo di sicurezza e aggiunto 1 controllo di sicurezza

Trusted Advisor ha aggiornato 1 controllo di eccellenza operativa il 22 agosto 2024:

- c1fd6b96l4

Trusted Advisor ha aggiunto 1 controlli di sicurezza il 22 agosto 2024:

- c2vlf0f4h

Per ulteriori informazioni, consulta [AWS Trusted Advisor verifica riferimento](#).

6 controlli di sicurezza aggiornati

Trusted Advisor 6 controlli di sicurezza aggiornati il 20 agosto 2024:

- nNauJisYIT
- C9D319e7sg
- A2 sec 6 ILx
- HCP4007jGY
- 1 iG5 NDGVre
- YW2K9pUPZL

Per ulteriori informazioni, consulta [AWS Trusted Advisor verifica riferimento](#).

1 controllo di tolleranza ai guasti aggiornato

Trusted Advisor ha aggiornato 1 controllo di tolleranza agli errori e 1 di sicurezza il 12 agosto 2024:

- Ridondanza del Tunnel VPN
- È richiesto l'aggiornamento della versione secondaria del motore Amazon RDS

Per ulteriori informazioni, consulta [AWS Trusted Advisor verifica riferimento](#).

9 controlli aggiornati

Trusted Advisor ha aggiornato i 9 controlli il 21 luglio 2024:

- 7q GXs KIUw
- ZRxQIPsb6 c
- N425 c 450 f2
- 7 cani DAFemo
- Pfx0 RwqBli
- H7 IgTzj TYb
- C056F80Cr3
- YW2K9PuPzL
- XsQx82fqu

Per ulteriori informazioni, consulta [AWS Trusted Advisor verifica riferimento](#).

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:

- Direct Connect Ridondanza di connessione
- Direct Connect Ridondanza di ubicazione
- 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:

- 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 multiple) AZs

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 una novità che consente APIs di accedere in modo programmatico ai controlli delle best practice, ai consigli e ai consigli con priorità di Trusted Advisor. Trusted Advisor APIs consentono l'integrazione programmatica Trusted Advisor con lo strumento operativo preferito per automatizzare e ottimizzare i carichi di lavoro su larga scala. Disponibile per i clienti Business, Enterprise On-Ramp o Enterprise Support, il nuovo APIs fornisce 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.

La nuova Trusted Advisor APIs sostituirà le 3 funzionalità precedentemente offerte tramite AWS Support API (SAPI). SAPI continuerà a offrire casi e altre informazioni di supporto.

Trusted Advisor APIs 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 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 [Visualizza AWS Trusted Advisor i controlli 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

- Auto Scaling disponibile nelle sottoreti IPs
- 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 [Performance](#).

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 sviluppatori di Amazon MemoryDB](#)

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 Advisor AWS Security Hub CSPM

Trusted Advisor ha effettuato il seguente aggiornamento il 17 novembre 2022.

Se disabiliti Security Hub CSPM 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 CSPM di Security Hub Trusted Advisor era di 90 giorni.

Per ulteriori informazioni, consulta le sezioni seguenti nell'argomento [Risoluzione dei problemi](#):

- [Ho disattivato Security Hub \(CSPM\) o AWS Config in una regione](#)
- [Il mio controllo è archiviato in Security Hub CSPM, ma vedo 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 sviluppatori di Amazon MemoryDB](#)

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 denominata Trusted Advisor Raccomandazioni. 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' Supporto API come al solito.

Per ulteriori informazioni, consulta [Inizia a usare i Trusted Advisor consigli](#).

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 i controlli CSPM di Security Hub a Trusted Advisor

A partire dal 23 giugno 2022, supporta Trusted Advisor solo i controlli CSPM di 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 AWS Security Hub CSPM dei controlli 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 CSPM.

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	C0r6dfpM03
Volumi Amazon EBS con provisioning insufficiente	Performance	C0r6dfpM04
AWS Lambda funzioni sovradimensionate per le dimensioni della memoria	Ottimizzazione dei costi	C0r6dfpM05
AWS Lambda funzioni con dotazione insufficiente per le dimensioni della memoria	Performance	C0r6dfpM06

Devi optare Account AWS per Compute Optimizer in modo che questi controlli possano ricevere dati dalle tue risorse Lambda e Amazon EBS. 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	12Fnkp18Y5

Trusted Advisor ora aggiorna automaticamente questo controllo. Questo controllo non può essere aggiornato manualmente dalla Trusted Advisor console o dall' API Supporto AWS. 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 CSPM controlli aggiunti alla AWS Trusted Advisor console

AWS Trusted Advisor ha aggiunto 111 controlli CSPM Security Hub alla categoria Sicurezza il 18 gennaio 2022.

Puoi visualizzare i risultati relativi ai controlli CSPM 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 AWS Security Hub CSPM dei controlli in AWS Trusted Advisor](#).

Nuovi controlli per Amazon EC2 e Well-Architected AWS

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 per l'Amazon OpenSearch Service Reserved Instance Optimization assegnato 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 CloudWatch allarmi Amazon 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	dH7RR016J3
Archiviazione di volumi SSD (io2) IOPS con provisioning EBS	Limiti del servizio	gI7MM017J2

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	aW9HH018J6

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 di Amazon, vengono aggiornati anche i nomi delle metriche per questi cinque controlli. Per ulteriori informazioni, consulta [Creazione di CloudWatch allarmi Amazon per monitorare i parametri AWS Trusted Advisor](#).

Nome di controllo	Categoria di controllo	ID di controllo	Metrica aggiornat 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	dH7RR016J9	Archiviazione di volumi SSD (gp2) a scopo generico (TiB)
Archiviazioni di volumi magnetici (standard) EBS	Limiti del servizio	cG7HH017J9	Archiviazione di volumi magnetici (standard) (TiB)

Nome di controllo	Categoria di controllo	ID di controllo	Metrica aggiornat a CloudWatch per ServiceLimit
Archiviazione di volumi SSD (io1) IOPS con provisioning EBS	Limiti del servizio	gI7MM017J9	Archiviazione (SSD) IOPS con provisioning (TiB)
Archiviazione di volumi HDD ottimizza ti per la velocità effettiva (st1) EBS	Limiti del servizio	wH7DD013J9	Archiviazione di volumi HDD ottimizza ti 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	V77i0L1Bqz
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	Wnwm9I15bG
Volumi EBS attivi	Limiti del servizio	fH7LL017J9

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	Performance	eW7HH017J9

Supporto AWS App in Slack

Puoi utilizzare l' Supporto AWS 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' Supporto AWS app per gestire rapidamente i casi di assistenza in Slack.

Usa l' Supporto AWS app per effettuare le seguenti operazioni:

- Creazione, aggiornamento, ricerca e risoluzione dei casi di supporto nei canali Slack
- Allegare file ai casi di supporto
- 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' Supporto AWS 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.
- È possibile creare una richiesta di assistenza per l'account e la fatturazione e il supporto tecnico.

Argomenti

- [Prerequisiti](#)
- [Autorizzazione di un workspace Slack](#)
- [Configurazione di un canale Slack](#)
- [Creazione di casi di supporto in un canale Slack](#)
- [Risposta ai casi di supporto in Slack](#)
- [Partecipa a una sessione di chat dal vivo con Supporto](#)
- [Ricerca di casi di supporto in Slack](#)

- [Risoluzione di un caso di supporto in Slack](#)
- [Riapertura di un caso di supporto in Slack](#)
- [Eliminazione di una configurazione di canale Slack dall'app Supporto AWS](#)
- [Eliminazione di una configurazione dell'area di lavoro Slack dall'app Supporto AWS](#)
- [Supporto AWS Comandi dell'app in Slack](#)
- [Visualizza le corrispondenze Supporto AWS dell'app nel AWS Support Center Console](#)
- [Creazione di Supporto AWS app nelle risorse Slack con AWS CloudFormation](#)

Prerequisiti

Devi soddisfare i seguenti requisiti per utilizzare l' Supporto AWS App in Slack:

- Hai un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations. Puoi trovare il tuo piano di supporto dalla AWS Support Center Console o dalla pagina [Piani di supporto](#). Per ulteriori informazioni, [consulta Confronta Supporto AWS](#) i piani.
- 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 Account AWS come utente o ruolo AWS Identity and Access Management (IAM) con le autorizzazioni richieste. Per ulteriori informazioni, consulta [Gestione dell'accesso al widget Supporto AWS dell'app](#).
- Dovrai creare un ruolo IAM con le autorizzazioni necessarie per eseguire operazioni al posto tuo. L' Supporto AWS app utilizza questo ruolo per effettuare chiamate API a diversi servizi. Per ulteriori informazioni, consulta [Gestione dell'accesso all' Supporto AWS app](#).

Argomenti

- [Gestione dell'accesso al widget Supporto AWS dell'app](#)
- [Gestione dell'accesso all' Supporto AWS app](#)

Gestione dell'accesso al widget Supporto AWS dell'app

Puoi allegare una policy AWS Identity and Access Management (IAM) per concedere a un utente IAM l'autorizzazione a configurare il widget Supporto AWS App nel 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 nel tuo Account AWS, ma non ti consigliamo di farlo. 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.

JSON

```
{
  "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' Supporto AWS app a Slack

L' Supporto AWS app include azioni soggette a solo 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' Supporto AWS App 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. Pertanto, queste azioni API non sono incluse nel AWS CLI e. AWS SDKs

Gestione dell'accesso all' Supporto AWS app

Dopo aver ottenuto le autorizzazioni per il widget dell' Supporto AWS app, devi anche creare un ruolo AWS Identity and Access Management (IAM). Questo ruolo esegue Servizi AWS per te azioni altrui, come l' Supporto AWS API 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 richiedi una chat dal vivo con un agente dell'assistenza e scegli un nuovo canale privato come preferenza per il canale di chat dal vivo, l' Supporto AWS App 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 tutti i nuovi canali Slack di chat dal vivo che l' Supporto AWS App crea per te.

Segui queste procedure per creare il ruolo e la policy IAM.

Argomenti

- [Utilizza una policy AWS gestita o crea una policy gestita dai clienti](#)
- [Creazione di un ruolo IAM](#)
- [Risoluzione dei problemi](#)

Utilizza una policy AWS gestita o crea una policy gestita dai clienti

Per concedere le autorizzazioni di ruolo, puoi utilizzare una politica AWS gestita o una politica 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 politiche gestite dispongono automaticamente delle autorizzazioni necessarie per l' Supporto AWS App. Non è necessario aggiornare le policy manualmente. Per ulteriori informazioni, consulta [AWS politiche gestite per Supporto AWS 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.

Per creare una politica gestita dal cliente per l'App Supporto AWS

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli Policy.
3. Scegli Create Policy (Crea policy).
4. Scegliere la scheda JSON.
5. 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. Scegli Prossimo: Rivedi.
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 consente al ruolo di disporre delle autorizzazioni complete per tutte le azioni richieste per l' Supporto AWS App. Dopo aver configurato un canale Slack con il ruolo, qualsiasi utente del tuo canale dispone delle stesse autorizzazioni.

Note

Per un elenco delle politiche AWS gestite, vedere [AWS politiche gestite per Supporto AWS App in Slack](#).

Puoi aggiornare la politica per rimuovere un'autorizzazione dall' Supporto AWS App.

JSON

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

```

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 Supporto AWS](#)
- [Operazioni, risorse e chiavi di condizione per Service Quotas](#)
- [Azioni, 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.

Per creare un ruolo per l' Supporto AWS app

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
3. In Select trusted entity (Seleziona entità attendibile), scegli Servizio AWS.
4. Seleziona l'app Supporto AWS .
5. Scegli Successivo: autorizzazioni.
6. Inserisci il nome della policy. Puoi scegliere la policy AWS gestita o scegliere 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. Scegli Prossimo: Rivedi.
10. In Role name (Nome ruolo), digita un nome, come *AWSSupportAppRole*.
11. (Facoltativo) In Descrizione del ruolo, immetti 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, consulta [Configurazione di un canale Slack](#).

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

Risoluzione dei problemi

Consulta i seguenti argomenti per gestire l'accesso all' Supporto AWS app.

Indice

- [Desidero limitare determinate operazioni a utenti specifici del mio canale Slack](#)
- [Quando configuro un canale Slack, non vedo il ruolo IAM che ho creato](#)
- [Al mio ruolo IAM manca un'autorizzazione](#)
- [Un errore di Slack segnala che il mio ruolo IAM non è valido](#)
- [L' Supporto AWS app dice che mi manca un ruolo IAM per Service Quotas](#)

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 nel canale ha accesso in lettura o scrittura ai tuoi casi di supporto, indipendentemente dal fatto che abbia Account AWS o meno un utente IAM.

È preferibile seguire le best practice seguenti:

- Configura i canali Slack privati con l'app Supporto AWS
- 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 Supporto AWS . Per informazioni, consulta [AWS politiche gestite per Supporto AWS 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 del ruolo IAM per l' Supporto AWS app, significa che il ruolo non ha l' Supporto AWS App come entità attendibile o che il ruolo è stato eliminato. Puoi aggiornare il ruolo esistente oppure crearne un altro. Per informazioni, consulta [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' Supporto AWS App assume questo ruolo per eseguire queste azioni per te.

Se ricevi un errore relativo a un'autorizzazione mancante dall' Supporto AWS App, verifica che la politica allegata 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 alla pagina AWS Support Center Console all'indirizzo <https://console.aws.amazon.com/support/app#/config>.
2. Scegli il canale che hai configurato con l'App. Supporto AWS
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' Supporto AWS app dice che mi manca 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. Quindi,

puoi utilizzare l' Supporto AWS app 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](#) consente all' Supporto AWS App di creare il ruolo Service Quotas per te.

```
{
  "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 consentire all' Supporto AWS App di crearne uno per te.

Autorizzazione di un workspace Slack

Dopo aver autorizzato il tuo spazio di lavoro e dato all' Supporto AWS App il permesso di accedervi, avrai bisogno di un ruolo AWS Identity and Access Management (IAM) per te. Account AWS L' Supporto AWS App utilizza questo ruolo per richiamare le operazioni API [Supporto AWS](#) e [Service Quotas](#) per te. Ad esempio, l' Supporto AWS App utilizza il ruolo per chiamare l'CreateCaseoperazione per creare una richiesta di supporto per te in Slack.

Note

- Il tuo canale Slack eredita le autorizzazioni dal ruolo IAM. Tutti gli utenti del canale Slack dispongono delle stesse autorizzazioni specificate nella policy IAM allegata al ruolo. Ad esempio, se la tua policy IAM concede autorizzazioni complete di lettura e scrittura ai tuoi casi di supporto, chiunque nel tuo canale Slack può creare, aggiornare e risolvere i tuoi casi di supporto. Se la tua policy IAM consente autorizzazioni di sola lettura per il ruolo, gli utenti del tuo canale Slack possono solo visualizzare 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 ne hai più di uno Account AWS, devi accedere a ciascun account e ripetere la procedura seguente per autorizzare l'area di lavoro. Se il tuo account appartiene a un'organizzazione in AWS Organizations e desideri autorizzare più account, vai a [Autorizzazione di più account](#).

Per autorizzare l'area di lavoro 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. Quando Supporto AWS si richiede l'autorizzazione per accedere alla pagina your-workspace-name Slack, scegli Consenti.

Note

Se non riesci a consentire a Slack di accedere al tuo spazio di lavoro, assicurati di disporre delle autorizzazioni dell'amministratore Slack per aggiungere l'app all'area di lavoro. Supporto AWS Per informazioni, consulta [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 tuo numero Account AWS ID 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' Supporto AWS app utilizza questo nome per identificare il tuo account nel canale Slack. Puoi aggiornare questo nome in qualsiasi momento.

Edit account name

Choose an account name that you can easily recognize in Slack. This name won't appear in your AWS account settings.

Account name

Maximum 30 characters (5 remaining)

Example Usage:

Account name being used by Support Slack App Bot

- **AWS account:** aws-administrator-account (ID: 123456789012)

Cancel Save

Il nome del workspace e dell'account vengono visualizzati nella pagina Slack configuration (Configurazione di Slack).

Slack configuration

Workspaces

Delete Authorize workspace Add multiple accounts 

Workspace
troubleshooting

Account name

Delete Edit

Name used in Slack
aws-administrator-account

Autorizzazione di più account

Se il tuo account appartiene a un'organizzazione in AWS Organizations, puoi autorizzare più utenti Account AWS a utilizzare lo stesso spazio di lavoro Slack. Puoi utilizzare AWS CloudFormation modelli per automatizzare questo processo oppure configurare manualmente ogni account utilizzando l'API dell'app. Supporto AWS

Usa i modelli AWS CloudFormation

Puoi utilizzare [AWS CloudFormation](#) o [Terraform](#) per creare le risorse della tua Supporto AWS app su più account. Questo è l'approccio consigliato per la gestione di più account su larga scala.

Per ulteriori informazioni, consulta [Creazione di Supporto AWS app nelle risorse Slack con AWS CloudFormation](#).

Usa l'API Supporto AWS dell'app

Se preferisci non utilizzare i AWS CloudFormation modelli, puoi autorizzare manualmente più account utilizzando l'API dell' Supporto AWS app. Completa i seguenti passaggi per ogni account membro che desideri aggiungere all'area di lavoro di Slack.

Per autorizzare manualmente più account

1. Nell'account di gestione (l'account in cui hai creato l'area di lavoro Slack), autorizza l'area di lavoro Slack. Per ulteriori informazioni, consulta la procedura in. [Autorizzazione di un workspace Slack](#)
2. In ogni account membro, chiama l'operazione [RegisterSlackWorkspaceForOrganization](#) API per registrare l'area di lavoro Slack per quell'account.

Questa operazione aggiunge l'account membro all'area di lavoro Slack che è stata autorizzata dall'account di gestione.

3. In ogni account membro, crea un ruolo IAM con le autorizzazioni richieste per l'App. Supporto AWS Per ulteriori informazioni, consulta [Gestione dell'accesso all' Supporto AWS app](#).
4. In ogni account membro, richiama l'operazione [CreateSlackChannelConfiguration](#) API per configurare un canale Slack per quell'account.

Questa operazione associa il canale Slack all'account membro e specifica il ruolo IAM utilizzato dall' Supporto AWS App per chiamare e le operazioni di Service Supporto AWS Quotas.

 Note

Ogni account membro deve far parte della stessa organizzazione dell'account di gestione che ha autorizzato l'area di lavoro Slack. AWS Organizations

Configurazione di un canale Slack

Dopo aver autorizzato il tuo workspace Slack, puoi configurare i tuoi canali Slack affinché utilizzino l'app Supporto AWS .

Nel canale in cui inviti e aggiungi l' Supporto AWS app, puoi creare e cercare casi e ricevere notifiche sui casi. Questo canale mostra gli aggiornamenti dei casi, inclusi i casi appena creati o risolti, la corrispondenza aggiunta e i dettagli condivisi dei casi.

Il tuo canale Slack eredita le autorizzazioni dal ruolo IAM. Tutti gli utenti del canale Slack dispongono delle stesse autorizzazioni specificate nella policy IAM allegata al ruolo. Ad esempio, se la tua policy IAM concede autorizzazioni complete di lettura e scrittura per i tuoi casi di supporto, chiunque nel tuo canale Slack può creare, aggiornare e risolvere i tuoi casi di supporto. Se la tua policy IAM consente autorizzazioni di sola lettura per il ruolo, gli utenti del tuo canale Slack possono solo visualizzare i tuoi casi di supporto.

Puoi aggiungere fino a 20 canali per. Account AWS Ogni canale Slack supporta fino a 100 Account AWS. Ciò significa che solo 100 account possono aggiungere lo stesso canale Slack all'app Supporto AWS . Per ridurre al minimo le distrazioni, ti consigliamo di aggiungere solo gli account necessari per gestire i casi di supporto della tua organizzazione.

Ciascuno Account AWS deve configurare un canale Slack separatamente nell' Supporto AWS app. In questo modo, l' Supporto AWS App può accedere ai relativi casi di assistenza. Account AWS Se un altro Account AWS membro della tua organizzazione ha già invitato l' Supporto AWS app a quel canale Slack, vai al passaggio 3.

 Note

Puoi configurare i canali che fanno parte di [Slack Connect](#) e i canali condivisi con più workspace. Tuttavia, solo la prima area di lavoro che ha configurato il canale condiviso per un uomo Account AWS può utilizzare l'app. Supporto AWS L' Supporto AWS App restituisce

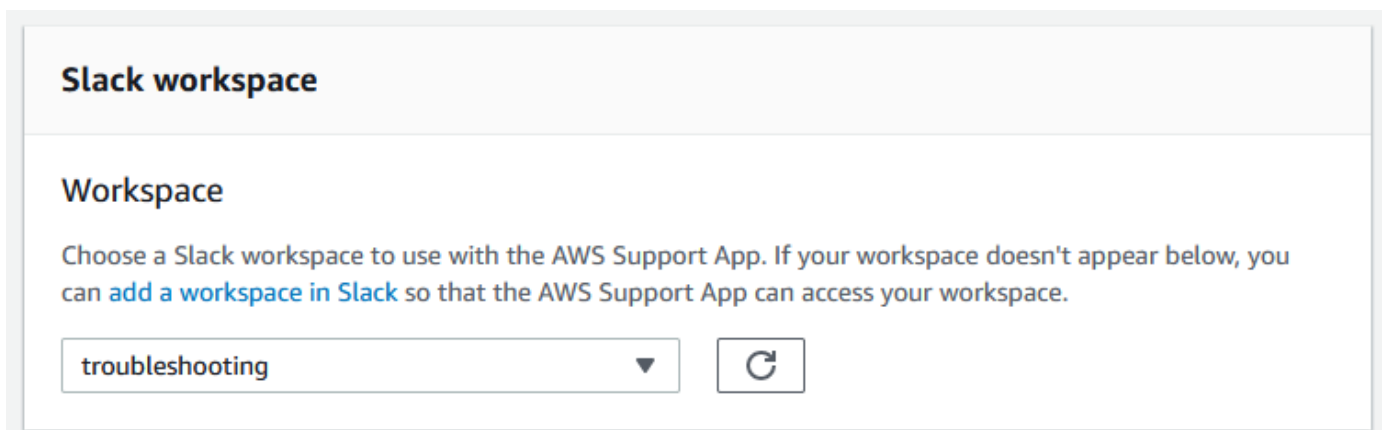
un messaggio di errore se provi a configurare lo stesso canale Slack per un altro spazio di lavoro.

Come configurare un canale Slack

1. Dalla tua applicazione Slack, scegli il canale Slack che desideri utilizzare con l'app. Supporto AWS
2. Completa i seguenti passaggi per invitare l' Supporto AWS app sul tuo canale:
 - a. Apri il menu contestuale (fai clic con il pulsante destro del mouse) sul nome del canale, quindi scegli Visualizza i dettagli del canale.
 - b. Scegli la scheda Integrazioni, quindi scegli Aggiungi un'app.
 - c. Per cercare l'app, inserisci Supporto AWS App.
 - d. Scegli Add (Aggiungi) accanto ad Supporto AWS 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 Supporto AWS (passaggio 2). Se il tuo canale non compare nell'elenco, scegli l'icona di aggiornamento e riprova.
 - Privato: in ID canale, inserisci l'ID o l'URL del canale Slack a cui hai invitato l' Supporto AWS app.

 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 tuo canale è il valore che appare **C01234A5BCD**.

7. In Nome di configurazione del canale, inserisci un nome che identifichi facilmente la configurazione del tuo canale Slack per l' Supporto AWS app. Questo nome appare solo in Slack Account AWS e non appare in Slack. Puoi rinominare la configurazione del canale in un secondo momento.

Il tipo di canale Slack potrebbe essere simile al seguente esempio.

▼ Slack channel

Channel Type

- ☐ Public
Choose a public channel from the list.
- ☒ Private
A channel member must invite a user to join or view.

Channel ID

Channel configuration name

Choose a name that you can easily identify. You can change the name at any time.



Tip

Tip To find the channel ID, right-click your channel name in Slack, choose **Copy** and then choose **Copy link**. Your channel ID is the value that looks like **C01234A5BCD**.

8. In Autorizzazioni, per il ruolo IAM per l' Supporto AWS app in Slack, scegli un ruolo che hai creato per l'app. Supporto AWS Nell'elenco vengono visualizzati solo i ruoli che hanno Supporto AWS l'App come entità attendibile.

▼ Permissions

IAM role for the AWS Support App

Choosing another IAM role for this Slack channel configuration can affect the permissions for any chat channels created from this troubleshooting channel. You can verify that your role has the required permissions. [Learn more](#)



 Note

Se non hai creato un ruolo o non lo vedi nell'elenco, consulta la pagina [Gestione dell'accesso all' Supporto AWS app](#).

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 iniziale dei casi di assistenza](#).
 - 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.

▼ Notifications

Additional case notifications
Choose when to get notified for cases created and updated.

☒ All cases

☐ High-severity cases

☐ None

Notification types
Get notified for the following types of cases that are created.

☒ New and reopened cases

☒ Case correspondences

☒ Resolved cases

Note: You will receive notifications in your Slack channel for all case updates for this account.

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 **channelName** pagina, puoi eseguire le seguenti attività:
 - Scegli Rename (Rinomina) per aggiornare il nome della configurazione del canale. Questo nome appare solo in Slack Account AWS e non apparirà in Slack.
 - Scegli Elimina per eliminare la configurazione del canale dall' Supporto AWS app. Per informazioni, consulta [Eliminazione di una configurazione di canale Slack dall'app Supporto AWS](#).
 - 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, ad esempio come stai utilizzando un Servizio AWS e quali passaggi di risoluzione dei problemi hai provato.

aws **Create a support case**  

Step 1 of 3

You can create a case with AWS Support for technical and account-related issues.

AWS account

dev-ops-production (ID:123456789012) 

Subject

AWS resources issue

Description

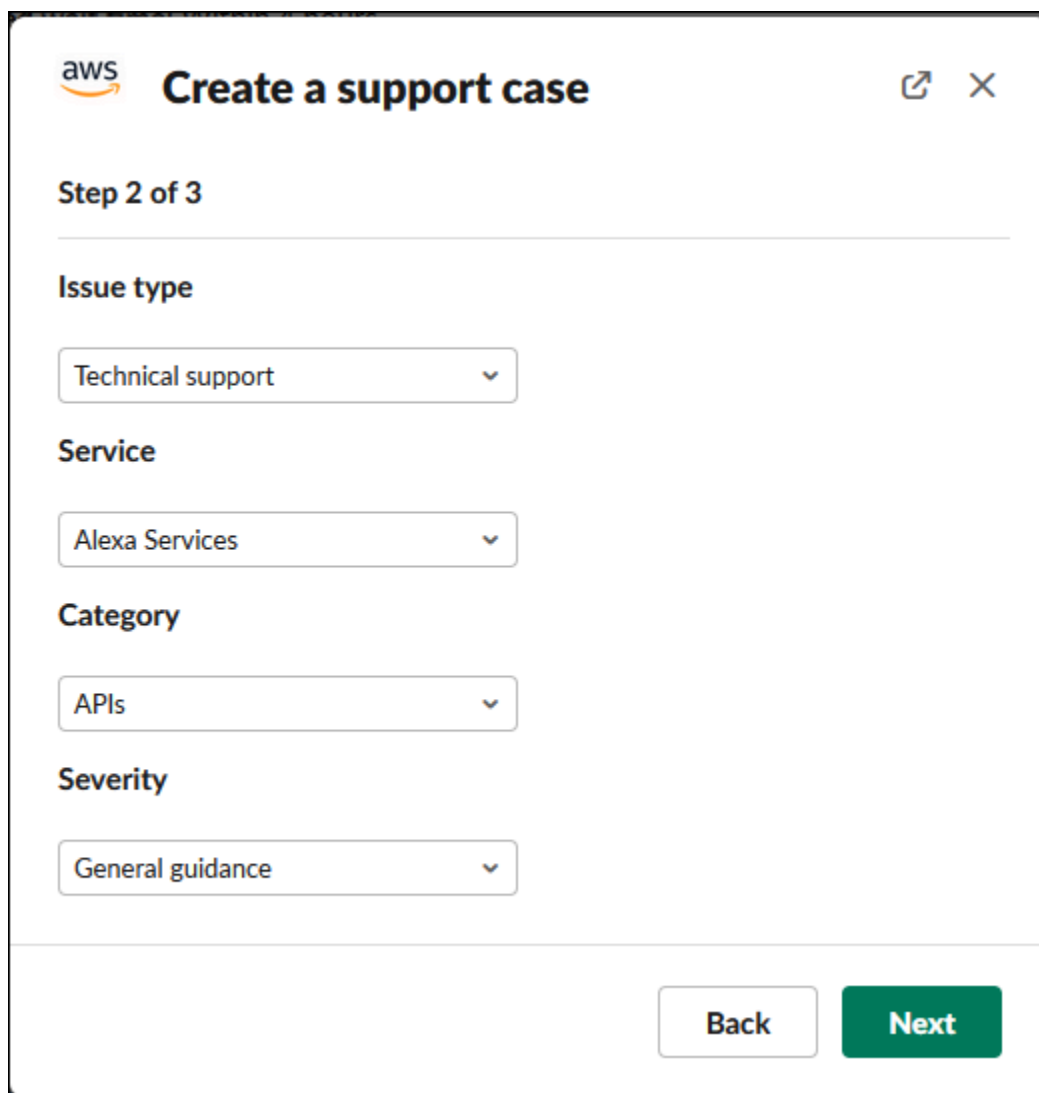
I can't find my resource in my AWS account. 2457 

Note: You can add attachments after step 3 when you confirm the case.

Cancel **Next**

3. Scegli Next (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 Alexa Servizi.



aws **Create a support case**

Step 2 of 3

Issue type

Technical support

Service

Alexa Services

Category

APIs

Severity

General guidance

Back Next

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.

 **Create a support case** ✕

Step 3 of 3

Contact language

English ▾

Contact method

☒ Live chat in Slack

☐ Email and Slack notifications

Live chat channel preference

New private channel ▾

 A new channel will be created for your live chat session, and anyone who is invited to the channel can see previous chat history.

Additional chat members (optional)

Add chat members

You will be added to the live chat automatically.

Back

Review

- 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' Supporto AWS agente, mentre il canale corrente utilizzerà un thread nel canale corrente per consentirti di chattare con l' Supporto AWS agente.
- b. (Facoltativo) Se scegli Live chat in Slack, puoi inserire i nomi degli altri membri di Slack. Per Nuovo canale privato, l' Supporto AWS app aggiungerà automaticamente te e i membri selezionati al nuovo canale. Per il canale corrente, l' Supporto AWS App taggherà automaticamente te e i membri selezionati nel thread della chat quando l' Supporto AWS agente 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 live chat per un caso di supporto esistente, l' Supporto AWS App utilizza lo stesso canale o thread di chat utilizzato per una precedente chat dal vivo. L' Supporto AWS App utilizza anche la stessa preferenza del 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. Scegli 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 modo seguente:
 - 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

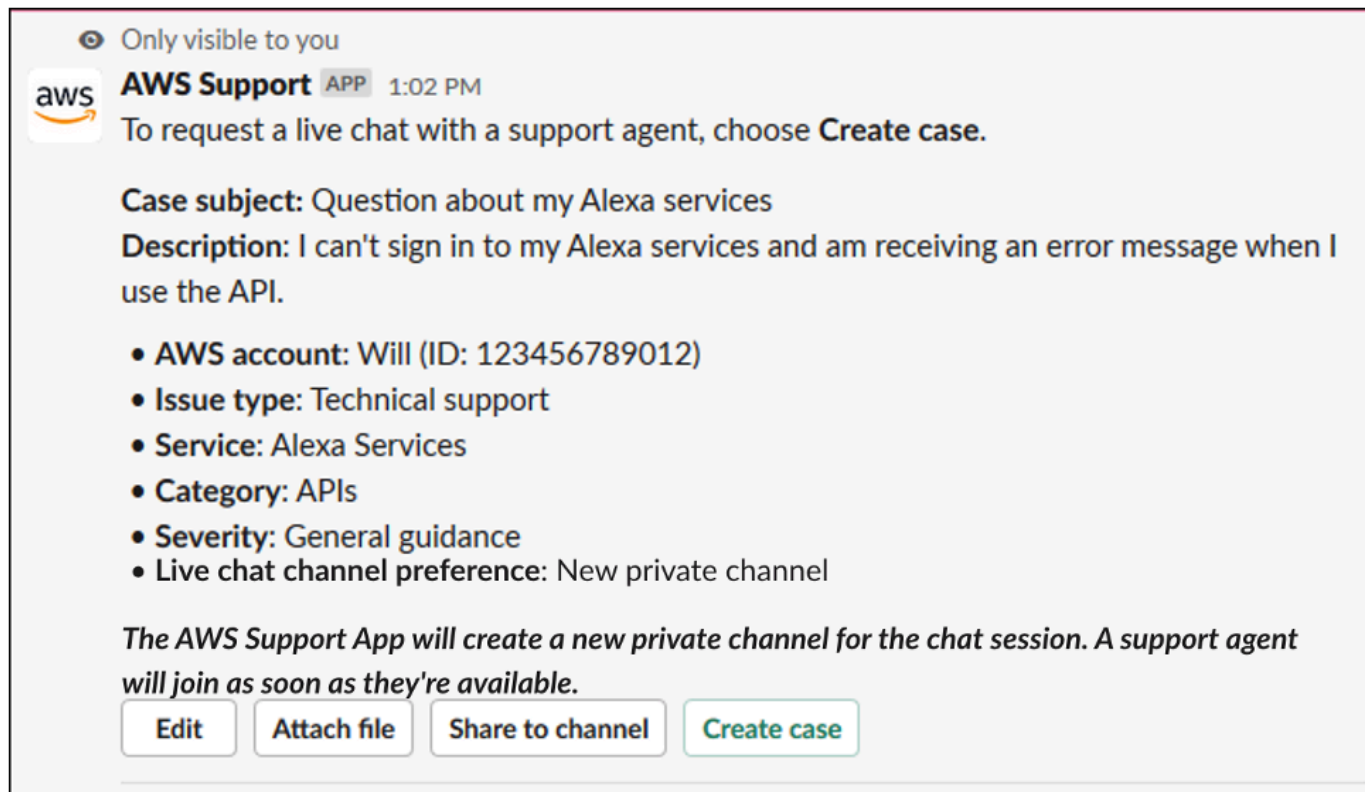
- Puoi allegare fino a tre file. Ogni file può essere fino a 5 MB.

- 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 Alexa Servizi.



The screenshot shows the AWS Support App interface within a Slack channel. At the top, it says "Only visible to you". Below that is the AWS Support App icon and name, followed by the time "1:02 PM". The main text says: "To request a live chat with a support agent, choose **Create case**." Below this, the case details are listed: "Case subject: Question about my Alexa services", "Description: I can't sign in to my Alexa services and am receiving an error message when I use the API.", and a bulleted list of details: "AWS account: Will (ID: 123456789012)", "Issue type: Technical support", "Service: Alexa Services", "Category: APIs", "Severity: General guidance", and "Live chat channel preference: New private channel". At the bottom, there is a note: "The AWS Support App will create a new private channel for the chat session. A support agent will join as soon as they're available." and four buttons: "Edit", "Attach file", "Share to channel", and "Create case".

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 l' AWS Support Center Console per rispondere agli agenti dell'assistenza. Per ulteriori informazioni, consulta [Esperienza precedente: aggiornamento, risoluzione e riapertura del caso](#).
- Non è possibile aggiungere corrispondenze ai casi dai canali di chat creati dall' Supporto AWS App. I canali di live chat inviano messaggi agli agenti solo durante la live chat.

Come rispondere a un caso di supporto in Slack

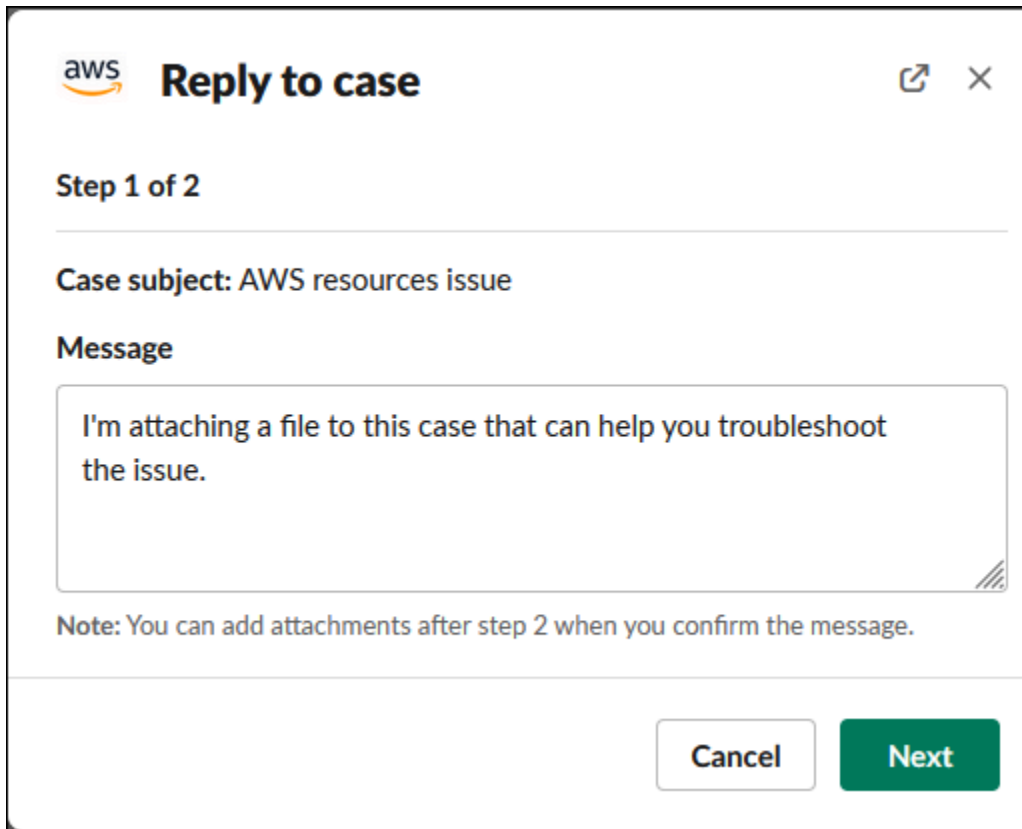
1. Nel tuo canale Slack, scegli il caso al quale desideri rispondere. Puoi inserire `/awssupport search` per trovare il caso di supporto.
2. Scegli See details (Vedi i dettagli) accanto al caso che ti interessa.
3. Nella parte inferiore dei dettagli del caso, scegli Reply (Rispondi).

Share to channel

Reply

Resolve case

4. Nella finestra di dialogo Reply to case (Rispondi al caso), inserisci una breve descrizione del problema nel campo Message (Messaggio). Quindi scegli Successivo.



The screenshot shows a dialog box titled "aws Reply to case" with a close button (X) and a share icon. It is labeled "Step 1 of 2". The "Case subject" is "AWS resources issue". The "Message" field contains the text: "I'm attaching a file to this case that can help you troubleshoot the issue." Below the message field is a note: "Note: You can add attachments after step 2 when you confirm the message." At the bottom right are "Cancel" and "Next" buttons.

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. Scegli 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

Only visible to you

 **AWS Support** APP 10:53 AM

To respond to this case, review and then choose **Send message**.

Case subject: AWS resources issue

Message: I'm attaching a file to this case that can help you troubleshoot the issue.

We will contact you by email and Slack notifications within 24 hours.

Additional contacts to notify: None

Attachments: error-log

✓ You successfully attached 1 file. Choose **Create case** within 1 hour to include the file with your case.

Partecipa a una sessione di chat dal vivo con Supporto

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' Supporto AWS 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.

ℹ 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' Supporto AWS App per rispondere a queste corrispondenze.

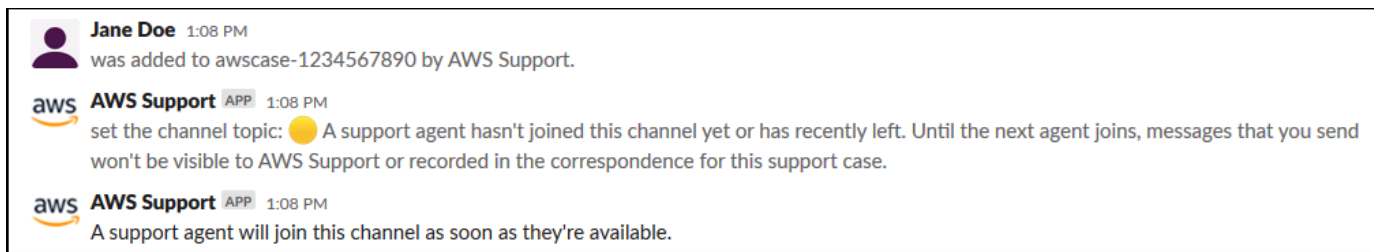
Per partecipare a una sessione di chat dal vivo Supporto in un nuovo canale

1. Nell'applicazione Slack, vai al canale che l' Supporto AWS App crea per te. Il nome del canale include l'ID del caso di assistenza, ad esempio **awscase-1234567890**.

Note

L' Supporto AWS 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.



The screenshot shows a Slack channel interface. At the top, a message from Jane Doe (1:08 PM) states: "was added to awscase-1234567890 by AWS Support." Below this, a message from the AWS Support App (1:08 PM) says: "set the channel topic: 🟡 A support agent hasn't joined this channel yet or has recently left. Until the next agent joins, messages that you send won't be visible to AWS Support or recorded in the correspondence for this support case." At the bottom, another message from the AWS Support App (1:08 PM) states: "A support agent will join this channel as soon as they're available."

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 Supporto AWS 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' Supporto AWS app salva automaticamente i file e il registro della chat nella corrispondenza relativa al caso.

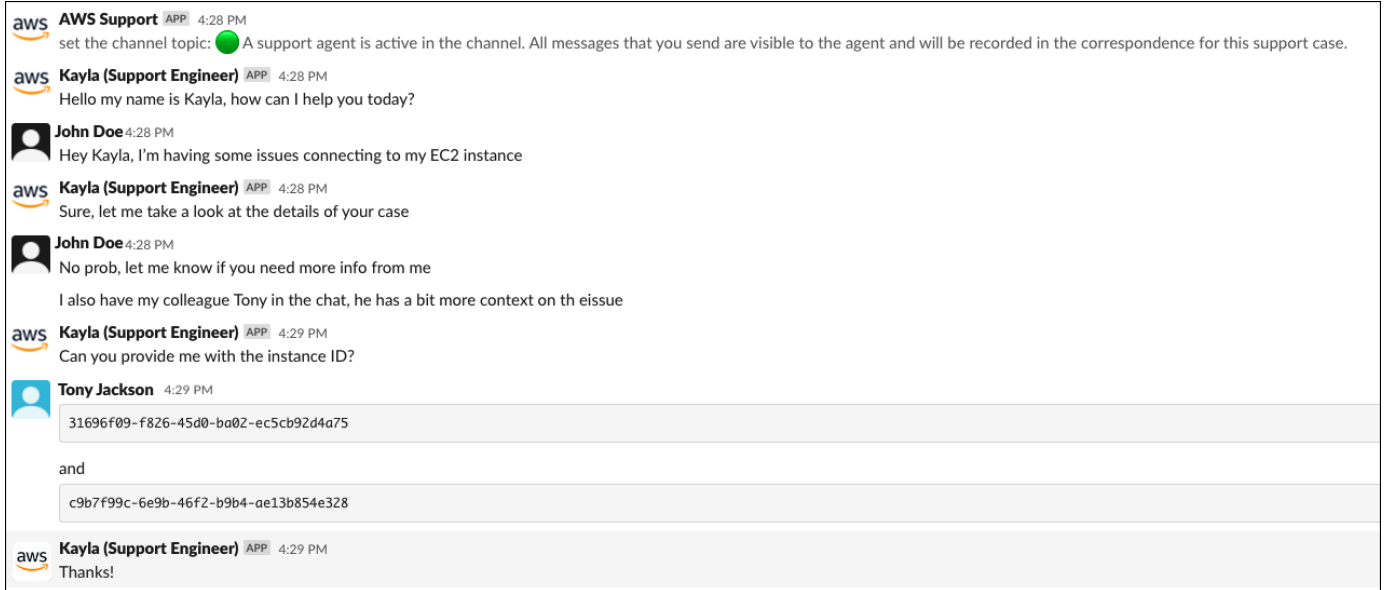
 Note

Quando chatti con un agente dell'assistenza, tieni presente le seguenti differenze in Slack per l' Supporto AWS 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 sessione di chat dal vivo con un agente di supporto per risolvere un problema di connettività per due istanze di Amazon Elastic Compute Cloud (Amazon EC2).



The screenshot shows a Slack chat window with the following messages:

- aws AWS Support** (APP) 4:28 PM: set the channel topic:  A support agent is active in the channel. All messages that you send are visible to the agent and will be recorded in the correspondence for this support case.
- aws Kayla (Support Engineer)** (APP) 4:28 PM: Hello my name is Kayla, how can I help you today?
- John Doe** 4:28 PM: Hey Kayla, I'm having some issues connecting to my EC2 instance
- aws Kayla (Support Engineer)** (APP) 4:28 PM: Sure, let me take a look at the details of your case
- John Doe** 4:28 PM: No prob, let me know if you need more info from me
I also have my colleague Tony in the chat, he has a bit more context on th eissue
- aws Kayla (Support Engineer)** (APP) 4:29 PM: Can you provide me with the instance ID?
- Tony Jackson** 4:29 PM:

31696f09-f826-45d0-ba02-ec5cb92d4a75

and

c9b7f99c-6e9b-46f2-b9b4-ae13b854e328
- aws Kayla (Support Engineer)** (APP) 4:29 PM: Thanks!

5. (Facoltativo) Per interrompere la live chat, scegli End chat (Termina la chat). L'agente di supporto lascia il canale e l' Supporto AWS 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 aggiunto mostra i dettagli del caso relativo a un' EC2 istanza Amazon. Puoi trovare i messaggi appuntati sotto il nome del canale Slack.

 Pinned by AWS Support

 **AWS Support** APP 2:33 PM

This is a live chat channel for the following case.

Case subject: Cannot connect to ec2 instance (Case ID: 6887208841)

Description: The ec2 instance i-09f00da444 was unable to lookup our dns region. We had full access yesterday. Now we get "Access denied" message.

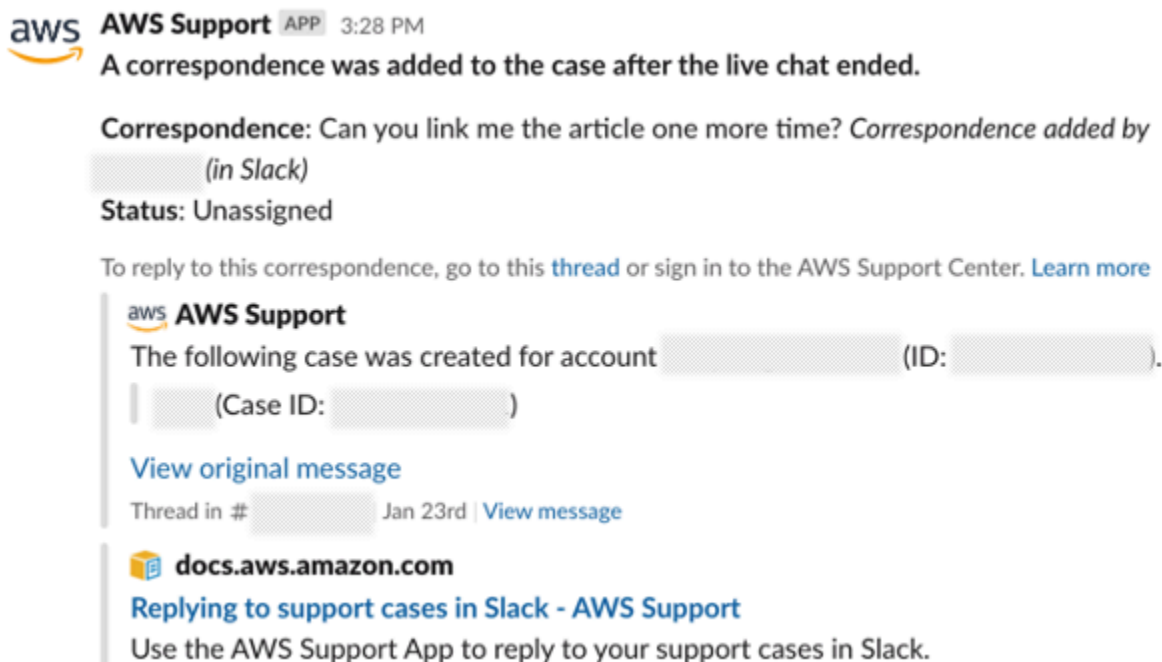
Case created by Jane Doe (in Slack)

- **Status:** Unassigned
- **Created:** 02/16/2021, 2:33PM PST
- **AWS account:** Instance Management (ID: 111122223333)
- **Issue type:** Technical support
- **Service:** Elastic Compute Cloud (EC2-Linux)
- **Category:** SSH Issue
- **Severity:** Production system impaired

End chat Resolve case

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 Supporto utilizzando il canale corrente

1. Nell'applicazione Slack, vai al thread nel canale corrente che l' Supporto AWS 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 Supporto, anche quando una chat è attiva.

Thread aws-support-communications**AWS Support** APP < 1 minute ago

The following case was created for account [REDACTED].

Question about my Alexa services (Case ID: [REDACTED])



A support agent hasn't joined this chat session yet or has recently left

Get updates

See details

End chat

Reply

Resolve case

7 replies

**AWS Support** APP < 1 minute ago

@Jane Doe requested a chat for this case.

Question about my Alexa services (Case ID: [REDACTED])

**AWS Support** APP < 1 minute ago

A support agent will join this chat session as soon as they're available.

**Tip:** Editing and deleting messages is not supported during the chat session. Support agents will still see original messages.

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.

Thread  aws-support-communications

 **AWS Support** APP < 1 minute ago

The following case was created for account [REDACTED].

Question about my Alexa services (Case ID: [REDACTED])

 A support agent hasn't joined this chat session yet or has recently left

[Get updates](#) [See details](#) [End chat](#) [Reply](#) [Resolve case](#)

7 replies

Ricerca di casi di supporto in Slack

Dal tuo canale Slack, puoi cercare casi di assistenza relativi al tuo account Account AWS e ad altri account che hanno configurato lo stesso canale e lo stesso spazio di lavoro. Ad esempio, se il tuo account (123456789012) e l'account del tuo collega (111122223333) hanno configurato lo stesso spazio di lavoro e gli stessi canali in AWS Support Center Console, puoi utilizzare l'App per cercare i Supporto AWS reciproci casi di assistenza.

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.

👁 Only visible to you

 **AWS Support** APP 1:07 PM

Search for cases created by account **aws-administrator-account** (ID: 123456789012).

I want to search for cases by:

☒ Filter options

☐ Case ID

Date range:

 10/01/2022 

 Today 

Case status:

All cases 

Case created in:

English 

Search

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 hai più account nel canale, scegli per cercare il caso. Account AWS
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.

 Only visible to you

 **AWS Support** APP 1:51 PM

3 results found for cases created from 10/01/2022 to 12/28/2022 with AWS account aws-administrator-account (ID:123456789012).

Case subject: Can't retrieve info about my certificate (Case ID: 1234567890)

Created: 10/25/2022, 10:30 PM UTC

Status: Resolved

[See details](#)

Case subject: Question about my AWS account bill (Case ID: 4445556660)

Created: 10/14/2022, 7:35 PM UTC

Status: Resolved

[See details](#)

Case subject: Technical support for EC2 instances (Case ID: 9087654321)

Created: 10/13/2022, 2:28 PM UTC

Status: In progress

[See details](#)

[Edit Search](#) [Share to channel](#)

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).

 Only visible to you

This case was created on 10/14/2022, 10:30 PM UTC.

Case subject: Question about my AWS account bill (Case ID: 4445556660)

Description: I have a question about a charge for my last statement

- **Status:** Resolved
- **AWS account:** aws-administrator-account (ID: 123456789012)
- **Issue type:** Account and billing support
- **Service:** Academy
- **Category:** Account/Lab access issue
- **Severity:** General question
- **Language:** English

Correspondence:

Amazon Web Services, 10/25/2022, 10:30 PM UTC

This case has been resolved. Please contact us again if you need further assistance.

[Share to channel](#)

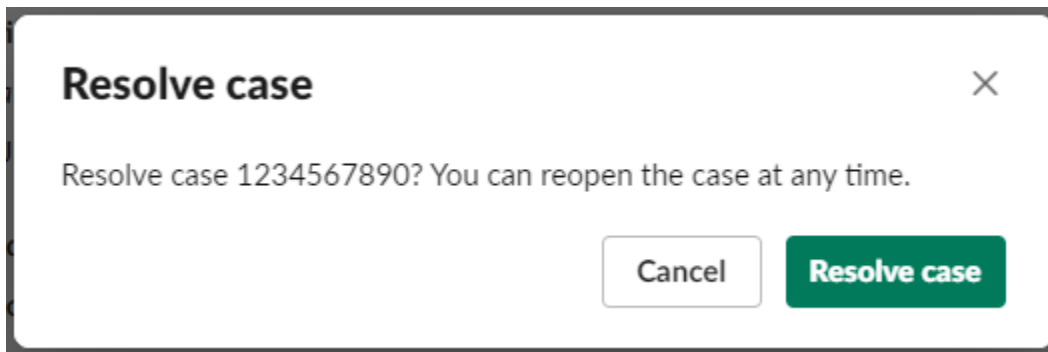
[Reopen case](#)

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, consulta [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.

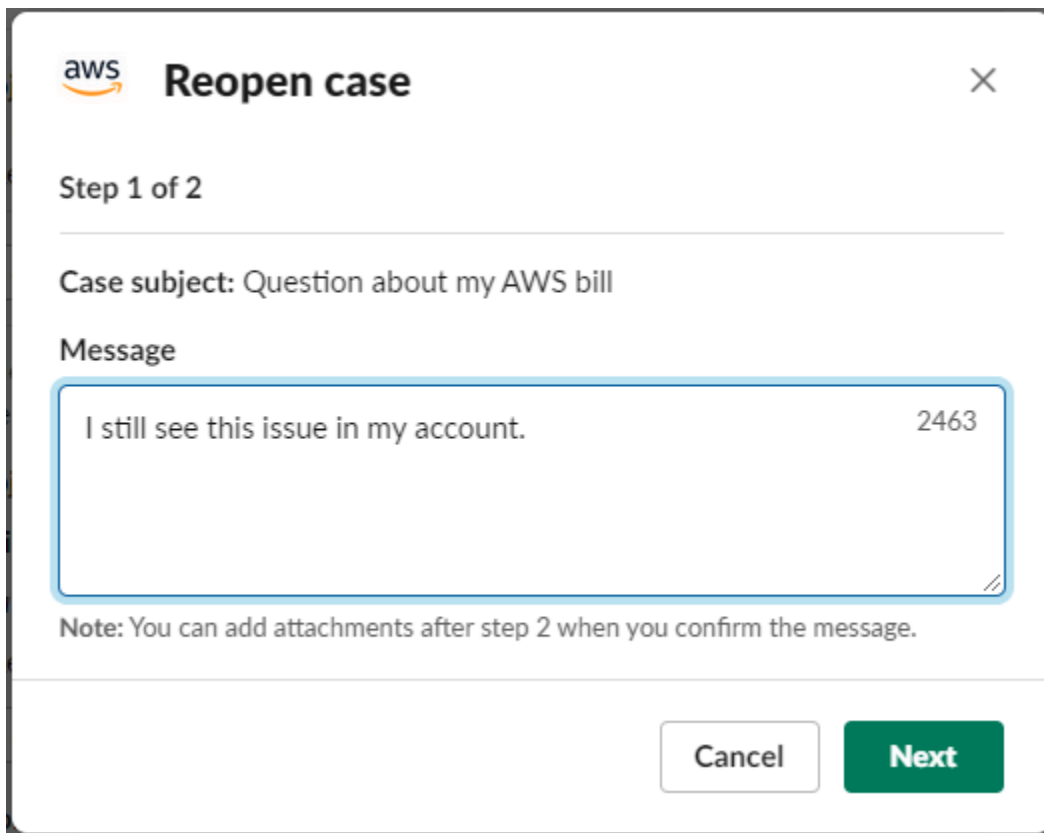


Riapertura di un caso di supporto in Slack

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, consulta [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. Scegli Next (Successivo).



aws **Reopen case** X

Step 1 of 2

Case subject: Question about my AWS bill

Message

I still see this issue in my account. 2463

Note: You can add attachments after step 2 when you confirm the message.

Cancel Next

6. (Facoltativo) Inserisci contatti aggiuntivi.
7. Scegli 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.

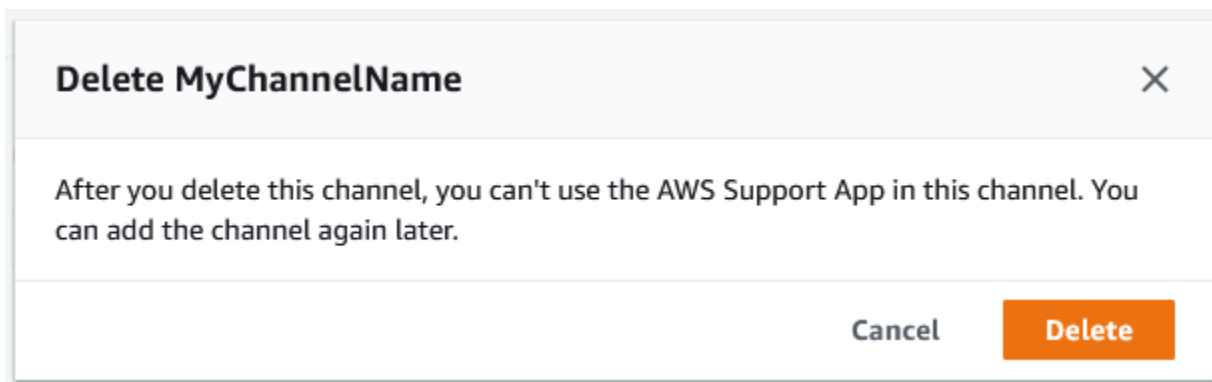
Eliminazione di una configurazione di canale Slack dall'app Supporto AWS

Puoi eliminare la configurazione di un canale dall' Supporto AWS app se non ne hai bisogno. Questa azione rimuove solo il canale dall' Supporto AWS App e dal 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). Puoi aggiungere nuovamente questo canale all' Supporto AWS App in un secondo momento.



Eliminazione di una configurazione dell'area di lavoro Slack dall'app Supporto AWS

Puoi eliminare una configurazione dell'area di lavoro dall' Supporto AWS App se non ne hai bisogno. Questa azione rimuove solo l'area di lavoro dall' Supporto AWS App e dal. 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.

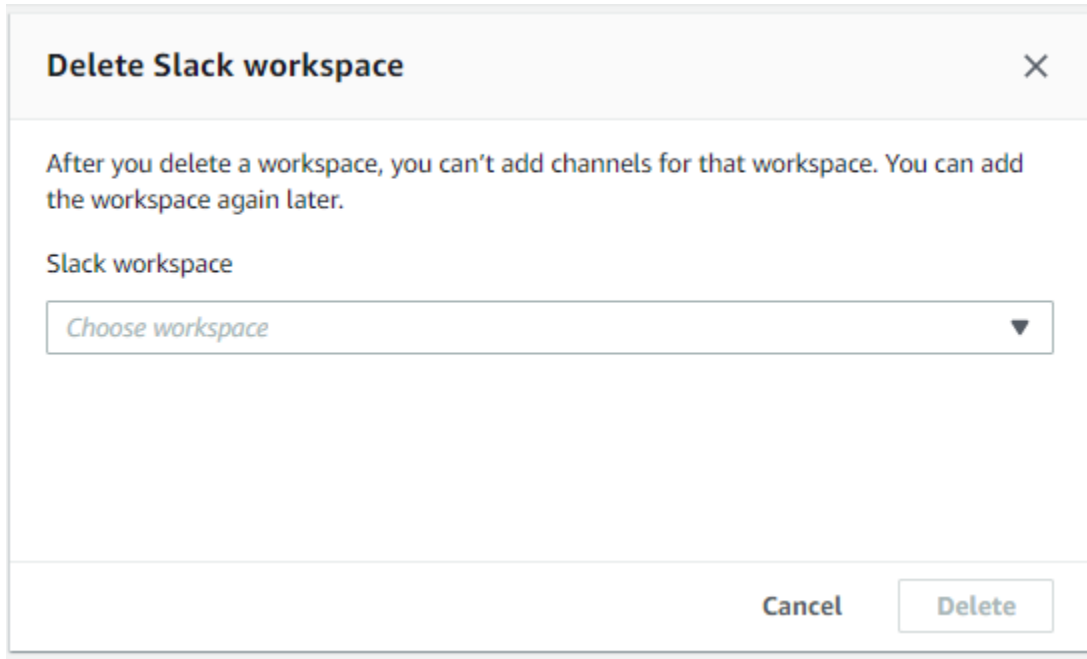
Note

Se hai aggiunto canali da questo spazio di lavoro all' Supporto AWS App, devi prima eliminare questi canali prima di poter eliminare l'area di lavoro. Per informazioni, consulta [Eliminazione di una configurazione di canale Slack dall'app Supporto AWS](#).

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 l'area di lavoro al tuo Account AWS in un secondo momento.



Supporto AWS Comandi dell'app in Slack

Comandi del canale Slack

Puoi inserire i seguenti comandi nel canale Slack al quale hai invitato l'app Supporto AWS . 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 assistenza per chi Account AWS ha configurato l' Supporto AWS app 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 l' Supporto AWS App crea per te se scegli un nuovo canale con Supporto cui chattare. I canali di chat includono l'ID del caso di assistenza, ad esempio *aws-case-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.

Visualizza le corrispondenze Supporto AWS dell'app nel 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.

Correspondence	
MyIAMRole (Role) Thu Feb 24 2022 09:09:33 GMT-0800 (Pacific Standard Time)	I am having difficulty retrieving information about my certificates. _Case created by JaneDoe (in Slack)_

Creazione di Supporto AWS app nelle risorse Slack con AWS CloudFormation

Supporto AWS App in Slack è integrata con AWS CloudFormation un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da poter dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come le tue AccountAlias e SlackChannelConfiguration) e fornisce e CloudFormation configura tali risorse per te.

Quando lo utilizzi CloudFormation, puoi riutilizzare il modello per configurare le risorse Supporto AWS dell'app in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS aree geografiche.

Supporto AWS App e CloudFormation modelli

Per fornire e configurare le risorse per Supporto AWS l'App e i servizi correlati, è necessario comprendere [CloudFormation i modelli](#). I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri fornire nei tuoi CloudFormation stack. Se non conosci JSON o YAML, puoi usare CloudFormation Designer per iniziare a usare i modelli.

CloudFormation [Per ulteriori informazioni, consulta Cos'è Designer? CloudFormation](#) nella Guida AWS CloudFormation per l'utente.

Supporto AWS L'app supporta la creazione di file AccountAlias e SlackChannelConfiguration in CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per SlackChannelConfiguration le risorse AccountAlias and, consulta il [riferimento al tipo di risorsa dell'Supporto AWS app](#) nella Guida per l'AWS CloudFormation utente.

Creazione di risorse di configurazione Slack per la tua organizzazione

Puoi utilizzare CloudFormation i modelli per creare le risorse necessarie per l'App. Supporto AWS 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 dell'area di lavoro Slack per tutti gli account dell'organizzazione, ma poi utilizzare modelli separati per creare diverse configurazioni del canale Slack per unità specifiche Account AWS o organizzative (). OUs 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 CloudFormation i modelli o meno. Se scegli di non utilizzare i modelli CloudFormation , completa manualmente i seguenti passaggi:

- Crea le risorse Supporto AWS dell'app in AWS Support Center Console.
- Effettua una chiamata all'operazione API [RegisterSlackWorkspaceForOrganization](#) per registrare un workspace di Slack per il tuo account. Lo CloudFormation stack chiama questa operazione API per te.
- Crea un ruolo IAM con le autorizzazioni richieste per ogni account membro.
- Chiama l'operazione [CreateSlackChannelConfiguration](#)API per configurare un canale Slack per ogni account membro.

Per i passaggi manuali dettagliati, consulta [Autorizzazione di più account](#).

Segui queste procedure per caricare il CloudFormation modello nella tua organizzazione. Puoi usare i modelli di esempio inclusi nella pagina [Documentazione di riferimento sul tipo di risorsa dell'app Supporto AWS](#).

I modelli indicano CloudFormation di creare le seguenti risorse:

- Una [configurazione del canale Slack](#).
- Una [configurazione del workspace di Slack](#).
- Un [ruolo IAM](#) denominato `AWSSupportSlackAppCFNRole`. La politica `AWSSupportAppFullAccess` AWS gestita è allegata.

Indice

- [Aggiorna i tuoi CloudFormation modelli per Slack](#)
- [Creazione di uno stack per l'account di gestione](#)
- [Creazione di un set di stack per l'organizzazione](#)

Aggiorna i tuoi CloudFormation modelli 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 AccountAlias risorsa identifica in modo univoco un utente Account AWS nell'App. Supporto AWS I tuoi account membri possono immettere un nome account nella console del Centro assistenza. Per ulteriori informazioni, consulta [Autorizzazione di un workspace Slack](#).

Per aggiornare i CloudFormation modelli per Slack

1. Se sei l'account di gestione di un'organizzazione, devi autorizzare manualmente un'area di lavoro Slack per il tuo account prima che gli account dei membri possano essere utilizzati per creare CloudFormation 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 Supporto AWS](#), 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 l'area di lavoro e il canale IDs, 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/T012ABCDEFGH/C01234A5BCD`, T012ABCDEFGH 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 utilizzare l'app. Supporto AWS

Come creare uno stack per l'account di gestione

1. Accedi Console di gestione AWS come account di gestione della tua organizzazione.
2. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Se non l'hai già fatto, nel selettore della regione, scegli una delle seguenti opzioni: Regioni AWS
 - 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 CloudFormation](#).

Dopo aver creato CloudFormation correttamente lo stack, 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 quello OUs che desideri. 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 a Console di gestione AWS come account di gestione della tua organizzazione.
2. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Se non l'hai già fatto, nel selettore Regione, scegli la stessa Regione AWS che hai usato nella procedura precedente.
4. Nel pannello di navigazione, scegli StackSets.
5. Scegli Create StackSet (Crea).
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 Specificare StackSet i dettagli, inserite un nome per lo stack **support-app-slack-workspace**, ad esempio, immettete una descrizione, quindi scegliete Avanti.
 10. Nella pagina Configura StackSet opzioni, mantieni le opzioni predefinite, quindi scegli 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. Per gli obiettivi di distribuzione, scegli se desideri creare lo stack per l'intera organizzazione o per uno specifico OUs. Se scegli un'unità organizzativa, inserisci l'ID UO.
 13. Per Specificare le regioni, inserisci solo una delle seguenti opzioni: Regioni AWS
 - 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 lo stesso Regione AWS che hai scelto nel passaggio 3.
- La scelta di più di uno Regione AWS può causare conflitti con la creazione dello stack.

14. Per Opzioni di distribuzione, per Tolleranza agli errori: facoltativo, inserisci il numero di account in cui gli stack possono fallire prima che l'operazione venga CloudFormation interrotta. 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. Ciò significa che anche se l'operazione CloudFormation fallisce 9 volte, almeno un account avrà successo.

15. Scegli Next (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 allega una policy AWS gestita. Questo ruolo dispone delle autorizzazioni necessarie per accedere ad altri servizi per conto tuo. Per ulteriori informazioni, consulta [Gestione dell'accesso all' Supporto AWS app](#).

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 aver CloudFormation creato gli stack, ogni account membro può accedere alla console del Support Center e trovare le aree di lavoro e i canali Slack configurati. Possono quindi utilizzare l' Supporto AWS App per i loro. Account AWS Per informazioni, consulta [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.

Scopri di più su CloudFormation

Per ulteriori informazioni CloudFormation, consulta le seguenti risorse:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guida per l'utente](#)
- [CloudFormation Documentazione di riferimento delle API](#)
- [AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando](#)

Crea risorse Supporto AWS per app utilizzando Terraform

Puoi anche usare [Terraform](#) per creare le risorse dell' Supporto AWS app per te. Account AWS Terraform è uno infrastructure-as-code strumento che puoi utilizzare per le tue applicazioni cloud. Puoi utilizzare Terraform per creare risorse per Supporto AWS app invece di distribuire uno CloudFormation stack su un account.

Dopo aver installato Terraform, puoi specificare le risorse dell' Supporto AWS app che desideri. 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 degli CloudFormation stack set, non puoi utilizzare Terraform per creare le risorse dell' Supporto AWS app per un'unità organizzativa della 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 Supporto AWS dell'app nelle chiamate dell'API Slack utilizzando AWS CloudTrail](#).

Ulteriori informazioni

Per ulteriori informazioni su Terraform, consulta i seguenti argomenti:

- [Installazione di Terraform](#)
- [Tutorial Terraform: crea un'infrastruttura per AWS](#)
- [awscc_support_app_account_alias](#)
- [awscc_supportapp_slack_workspace_configuration](#)
- [awscc_supportapp_slack_channel_configuration](#)

Sicurezza in Supporto AWS

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 Supporto AWS, consulta la sezione [AWS Servizi rientranti nell'ambito del programma di conformità](#).
- **Sicurezza nel cloud:** la tua responsabilità è determinata da Servizio AWS ciò che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

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

Argomenti

- [Protezione dei dati in Supporto AWS](#)
- [Sicurezza per i tuoi casi Supporto AWS](#)
- [Gestione delle identità e degli accessi per Supporto AWS](#)
- [Risposta agli incidenti](#)
- [Registrazione e monitoraggio in Supporto AWS e AWS Trusted Advisor](#)
- [Convalida della conformità per Supporto AWS](#)
- [Resilienza in Supporto AWS](#)
- [Sicurezza dell'infrastruttura in Supporto AWS](#)
- [Analisi della configurazione e delle vulnerabilità in Supporto](#)

Protezione dei dati in Supporto AWS

Il [modello di responsabilità AWS condivisa](#) di si applica alla protezione dei dati in Supporto. 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 maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

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. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

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

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

vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

 Important

In caso di corrispondenza, non condividere mai informazioni sensibili, come credenziali, carte di credito, informazioni URLs firmate o di identificazione personale.

Sicurezza per i tuoi casi Supporto AWS

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:

- Supporto AWS 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: Supporto AWSAWS AWSSupport ServiceRolePolicy](#)
- Puoi visualizzare le chiamate API a quelle Supporto AWS 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 Supporto AWS API con AWS CloudTrail](#).
- Puoi usare l' API Supporto AWS 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. Puoi visualizzare i dettagli del caso fino a 24 mesi dopo la sua creazione. Per ulteriori informazioni, consulta [DescribeCases](#) nella documentazione di riferimento dell'API Supporto AWS .
- I casi di supporto seguono la [Convalida della conformità per Supporto AWS](#).
- 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. Supporto AWS 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 [Supporto AWS FAQs](#).

- Puoi modificare il tuo Supporto AWS piano per ottenere l'assistenza di cui hai bisogno per il tuo account. Per ulteriori informazioni, [consulta Confronto Supporto AWS dei piani](#) e [Modifica del Supporto AWS piano](#).

Gestione delle identità e degli accessi per Supporto AWS

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. Supporto IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come Supporto AWS funziona con IAM](#)
- [Supporto AWS esempi di politiche basate sull'identità](#)
- [Uso di ruoli collegati ai servizi](#)
- [AWS politiche gestite per Supporto AWS](#)
- [Gestisci l'accesso al Centro Supporto AWS](#)
- [Gestisci l'accesso ai piani Supporto AWS](#)
- [Gestisci l'accesso a AWS Trusted Advisor](#)
- [Esempi di politiche di controllo dei servizi per AWS Trusted Advisor](#)
- [Risoluzione dei problemi di Supporto AWS identità e accesso](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi di Supporto AWS identità e accesso](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come Supporto AWS funziona con IAM](#))

- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [Supporto AWS 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 autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

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

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

AWS account (utente root)

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

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida](#) per l'utente IAM.

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

Ruoli IAM

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

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

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

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

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

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Altri tipi di policy

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

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

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

Come Supporto AWS funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Supporto, è necessario comprendere con quali funzionalità IAM è disponibile l'uso Supporto. Per avere una visione di alto livello di come Supporto 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'uso di Supporto di IAM, consulta [Manage access for Supporto](#).

Argomenti

- [Supporto politiche basate sull'identità](#)
- [Supporto Ruoli IAM](#)

Supporto politiche basate sull'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. Supporto 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. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

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

Le azioni politiche Supporto 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`. Supporto definisce una propria serie di operazioni che descrivono le attività eseguibili 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 Supporto azioni, consulta [Actions Defined by Supporto AWS](#) nella IAM User Guide.

Esempi

Per visualizzare esempi di politiche Supporto basate sull'identità, consulta. [Supporto AWS esempi di politiche basate sull'identità](#)

Supporto Ruoli IAM

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

Utilizzo di credenziali temporanee con Supporto

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 [AssumeRole](#) o [GetFederationToken](#).

Supporto 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.

Supporto supporta ruoli collegati ai servizi. Per informazioni dettagliate sulla creazione o la gestione di ruoli Supporto collegati ai servizi, vedere [Utilizzo dei ruoli collegati ai servizi per Supporto AWS](#).

Ruoli dei servizi

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

Supporto supporta i ruoli di servizio.

Supporto AWS esempi di politiche basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse Supporto. Inoltre, non possono eseguire attività utilizzando l'API Console di gestione AWS 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](#)
- [Utilizzo della console Supporto](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

Best practice delle policy

Le policy basate su identità sono molto efficaci. Determinano se qualcuno può creare, accedere o eliminare Supporto risorse nel tuo account. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia a utilizzare le politiche AWS gestite: per iniziare a utilizzare Supporto 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, consulta [Elementi delle policy JSON di IAM: Condizioni](#) nella Guida per l'utente IAM.

Utilizzo della console Supporto

Per accedere alla Supporto AWS console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle Supporto 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 Supporto 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, è possibile 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 collegate 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

Supporto AWS 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. Supporto Trusted Advisor In ogni caso, il ruolo collegato ai servizi è un ruolo predefinito. Questo ruolo include tutte le autorizzazioni necessarie Supporto 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. Supporto Trusted Advisor

Argomenti

- [Utilizzo dei ruoli collegati ai servizi per Supporto AWS](#)
- [Utilizzo di ruoli collegati ai servizi per Trusted Advisor](#)

Utilizzo dei ruoli collegati ai servizi per Supporto AWS

Supporto AWS 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, Supporto 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. Supporto Questo ruolo collegato al servizio è predefinito e include le autorizzazioni necessarie per chiamare altri servizi per Supporto 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 Supporto accesso ai metadati delle risorse, non ai dati dei clienti. Solo Supporto 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 chiamata [GetExecutionHistory](#) per la chiamata AWS Step Functions API non sono visibili a Supporto. Usiamo AWS KMS keys per crittografare i campi sensibili. Questi campi sono oscurati nella risposta dell'API e non sono visibili agli Supporto AWS 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 Supporto AWS 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'utente Supporto. Per informazioni in merito CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#).

Autorizzazioni di ruolo collegate al servizio per Supporto

Questo ruolo utilizza la politica gestita. `AWSSupportServiceRolePolicy` AWS 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: Supporto 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 Supporto 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: Supporto 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

Supporto AWS 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 Supporto AWS](#).

Creazione di un ruolo collegato al servizio per Supporto

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 Supporto 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 Supporto

È possibile utilizzare IAM per modificare la descrizione del ruolo collegato ai servizi `AWSServiceRoleForSupport`. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Il `AWSServiceRoleForSupport` ruolo è necessario per Supporto 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.

I clienti che hanno effettuato l'onboarding AWS Organizations e che dispongono di un Supporto piano Enterprise possono eliminare il ruolo collegato al `AWSServiceRoleForSupport` servizio. L'eliminazione di questo ruolo limita l'accesso alle tue risorse da parte Supporto AWS degli ingegneri, limitando la loro capacità di eseguire azioni per tuo conto. Per ulteriori informazioni o per richiedere l'eliminazione del ruolo `AWSServiceRoleForSupport` legato al servizio, contattate il vostro Technical Account Manager (TAM).

Per ulteriori informazioni sul ruolo `AWSServiceRoleForSupport` o sui suoi utilizzi, contatta [Supporto](#).

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

Supporto AWS 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 dei ruoli collegati ai servizi per Supporto AWS](#).

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 di ruolo collegate al servizio per Trusted Advisor](#)
- [Gestione dei permessi per ruoli collegati ai servizi](#)
- [Creazione di un ruolo collegato al servizio per Trusted Advisor](#)
- [Modifica di un ruolo collegato al servizio per Trusted Advisor](#)

- [Eliminazione di un ruolo collegato al servizio per Trusted Advisor](#)

Autorizzazioni di ruolo collegate al servizio 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 policy attribuita, consulta la sezione

[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 al servizio è necessario 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'[AdministratorAccess](#) accesso completo a Trusted Advisor

Creazione di un ruolo collegato al servizio 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 Console di gestione AWS, 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 (Trusted 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 al servizio per Trusted Advisor

Dopo aver creato un ruolo collegato ai servizi, non è possibile modificarne il nome, perché potrebbero riferirsi diverse entità. Tuttavia, puoi utilizzare la console IAM o AWS CLI l'API IAM per modificare la descrizione del ruolo. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Trusted Advisor

Se non è necessario utilizzare le funzionalità o i servizi di Trusted Advisor, è possibile eliminare il ruolo. `AWSServiceRoleForTrustedAdvisor` 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 Console di gestione AWS e vai alla Trusted Advisor console all'indirizzo <https://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'API IAM per eliminare il ruolo Trusted Advisor collegato al servizio denominato `AWSServiceRoleForTrustedAdvisor`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

AWS politiche gestite per Supporto AWS

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 Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite 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 AWS](#) nella Guida per l'utente di IAM.

Argomenti

- [AWS politiche gestite per Supporto AWS](#)
- [AWS politiche gestite per Supporto AWS App in Slack](#)
- [AWS politiche gestite per AWS Trusted Advisor](#)
- [AWS politiche gestite per Supporto AWS Plans](#)
- [AWS politiche gestite per AWS Partner-Led Support](#)

AWS politiche gestite per Supporto AWS

Supporto AWS dispone delle seguenti politiche gestite.

Indice

- [AWS politica gestita: AWSSupportAccess](#)
- [AWS politica gestita: AWSSupportServiceRolePolicy](#)
- [Supporto AWS aggiornamenti alle politiche AWS gestite](#)
- [Modifica delle autorizzazioni per AWSSupportServiceRolePolicy](#)

AWS politica gestita: AWSSupportAccess

Supporto AWS utilizza la politica [AWSSupportAccess](#) AWS gestita. Questa policy gestisce il ciclo di vita dei casi di assistenza tramite l' Supporto API. Le funzionalità avanzate di sono fornite tramite AWS Support Center Console il servizio API della console di supporto. Puoi allegare questa policy alle tue entità IAM. Per ulteriori informazioni, consulta [Autorizzazioni di ruolo collegate al servizio per Supporto](#).

Per vedere le autorizzazioni per questa policy, consulta [AWSSupportAccess](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSSupportServiceRolePolicy

Supporto AWS 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 di ruolo collegate al servizio per Supporto](#).

Per vedere le autorizzazioni per questa policy, consulta [AWSSupportServiceRolePolicy](#) nella Guida di riferimento sulle policy gestite da AWS .

Per un elenco delle modifiche della policy, consulta [Supporto AWS aggiornamenti alle politiche AWS gestite](#) e [Modifica delle autorizzazioni per AWSSupportServiceRolePolicy](#).

Supporto AWS aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite Supporto AWS 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 Supporto AWS gestite dal 17 febbraio 2022.

Supporto AWS

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento a una policy esistente	Sono state aggiunte 105 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 Bedrock: per risolvere i problemi relativi ad Amazon Bedrock. • Amazon Braket: per eseguire il debug di problemi relativi ad Amazon Braket. • Amazon Connect: per eseguire il debug di problemi relativi ad Amazon Connect. • Amazon Aurora DSQL: per risolvere i problemi relativi ad Amazon Aurora DSQL. • AWS Compute Optimizer — Per eseguire il debug di problemi relativi a. AWS Compute Optimizer • Amazon Connect: per eseguire il debug di problemi relativi ad Amazon Connect.	29 gennaio 2026

Modifica	Descrizione	Data
	• Amazon EBS: per eseguire il debug di problemi relativi ad Amazon EBS. • Amazon EC2: per risolvere i problemi relativi ad Amazon EC2. • Amazon EKS: per eseguire il debug di problemi relativi ad Amazon EKS. • AWS Elastic Beanstalk — Per eseguire il debug di problemi relativi a. AWS Elastic Beanstalk • AWS Glue — Per risolvere i problemi relativi a. AWS Glue • AWS IoT Greengrass — Per eseguire il debug di problemi relativi a. AWS IoT Greengrass • Fatturazione AWS — Per eseguire il debug di problemi relativi a. Fatturazione AWS • Amazon Kinesis Video Streams: per eseguire il debug di problemi relativi ad Amazon Kinesis Video Streams. • AWS License Manager — Per eseguire il debug di problemi relativi a. AWS License Manager	

Modifica	Descrizione	Data
	• Amazon MemoryDB: per risolvere i problemi relativi ad Amazon MemoryDB. • Approvazione multipartita: per eseguire il debug di problemi relativi all'approvazione multipartita. • Amazon MQ: per risolvere i problemi relativi ad Amazon MQ. • Oracle Database@AWS — Per risolvere i problemi relativi a Oracle Database@.AWS • AWS Crittografia dei pagamenti: per eseguire il debug dei problemi relativi alla crittografia dei pagamenti. AWS • Amazon RDS: esecuzione e del debug di problemi relativi ad Amazon RDS. • AWS Impostazioni fiscali: per risolvere i problemi relativi alle impostazioni fiscali. AWS	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte 145 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 Amplify — Per risolvere i problemi relativi a. AWS Amplify • AWS AppSync — Per eseguire il debug di problemi relativi a. AWS AppSync • AWS Outposts — Per eseguire il debug di problemi relativi a. AWS Outposts • AWS Camere pulite: per risolvere i problemi relativi alle AWS camere bianche. • AWS Compute Optimizer — Per eseguire il debug di problemi relativi a. AWS Compute Optimizer • Amazon Connect: per eseguire il debug di problemi relativi ad Amazon Connect. • Amazon DynamoDB: esecuzione del debug di problemi relativi ad Amazon DynamoDB.	8 dicembre 2025

Modifica	Descrizione	Data
	• Amazon EMR: risoluzione problemi relativi ad Amazon EMR. • Amazon Location Service: per risolvere i problemi relativi ad Amazon Location Service. • Amazon GuardDuty : per eseguire il debug di problemi relativi ad Amazon GuardDuty. • AWS Network Firewall — Per eseguire il debug di problemi relativi a. AWS Network Firewall • AWS HealthOmics — Per risolvere i problemi relativi a. AWS HealthOmics • AWS Organizations — Per eseguire il debug di problemi relativi a. AWS Organizations • Amazon S3: esecuzione del debug di problemi relativi ad Amazon S3. • Tabelle Amazon S3: per eseguire il debug di problemi relativi alle tabelle Amazon S3. • Amazon S3 Vectors: per eseguire il debug di problemi relativi ad Amazon S3 Vectors.	

Modifica	Descrizione	Data
	• Amazon SageMaker AI: per risolvere i problemi relativi ad Amazon SageMaker AI. • AWS Security Hub CSPM — Per risolvere i problemi relativi a. AWS Security Hub CSPM • Amazon SES: per eseguire il debug di problemi relativi ad Amazon SES. • AWS Signer — Per eseguire il debug di problemi relativi a. AWS Signer • AWS STS — Per risolvere i problemi relativi a. AWS STS	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte 125 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: • Intelligenza artificiale per le operazioni IT (AIOps): per eseguire il debug di problemi relativi all'intelligenza artificiale per le operazioni IT (). AIOps • AWS Backup gateway — Per risolvere i problemi relativi a. AWS Backup gateway • CloudFormation — Per eseguire il debug di problemi relativi a. CloudFormation • Amazon Cognito Identity: per eseguire il debug di problemi relativi ad Amazon Cognito Identity. • Amazon Cognito: per risolvere i problemi relativi ad Amazon Cognito. • AWS Backup — Per eseguire il debug di problemi relativi a. AWS Backup	30 settembre 2025

Modifica	Descrizione	Data
	• Directory Service — Per eseguire il debug di problemi relativi a. Directory Service • Amazon EC2: per eseguire il debug di problemi relativi ad Amazon EC2. • AWS FIS — Per risolvere i problemi relativi a. AWS FIS • Amazon FSx : per risolvere i problemi relativi ad Amazon. FSx • AWS Global Accelerator — Per eseguire il debug di problemi relativi a. AWS Global Accelerator • AWS Identity Store: per eseguire il debug di problemi relativi a AWS Identity Store. • Fatturazione AWS — Per eseguire il debug di problemi relativi a. Fatturazione AWS • AWS Lake Formation — Per risolvere i problemi relativi a. AWS Lake Formation • AWS Network Firewall — Per eseguire il debug di problemi relativi a. AWS Network Firewall • Oracle Database@AWS — Per risolvere i problemi	

Modifica	Descrizione	Data
	relativi a Oracle Database@ .AWS • Amazon S3: esecuzione del debug di problemi relativi ad Amazon S3. • Amazon SES: per risolvere i problemi relativi ad Amazon SES. • AWS IAM Identity Center — Per risolvere i problemi relativi a. AWS IAM Identity Center	
AWSSupportAccess : aggiornamento di una policy esistente	Sono state aggiunte le autorizzazioni per l'API della console di supporto alla policy gestita. AWSSupportAccess	18 luglio 2025

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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: • CloudFormation — Per eseguire il debug di problemi relativi a CloudFormation • AWS Config — Per risolvere i problemi relativi a AWS Config • Amazon OpenSearch Service: per eseguire il debug di problemi relativi ad Amazon OpenSearch Service. • AWS Glue — Per eseguire il debug di problemi relativi a AWS Glue • AWS IAM: per risolvere i problemi relativi a IAM. AWS • Amazon Pinpoint: per risolvere problemi relativi ad Amazon Pinpoint. • AWS Outposts — Per eseguire il debug di problemi relativi a AWS Outposts	15 luglio 2025

Modifica	Descrizione	Data
	• AWS STS — Per eseguire il debug di problemi relativi a. AWS STS Per ulteriori informazioni, consulta Modifica delle autorizzazioni per AWSSupportServiceRolePolicy.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte 257 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 App Runner — Per eseguire il debug di problemi relativi a. AWS App Runner • AWS AppSync — Per risolvere i problemi relativi a. AWS AppSync • AWS Batch — Per eseguire il debug di problemi relativi a. AWS Batch • Amazon Bedrock: per risolvere i problemi relativi ad Amazon Bedrock. • Amazon CloudFront : per eseguire il debug di problemi relativi ad Amazon CloudFront. • AWS CodePipeline — Per risolvere i problemi relativi a. AWS CodePipeline • AWS Config — Per risolvere i problemi relativi a. AWS Config • Amazon Connect: per eseguire il debug di	17 giugno 2025

Modifica	Descrizione	Data
	problemi relativi ad Amazon Connect. • AWS DataSync — Per eseguire il debug di problemi relativi a. AWS DataSync • Direct Connect — Per risolvere i problemi relativi a. Direct Connect • Amazon EC2: per risolvere i problemi relativi ad Amazon EC2. • AWS Servizio Fault Injection : per eseguire il debug di problemi relativi al servizio Fault Injection. AWS • AWS Firewall Manager — Per risolvere i problemi relativi a. AWS Firewall Manager • AWS Glue — Per eseguire il debug di problemi relativi a. AWS Glue • Amazon GuardDuty : per eseguire il debug di problemi relativi ad Amazon GuardDuty. • EC2 Image Builder — Per risolvere i problemi relativi a EC2 Image Builder. • AWS IoT — Per risolvere i problemi relativi a. AWS IoT	

Modifica	Descrizione	Data
	• AWS IoT FleetWise — Per eseguire il debug di problemi relativi a. AWS IoT FleetWise • Amazon CloudWatch Logs: per eseguire il debug di problemi relativi ad Amazon CloudWatch Logs. • AWS Elemental MediaLive — Per eseguire il debug di problemi relativi a. AWS Elemental MediaLive • Network Flow Monitor: per risolvere i problemi relativi al Network Flow Monitor. • AWS Network Manager — Per risolvere i problemi relativi a. AWS Network Manager • Amazon CloudWatc h Observability Admin Service: per risolvere i problemi relativi ad Amazon CloudWatch Observability Admin Service. • AWS Parallel Computing Service: per eseguire il debug di problemi relativi al Parallel Computing Service. AWS • Amazon Redshift Serverles s: per risolvere i problemi	

Modifica	Descrizione	Data
	relativi ad Amazon Redshift Serverless. • Amazon Redshift: per risolvere i problemi relativi ad Amazon Redshift. • AWS Resilience Hub — Per eseguire il debug di problemi relativi a. AWS Resilience Hub • AWS Identity and Access Management Roles Anywhere: per eseguire il debug di problemi relativi a AWS Identity and Access Management Roles Anywhere. • Amazon S3 on Outposts: per risolvere i problemi relativi ad Amazon S3 on Outposts. • Amazon S3: per risolvere i problemi relativi ad Amazon S3. • Tabelle Amazon S3: per risolvere i problemi relativi alle tabelle Amazon S3. • Amazon SageMaker AI: per eseguire il debug di problemi relativi all' SageMaker intelligenza artificiale di Amazon. • AWS Security Hub CSPM — Per eseguire il debug	

Modifica	Descrizione	Data
	di problemi relativi a. AWS Security Hub CSPM • Amazon SQS: per eseguire il debug di problemi relativi ad Amazon SQS. • Strumento di gestione degli incidenti AWS Systems Manager — Per risolvere i problemi relativi a. Strumento di gestione degli incidenti AWS Systems Manager • AWS Systems Manager Configurazione rapida: per eseguire il debug dei problemi relativi alla AWS Systems Manager configurazione rapida. • AWS Systems Manager — Per eseguire il debug di problemi relativi a. AWS Systems Manager • Amazon WorkSpaces Thin Client: per risolvere i problemi relativi ad Amazon WorkSpaces Thin Client. • Amazon Timestream: per eseguire il debug di problemi relativi ad Amazon Timestream. • AWS Telco Network Builder: per risolvere i problemi	

Modifica	Descrizione	Data
	relativi a Telco Network Builder. AWS • AWS Transfer Family — Per eseguire il debug di problemi relativi a. AWS Transfer Family • Amazon VPC Lattice: per risolvere i problemi relativi ad Amazon VPC Lattice.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte 88 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: • Amazon Bedrock: per risolvere i problemi relativi ad Amazon Bedrock. • Amazon Connect: per eseguire il debug di problemi relativi ad Amazon Connect. • Amazon DataZone : per eseguire il debug di problemi relativi ad Amazon DataZone. • Amazon EC2: per risolvere i problemi relativi ad Amazon EC2. • Amazon EKS: per eseguire il debug di problemi relativi ad Amazon EKS. • AWS Glue — Per risolvere problemi relativi a. AWS Glue • Amazon Managed Service for Apache Flink: per risolvere i problemi relativi ad Amazon Managed Service for Apache Flink.	25 novembre 2024

Modifica	Descrizione	Data
	• AWS Lambda — Per eseguire il debug di problemi relativi a. AWS Lambda	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte 79 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: • Amazon OpenSearch Serverless: per risolvere i problemi relativi ad Amazon OpenSearch Serverless. • AWS AppConfig — Per eseguire il debug di problemi relativi a. AWS AppConfig • Segnali applicativi: per eseguire il debug di problemi relativi ai segnali di applicazione. • Amazon Athena: per risolvere i problemi relativi ad Amazon Athena. • Amazon CloudWatch : per eseguire il debug di problemi relativi ad Amazon CloudWatch. • Amazon DynamoDB: per risolvere i problemi relativi ad Amazon DynamoDB. • Amazon EC2: per risolvere i problemi relativi ad Amazon EC2.	8 ottobre 2024

Modifica	Descrizione	Data
	• AWS IoT — Per eseguire il debug di problemi relativi a. AWS IoT • AWS Lambda — Per risolvere i problemi relativi a. AWS Lambda • AWS Launch Wizard — Per risolvere i problemi relativi a. AWS Launch Wizard • AWS Security Hub CSPM — Per eseguire il debug di problemi relativi a. AWS Security Hub CSPM • Amazon WorkSpaces : per eseguire il debug di problemi relativi ad Amazon WorkSpaces.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di una policy esistente	Sono state aggiunte 79 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: • Account AWS — Per risolvere i problemi relativi a. Account AWS • AWS Auto Scaling — Per eseguire il debug di problemi relativi a. AWS Auto Scaling • Amazon Bedrock: per eseguire il debug di problemi relativi ad Amazon Bedrock. • AWS CodeConnections — Per risolvere i problemi relativi a. AWS CodeConnections • AWS Deadline Cloud: per eseguire il debug dei problemi relativi a Deadline Cloud. AWS • Servizio di Amazon Elastic Kubernetes: risoluzione di problemi relativi al servizio di Amazon Elastic Kubernetes. • Elastic Load Balancing — Per risolvere i problemi	5 agosto 2024

Modifica	Descrizione	Data
	relativi all'Elastic Load Balancing. • AWS Piano gratuito: per eseguire il debug dei problemi relativi al piano gratuito. AWS • Amazon Inspector: per risolvere i problemi relativi ad Amazon Inspector. • Amazon OpenSearch Ingestion: per risolvere i problemi relativi ad Amazon Ingestion. OpenSearch • Amazon WorkSpaces : per eseguire il debug di problemi relativi ad Amazon WorkSpaces. • AWS X-Ray — Per eseguire il debug di problemi relativi a. AWS X-Ray	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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'amministrazione e al supporto tecnico: • Amazon CloudWatch Network Monitor: per 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.	22 marzo 2024

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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 di 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 AI: per risolvere i problemi relativi al servizio Amazon SageMaker AI. • 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. • Ripristino di emergenza di elastico di AWS — Per risolvere i problemi relativi a. Ripristino di emergenza di elastico di AWS • 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.	

Modifica	Descrizione	Data
	• AWS Snowball Edge — Per risolvere i problemi relativi a. AWS Snowball Edge • AWS Health Imaging: per risolvere i problemi relativi all'imaging. AWS Health	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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
	• Ripristino di emergenza di elastico di AWS — Per risolvere i problemi relativi a. Ripristino di emergenza di elastico di AWS • 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 di 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: risoluzione 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 Quick: per eseguire il debug di problemi relativi ad Amazon Quick. • 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 AI: per eseguire il debug di problemi relativi ad Amazon SageMaker AI.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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 di 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. • Ripristino di emergenza di elastico di AWS — 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 di 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: esecuzione 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 di 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 di 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 Supporto AWS 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: Supporto AWS per consentire di interrogare le risorse Amazon IVS per risolvere i problemi dei clienti. • Amazon FSx : per consentire e lo sviluppo Supporto AWS di strumenti per supportare l'importazione e l'esportazione per un repository di FSx dati Amazon. • Amazon GameLift Servers: per risolvere i problemi relativi ai server 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	

Modifica	Descrizione	Data
	Kafka: per risolvere 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 di 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 Supporto AWS 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. • Modernizzazione del mainframe AWS — Per eseguire il debug di problemi relativi a. Modernizzazione del mainframe AWS • AWS Outposts — Per aiutare a Supporto AWS	4 ottobre 2022

Modifica	Descrizione	Data
	ottenere un elenco di host e risorse dedicati. • AWS Private 5G: risoluzione di problemi relativi a Private 5G. • AWS Tiro: per eseguire il debug dei problemi relativi a Tiro.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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 • Ripristino di emergenza di elastico di AWS — 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 configurazione dell'URL di una funzione per la risoluzione dei problemi. • Amazon Lookout per le apparecchiature: per	17 agosto 2022

Modifica	Descrizione	Data
	risolvere i problemi relativi a Lookout per le apparecchiature. • Amazon Route 53 e Amazon Route 53 Resolver: per ottenere configurazioni di resolver in modo Supporto AWS da controllare il comportamento di risoluzione DNS di un VPC.	

Modifica	Descrizione	Data
AWSSupportServiceRolePolicy : aggiornamento di 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 Supporto 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 di 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 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 di 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: per ottenere metadati sugli impegni in sospeso di Savings Plans. • 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 di 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 e 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. • Ripristino di emergenza di elastico di AWS — Per risolvere i problemi di replica e avvio negli account dei clienti. • Amazon FSx : per visualizzare la descrizione degli FSx snapshot di Amazon.	17 febbraio 2022

Modifica	Descrizione	Data
	• Amazon Lightsail – Per visualizzare i dettagli dei metadati e delle configurazioni per i bucket Lightsail. • Amazon Macie – Per visualizzare le configurazioni Macie, come processi di classificazione, identificatori 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). • Gateway di archiviazione AWS — Per visualizzare i metadati sulle politiche di creazione automatica dei nastri dei clienti. • Elastic Load Balancing - Per visualizzare la descrizione dei limiti delle risorse quando si utilizza la console Service Quotas. Per ulteriori informazioni, consulta Modifica delle autorizzazioni per AWSSupportServiceRolePolicy.	

Modifica	Descrizione	Data
Log delle modifiche pubblicato	Registro delle modifiche per le politiche Supporto AWS gestite.	17 febbraio 2022

Modifica delle autorizzazioni per AWSSupportServiceRolePolicy

La maggior parte delle autorizzazioni è stata aggiunta Supporto AWS 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:GetAnalyticsConfiguration
	s3.ListBucketAnalyticsConfiguration	
	s3.GetBucketNotificationConfiguration	s3:GetBucketNotification
	s3.GetBucketEncryption	s3:GetEncryptionConfiguration
	s3.GetBucketIntelligentTieringConfiguration	s3:GetIntelligentTieringConfiguration
	s3.ListBucketIntelligentTieringConfiguration	
	s3.GetBucketInventoryConfiguration	s3:GetInventoryConfiguration

Data	Nome operazione API	Policy autorizzazioni richieste
	s3.ListBucketInventoryConfiguration	
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.ListBucketMetricsConfiguration	
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket	s3:ListBucket
	s3.ListObjects	
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts
Autorizzazioni aggiunte il 15 luglio 2025	cloudcontrolapi:GetResource	cloudformation:GetResource
	cloudcontrolapi:ListResources	cloudformation:ListResources

AWS politiche gestite per Supporto AWS App in Slack

Note

Per accedere e visualizzare i casi di assistenza in AWS Support Center Console, consulta [Gestisci l'accesso al Centro Supporto AWS](#).

Supporto AWS L'app ha le seguenti politiche gestite.

Indice

- [AWS politica gestita: AWSSupportAppFullAccess](#)
- [AWS politica gestita: AWSSupportAppReadOnlyAccess](#)
- [Supporto AWS 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 [Supporto AWS App in Slack](#).

Per vedere le autorizzazioni per questa policy, consulta [AWSSupportAppFullAccess](#) nella Guida di riferimento sulle policy gestite da AWS .

Dettagli delle autorizzazioni

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.

Per ulteriori informazioni, consulta [Gestione dell'accesso all' Supporto AWS app](#).

AWS politica gestita: AWSSupportAppReadOnlyAccess

La [AWSSupportAppReadOnlyAccess](#) policy concede autorizzazioni che consentono all'entità di eseguire azioni relative all'app di sola lettura Supporto AWS . Per ulteriori informazioni, consulta [Supporto AWS App in Slack](#).

Per vedere le autorizzazioni per questa policy, consulta [AWSSupportAppReadOnlyAccess](#) nella Guida di riferimento sulle policy gestite da AWS .

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `support:` descrive i dettagli e le comunicazioni dei casi di supporto aggiunti ai casi di supporto.

Supporto AWS Aggiornamenti delle app alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Supporto AWS 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' Supporto AWS app dal 17 agosto 2022.

Supporto AWS App

Modifica	Descrizione	Data
AWSSupportAppFullAccess e AWSSupportAppReadOnlyAccess Nuove politiche AWS gestite per l' Supporto AWS app	Puoi utilizzare queste policy per il ruolo IAM che configuri per la configurazione del canale Slack. Per ulteriori informazioni, consulta Gestione dell'accesso all' Supporto AWS app .	19 agosto 2022

Modifica	Descrizione	Data
Log delle modifiche pubblicato	Registro delle modifiche per le politiche gestite Supporto AWS 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](#)
- [AWS politica gestita: AWSTrustedAdvisorPriorityReadOnlyAccess](#)
- [AWS politica gestita: AWSTrustedAdvisorServiceRolePolicy](#)
- [AWS politica gestita: AWSTrustedAdvisorReportingServiceRolePolicy](#)
- [Trusted Advisor aggiornamenti alle politiche gestite AWS](#)

AWS politica gestita: AWSTrustedAdvisorPriorityFullAccess

La [AWSTrustedAdvisorPriorityFullAccess](#) politica 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 delle autorizzazioni

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.

JSON

```
{
  "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 [AWSTrustedAdvisorPriorityReadOnlyAccess](#) politica concede autorizzazioni di sola lettura a Trusted Advisor Priority, inclusa l'autorizzazione a visualizzare gli account degli amministratori delegati.

Dettagli delle autorizzazioni

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

JSON

```

{
  "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"
        ]
      }
    }
  }
]
}

```

AWS politica gestita: 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 Trusted Advisor valutazione del tuo account.

Dettagli delle autorizzazioni

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TrustedAdvisorServiceRolePermissions",
      "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:DescribeListeners",
"elasticloadbalancing:DescribeRules",
"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 delle autorizzazioni

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

JSON

```
{
  "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 Supporto AWS 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 elasticloadbalancing:DescribeRules autorizzazioni elasticloadbalancing:DescribeListeners, e.	30 ottobre 2024
AWSTrustedAdvisorServiceRolePolicy	Trusted Advisor ha aggiunto nuove azioni per concedere le access-an	11 giugno 2024

Modifica	Descrizione	Data
Aggiornamento a una politica esistente.	<code>alyzer:ListAnalyzers</code> <code>cloudwatch:ListMetrics</code> <code>dax:DescribeClusters</code> <code>ec2:DescribeNatGateways</code> <code>ec2:DescribeRouteTables</code> <code>ec2:DescribeVpcEndpoints</code> <code>ec2:GetManagedPrefixListEntries</code> <code>elasticloadbalancing:DescribeTargetHealth</code> <code>iam:ListSAMLProviders</code> <code>kafka:DescribeClusterV2</code> <code>network-firewall:ListFirewalls</code> <code>network-firewall:DescribeFirewall</code> e <code>sqs:GetQueueAttributes</code> le autorizzazioni.	

Modifica	Descrizione	Data
AWSTrustedAdvisorServiceRolePolicy Aggiornamento a una politica esistente.	Trusted Advisor ha aggiunto nuove azioni per concedere <code>cloudtrail:GetTrail</code> <code>cloudtrail:ListTrails</code> <code>cloudtrail:GetEventSelectors</code> <code>outposts:GetOutpost</code> <code>le outposts:ListOutposts</code> autorizzazioni <code>outposts:ListAssets</code> e.	18 gennaio 2024
AWSTrustedAdvisorPriorityFullAccess Aggiornamento a una politica esistente.	Trusted Advisor ha aggiornato la politica <code>AWSTrustedAdvisorPriorityFullAccess</code> AWS gestita per includere una dichiarazione IDs.	6 dicembre 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Aggiornamento a una politica esistente.	Trusted Advisor ha aggiornato la politica <code>AWSTrustedAdvisorPriorityReadOnlyAccess</code> AWS gestita per includere una dichiarazione IDs.	6 dicembre 2023
AWSTrustedAdvisorServiceRolePolicy : aggiornamento di una policy esistente	Trusted Advisor ha aggiunto nuove azioni per concedere <code>ecs:ListTaskDefinitions</code> autorizzazioni <code>ec2:DescribeRegions</code> <code>s3:GetLifecycleConfiguration</code> <code>ecs:DescribeTaskDefinition</code> e.	9 novembre 2023

Modifica	Descrizione	Data
AWSTrustedAdvisorServiceRolePolicy : aggiornamento di una policy esistente	Trusted Advisor ha aggiunto nuove azioni route53resolver:ListResolveEndpoints IAM kafka:ListClusters V2 e ha introdotto nuovi controlli kafka:ListNodes di resilienza. route53resolver:ListResolveEndpointIpAddresses 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 di una policy esistente	Trusted Advisor ha aggiunto nuove azioni per concedere le <code>GetAccountPublicAccessBlock</code> autorizzazioni <code>DescribeTargetGroups</code> e. È richiesta l'autorizzazione <code>DescribeTargetGroup</code> per il Controllo dello stato del gruppo Auto Scaling per recuperare i non-Classical Load Balancers attribuiti a un gruppo Auto Scaling. È necessaria l'autorizzazione <code>GetAccountPublicAccessBlock</code> 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 Supporto AWS Plans

Supporto AWS Plans dispone delle seguenti politiche gestite.

Indice

- [AWS politica gestita: AWSSupportPlansFullAccess](#)

- [AWS politica gestita: AWSSupportPlansReadOnlyAccess](#)
- [Supporto AWS Piani, aggiornamenti alle politiche AWS gestite](#)

AWS politica gestita: AWSSupportPlansFullAccess

Supporto AWS 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
- Visualizza un elenco di tutti i modificatori del piano di supporto per il tuo Account AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule",
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource": "*"
    }
  ]
}
```

Per un elenco delle modifiche della policy, consulta la pagina [Supporto AWS Piani, aggiornamenti alle politiche AWS gestite](#).

AWS politica gestita: AWSSupportPlansReadOnlyAccess

Supporto AWS 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
- Visualizza un elenco di tutti i modificatori del piano di supporto per il tuo Account AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource": "*"
    }
  ]
}
```

Per un elenco delle modifiche della policy, consulta la pagina [Supporto AWS Piani, aggiornamenti alle politiche AWS gestite](#).

Supporto AWS 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.

Supporto AWS

Modifica	Descrizione	Data
AWSSupportPlansReadOnlyAccess - Aggiornamento a una policy esistente AWSSupportPlansFullAccess - Aggiornamento a una policy esistente	Aggiungi ListSupportPlanModifiers azioni AWSSupportPlansFullAccess e AWSSupportPlansReadOnlyAccess gestisci le politiche.	9 settembre 2024
AWSSupportPlansFullAccess - Aggiornamento a una policy esistente	Aggiungi azioni CreateSupportPlanSchedule alla policy gestita da AWSSupportPlansFullAccess.	08 maggio 2023
Log delle modifiche pubblicato	Log delle modifiche per le policy gestite dai piani di supporto.	29 settembre 2022

AWS politiche gestite per AWS Partner-Led Support

Una politica AWS gestita è una politica autonoma creata e amministrata da 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 Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite 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 AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AWSPartner LedSupportReadOnlyAccess

È possibile associare la policy `AWSPartnerLedSupportReadOnlyAccess` a utenti, gruppi e ruoli.

Questa politica può essere utilizzata per concedere l'accesso in sola lettura ai metadati di servizio in APIs grado di leggere i servizi del tuo account. AWS Puoi utilizzare questa politica per fornire ai tuoi partner del AWS Partner-Led Support Program l'accesso ai servizi specificati nella seguente sezione con i dettagli delle autorizzazioni.

Important

Sebbene `AWSPartnerLedSupportReadOnlyAccess` sia una politica gestita fornita da AWS, sei responsabile della revisione dei servizi e delle autorizzazioni inclusi nella politica per verificare che soddisfino i tuoi requisiti di supporto specifici. Non dare per scontato che questa politica gestita includa automaticamente tutte le politiche esistenti o nuove Servizi AWS. Potrebbe essere necessario creare e mantenere politiche personalizzate aggiuntive per coprire i servizi che non rientrano nell'ambito di questa politica gestita.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `acm`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Certificate Manager
- `acm-pca`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Autorità di certificazione privata
- `apigateway`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon API Gateway.
- `athena`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Athena.
- `backup`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Backup
- `backup-gateway`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a Backup AWS Gateway.

- `cloudformation`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS CloudFormation
- `cloudfront`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. CloudFront
- `cloudtrail`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS CloudTrail
- `cloudwatch`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. CloudWatch
- `codepipeline`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS CodePipeline
- `cognito-identity`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Cognito Identity.
- `cognito-idp`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ai pool di utenti di Amazon Cognito.
- `cognito-sync`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Cognito Sync.
- `connect`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Connect.
- `directconnect`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Direct Connect
- `dms`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Database Migration Service
- `ds`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Directory Service
- `ec2`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Elastic Compute Cloud. Ciò include le categorie di supporto tecnico in EC2 (Windows e Linux), Virtual Private Cloud (VPC) e VPC.
- `ecs`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Elastic Container Service.
- `eks`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Elastic Kubernetes Service.
- `elasticache`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. ElastiCache

- `elasticbeanstalk`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Elastic Beanstalk
- `elasticfilesystem`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Elastic File System.
- `elasticloadbalancing`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a Elastic Load Balancing.
- `emr-containers`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon EMR su EKS.
- `emr-serverless`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon EMR Serverless.
- `es`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi al servizio Amazon. OpenSearch Ciò include categorie di supporto tecnico come OpenSearch Service Managed Cluster.
- `events`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. EventBridge
- `fsx`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. FSx Ciò include categorie di supporto tecnico come FSX per Windows File Server.
- `glue`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Glue
- `guardduty`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. GuardDuty
- `iam`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Identity and Access Management
- `kafka`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Managed Streaming for Apache Kafka.
- `kafkaconnect`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Managed Streaming for Apache Kafka Connect.
- `lambda`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Lambda
- `logs`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Logs. CloudWatch
- `medialive`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Elemental MediaLive
- `mobiletargeting`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Pinpoint.

- `pipes`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Pipes.
- `EventBridge`
- `polly`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Polly.
- `quicksight`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Quick.
- `rds`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Relational Database Service. Ciò include categorie di supporto tecnico come: Relational Database Service (Aurora - MySQL-Compatible), Relational Database Service (Aurora - PostgreSQL-C), Relational Database Service (PostgreSQL), Relational Database Service (SQL Server), Relational Database Service (MySQL) e Relational Database Service (Oracle).
- `redshift`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Redshift.
- `redshift-data`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi all'API di Amazon Redshift Data.
- `redshift-serverless`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Redshift Serverless.
- `route53`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Route 53.
- `route53domains`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ai domini Amazon Route 53.
- `route53-recovery-cluster`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Route 53 Recovery Cluster.
- `route53-recovery-control-config`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a Amazon Route 53 Recovery Controls.
- `route53-recovery-readiness`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Route 53 Recovery Readiness.
- `route53resolver`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Route 53 Resolver.
- `s3`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Simple Storage Service.
- `s3express`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon S3 Express.

- `sagemaker`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon AI. SageMaker
- `scheduler`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Scheduler. EventBridge
- `servicequotas`— Consentire ai responsabili di risolvere i casi di supporto tecnico relativi a Service Quotas.
- `ses`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Simple Email Service.
- `sns`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Simple Notification Service.
- `ssm`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS Systems Manager
- `ssm-contacts`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ai Contatti. Strumento di gestione degli incidenti AWS Systems Manager
- `ssm-incidents`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. Strumento di gestione degli incidenti AWS Systems Manager
- `ssm-sap`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a SAP. AWS Systems Manager
- `swf`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon Simple Workflow Service.
- `vpc-lattice`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon VPC Lattice. Ciò include categorie di supporto tecnico come VPC - Transit Gateway.
- `waf`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a. AWS WAF
- `waf-regional`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi a Regional. AWS WAF
- `wafv2`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi alla V2. AWS WAF
- `workspaces`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon. WorkSpaces Ciò include categorie di supporto tecnico come Workspaces (Windows).
- `workspaces-web`— Consenti ai responsabili di risolvere i casi di supporto tecnico relativi ad Amazon WorkSpaces Secure Browser. Ciò include categorie di supporto tecnico come Workspaces (Windows).

Per vedere le autorizzazioni per questa policy, consulta [AWSPartnerLedSupportReadOnlyAccess](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS Aggiornamenti delle policy gestite tramite Partner-Led Support AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per AWS Partner-Led Support da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di supporto AWS guidati dai partner.

Modifica	Descrizione	Data
AWSPartnerLedSupportReadOnlyAccess : nuova policy	È stata aggiunta una nuova politica AWS gestita che contiene le autorizzazioni per leggere i metadati dei servizi del tuo account. AWS	22 novembre 2024
AWS Partner-Led Support ha iniziato a tenere traccia delle modifiche	AWS Partner-Led Support ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	22 novembre 2024

Gestisci l'accesso al Centro Supporto AWS

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:

- Usa AWS Identity and Access Management (IAM).
- Utilizza l'indirizzo e-mail e la password associati al tuo AWS account. Questa identità è chiamata utente root dell' AWS account (non consigliata).

Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puoi anche utilizzare l'[Supporto API](#) per accedere Supporto e Trusted Advisor operare a livello di codice. Per ulteriori informazioni, consulta la [documentazione di riferimento dell'API di Supporto AWS](#).

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.

Per informazioni sulle operazioni dell'API della console di Support Center e su come aggiungerle alle policy IAM, consulta [Aggiungere policy IAM per le operazioni dell'API Support Center Console](#).

AWS account (non consigliato)

Puoi accedere Console di gestione AWS 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 Supporto azioni nella console. Puoi anche specificare queste Supporto azioni in una policy IAM per consentire o negare azioni specifiche.

Note

Il rifiuto di una qualsiasi delle seguenti azioni nelle policy IAM potrebbe comportare un comportamento non intenzionale in Support Center durante la creazione o l'interazione con un caso di supporto.

Azione	Description
AddAttachmentsToSet	Concede l'autorizzazione ad aggiungere uno o più allegati a un set di allegati. Un set di allegati

Azione	Description
	è un contenitore temporaneo per gli allegati aggiunti a un caso o a una comunicazione di caso. Il set è disponibile per 1 ora dopo la creazione. L'ExpiryTime restituito nella risposta è quando il set scade.
AddCommunicationToCase	Concede l'autorizzazione ad aggiungere ulteriori comunicazioni con il cliente a un Supporto caso, incluso un set di indirizzi e-mail da copiare nella comunicazione.
CreateCase	Concede l'autorizzazione a creare un caso.
DescribeAttachment	Concede l'autorizzazione a recuperare un allegato su un caso.
DescribeCaseAttributes	Concede l'autorizzazione a consentire ai servizi secondari di leggere gli attributi dei casi Supporto . *Viene utilizzato internamente da Supporto Center per contrassegnare gli attributi sul caso.
DescribeCases	Concede l'autorizzazione a restituire un elenco di Supporto casi che corrisponde all'ID o al caso. IDs
DescribeCommunication	Concede l'autorizzazione a ricevere una singola comunicazione e allegati per un singolo caso. AWS Supporto
DescribeCommunications	Concede l'autorizzazione a restituire comunicazioni e allegati per uno o più casi. Supporto
DescribeCreateCaseOptions	Concede l'autorizzazione a restituire un elenco di CreateCaseOption tipi insieme alle ore supportate corrispondenti e alla disponibilità delle lingue.

Azione	Description
<code>DescribeIssueTypes</code>	Concede l'autorizzazione a restituire i tipi di problemi dei casi di Supporto . Viene utilizzato internamente da Supporto Center per ottenere i tipi di problemi disponibili per l'account.
<code>DescribeServices</code>	Concede l'autorizzazione a restituire l'elenco corrente dei AWS servizi e un elenco di categorie di servizi per ogni servizio. Quindi si utilizzano i nomi e le categorie dei servizi per creare un caso. Ogni AWS servizio ha il proprio set di categorie.
<code>DescribeSeverityLevels</code>	Concede l'autorizzazione a restituire l'elenco dei livelli di gravità che è possibile assegnare a un Supporto caso.
<code>DescribeSupportedLanguages</code>	Concede l'autorizzazione a restituire un elenco di lingue supportate per <code>CategoryCode</code> , <code>IssueType</code> e <code>ServiceCode</code> specificati.
<code>DescribeSupportLevel</code>	Concede l'autorizzazione a restituire il livello di supporto per un identificatore di account. AWS Viene utilizzato internamente da Supporto Center per identificare il livello di supporto dell'utente.
<code>DescribeTrustedAdvisorCheckRefreshStatuses</code>	Concede l'autorizzazione a restituire lo stato di aggiornamento dei AWS Trusted Advisor controlli con il controllo specificato. IDs
<code>DescribeTrustedAdvisorCheckResult</code>	Concede l'autorizzazione a restituire i risultati del AWS Trusted Advisor controllo con l'ID di controllo specificato.

Azione	Description
<code>DescribeTrustedAdvisorChecks</code>	Concede l'autorizzazione a restituire informazioni su tutti i AWS Trusted Advisor controlli disponibili, inclusi nome, ID, categoria, descrizione e metadati.
<code>DescribeTrustedAdvisorCheckSummaries</code>	Concede l'autorizzazione a restituire i risultati dei riepiloghi dei AWS Trusted Advisor controlli per il controllo IDs specificato.
<code>GetInteraction</code>	Concede l'autorizzazione a recuperare i dettagli su una specifica interazione tramite il relativo identificatore univoco. Viene utilizzato internamente da Supporto Center per recuperare e consigli personalizzati.
<code>InitiateCallForCase</code>	Concede l'autorizzazione per avviare una chiamata su Center. Supporto Viene utilizzato internamente da Supporto Center per avviare una chiamata per conto dell'utente.
<code>ListInteractionEntries</code>	Concede l'autorizzazione a recuperare un elenco di voci all'interno di una specifica interazione, inclusi messaggi, aggiornamenti di stato o altri punti dati pertinenti. Viene utilizzato internamente da Supporto Center per tracciare la traccia dettagliata di un'interazione.
<code>ListInteractions</code>	Concede l'autorizzazione a recuperare un elenco di interazioni, potenzialmente con filtri o impaginazione. Viene utilizzato internamente da Supporto Center per gestire e visualizzare una panoramica di più interazioni.

Azione	Description
InitiateChatForCase	Concede l'autorizzazione ad avviare una chat su Supporto Center. Viene utilizzato internamente da Supporto Center per avviare una chat per conto dell'utente.
PutCaseAttributes	Concede l'autorizzazione a consentire ai servizi secondari di allegare attributi ai Supporto casi. Viene utilizzato internamente da Supporto Center per aggiungere tag operativi ai Supporto casi.
RateCaseCommunication	Concede l'autorizzazione a valutare la comunicazione di un Supporto caso.
RefreshTrustedAdvisorCheck	Concede l'autorizzazione ad aggiornare l' AWS Trusted Advisor assegno specificato utilizzando l'ID del controllo.
ResolveCase	Concede l'autorizzazione a risolvere un caso. Supporto
ResolveInteraction	Concede l'autorizzazione a contrassegnare un'interazione come risolta utilizzando il relativo identificatore univoco, indicando che il problema è stato risolto completamente e non richiede ulteriori azioni. Una volta risolto, lo stato dell'interazione viene impostato su CHIUSO e diventa accessibile a tutti gli utenti all'interno dello stesso account.
SearchForCases	Concede l'autorizzazione a restituire un elenco di Supporto casi che corrispondono agli input forniti. Viene utilizzato internamente da Supporto Center per trovare i casi ricercati.

Azione	Description
StartInteraction	Concede l'autorizzazione ad avviare una nuova interazione per ricevere assistenza personalizzata per la risoluzione di problemi tecnici e relativi all'account. Viene utilizzato internamente da Supporto Center per avviare il processo di risoluzione dei problemi.
UpdateInteraction	Concede l'autorizzazione ad aggiornare un'interazione specifica tramite il relativo identificatore univoco con un altro messaggio . Viene utilizzato internamente da Supporto Center per aggiornare il processo di risoluzione dei problemi.

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' Supporto 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 Account AWS e lavorare nel Support Center. Gli utenti IAM che hanno Supporto AWS accesso possono vedere tutti i casi creati per l'account.

Per ulteriori informazioni, consulta [Accedere Console di gestione AWS come utente IAM nella Guida per](#) l'utente IAM.

Il modo più semplice per concedere le autorizzazioni consiste nell'associare la policy AWS gestita [AWSSupportAccess](#) all'utente, al gruppo o al ruolo. Supporto AWS consente autorizzazioni a livello di azione per controllare l'accesso a operazioni specifiche. Supporto AWS Supporto AWS 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 Supporto

La policy AWS gestita [AWSSupportAccess](#) concede a un utente IAM l'accesso a Supporto. Un utente IAM con questa policy può accedere a tutte le Supporto AWS operazioni e le risorse.

JSON

```
{
  "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 Supporto tranne risolvere un caso.

JSON

```
{
  "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 Supporto AWS-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 Supporto AWS](#).

Accesso a AWS Trusted Advisor

In Console di gestione AWS, un namespace `trustedadvisor` IAM separato controlla l'accesso a Trusted Advisor. Nell' API Supporto IAM, 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 Supporto AWS

Argomenti

- [Autorizzazioni per la console dei piani di supporto](#)
- [Operazioni dei piani di supporto](#)
- [Policy IAM di esempio per i piani di supporto](#)
- [Risoluzione dei problemi](#)

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 namespace `supportplans`. 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 Supporto AWS 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	Description
<code>GetSupportPlan</code>	Concede l'autorizzazione per visualizzare i dettagli relativi al piano di supporto attuale per questo Account AWS.
<code>GetSupportPlanUpdateStatus</code>	Concede l'autorizzazione per visualizzare i dettagli relativi allo stato di una richiesta di aggiornamento di un piano di supporto.
<code>StartSupportPlanUpdate</code>	Concede l'autorizzazione per avviare la richiesta di aggiornamento del piano di supporto per questo Account AWS.
<code>CreateSupportPlanSchedule</code>	Concede l'autorizzazione a creare pianificazioni per i piani di assistenza per tale Account AWS.
<code>ListSupportPlanModifiers</code>	Concede l'autorizzazione a visualizzare un elenco di tutti i modificatori del piano di supporto a tale scopo. 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.

JSON

```
{
  "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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "supportplans:Get*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "supportplans:List*",
      "Resource": "*"
    }
  ]
}
```

```
}
```

Rifiuto dell'accesso ai piani di supporto

La policy seguente non consente agli utenti di accedere ai piani di supporto.

JSON

```
{
  "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 Supporto AWS 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). SCPs sono un tipo di politica che gestisce le autorizzazioni in un'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:

- [Criteri di controllo del servizio \(SCPs\)](#) nella Guida per l'AWS Organizations utente.
- [Configurazione del controllo di diniego della regione](#) nella Guida per l'utente di AWS Control Tower
- [Negare l'accesso a AWS in 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. Console di gestione AWS Tutti Account AWS hanno accesso a una selezione di [Trusted Advisor controlli](#) di base. Se disponi di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, 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](#)
- [Trusted Advisor azioni](#)
- [Esempi di policy IAM](#)
- [Consulta anche](#)

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`. Supporto Invece, devi utilizzare lo spazio dei nomi `support` per `Supporto`.

Note

Se disponi delle autorizzazioni per l'[Supporto AWS API](#), il Trusted Advisor widget nella finestra Console di gestione AWS 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	Description
DescribeAccount	Concede l'autorizzazione a visualizzare il Supporto 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 .
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.

Azione	Description
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	Description
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 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.

Azione	Description
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 (OUs) dell'unità organizzativa principale o principale.
ListRoots	Concede il permesso di 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 [Esempi di politiche IAM 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 [Inizia a usare AWS Trusted Advisor Priority](#).

Azione	Description
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.
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

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 Supporto API per Trusted Advisor](#)
- [Esempi di politiche IAM per Trusted Advisor Priority](#)

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.

JSON

```
{
  "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 console. Trusted Advisor Gli utenti non possono apportare modifiche, ad esempio aggiornare i controlli o modificare le preferenze di notifica.

JSON

```
{
  "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.

JSON

```
{
  "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.

JSON

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

Controlla l'accesso alle operazioni Supporto API per Trusted Advisor

In Console di gestione AWS, un namespace `trustedadvisor` IAM separato controlla l'accesso a Trusted Advisor. Non puoi utilizzare lo spazio dei nomi `trustedadvisor` per consentire o negare le operazioni API nell'API Trusted Advisor. Supporto API, al contrario, utilizza lo spazio dei nomi `support`. È necessario disporre delle autorizzazioni per l'API Supporto per effettuare chiamate a livello di codice. Trusted Advisor

Ad esempio, se si desidera chiamare l'[RefreshTrustedAdvisorCheck](#) operazione, 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 Supporto API per Trusted Advisor, ma non al resto delle operazioni Supporto API. Ad esempio, gli utenti possono utilizzare l'API per visualizzare e aggiornare i controlli. Non possono creare, visualizzare, aggiornare o risolvere Supporto AWS casi.

Puoi utilizzare questa politica per richiamare le operazioni dell'API Trusted Advisor a livello di codice, ma non puoi utilizzare questa politica per visualizzare o aggiornare i controlli nella console. Trusted Advisor

JSON

```
{
  "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 Supporto and Trusted Advisor, consulta. [Azioni](#)

Esempi di politiche IAM per Trusted Advisor Priority

Puoi utilizzare le seguenti politiche AWS gestite per controllare l'accesso a Trusted Advisor Priority. Per ulteriori informazioni, consultare [AWS politiche gestite per AWS Trusted Advisor](#) e [Inizia a usare AWS Trusted Advisor Priority](#).

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](#)

Esempi di politiche di controllo dei servizi per AWS Trusted Advisor

AWS Trusted Advisor supporta le politiche di controllo del servizio (SCP). SCPs sono politiche che allegate agli elementi di un'organizzazione per gestire le autorizzazioni all'interno di tale organizzazione. Un SCP si applica a tutti gli AWS account inclusi [nell'elemento a cui si collega l'SCP](#). SCPs offrite il controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account della vostra organizzazione. Possono aiutarti a garantire che i tuoi AWS account rispettino le linee guida per il controllo degli accessi dell'organizzazione. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .

Argomenti

- [Prerequisiti](#)
- [Policy di controllo dei servizi di esempio](#)

Prerequisiti

Per utilizzarlo SCPs, devi prima fare quanto segue:

- Abilitazione di tutte le caratteristiche nell'organizzazione. Per ulteriori informazioni, consulta la sezione [Abilitazione di tutte le funzionalità nell'organizzazione](#) nella Guida per l'utente di AWS Organizations .
- Abilita SCPs per l'uso all'interno della tua organizzazione. Per ulteriori informazioni, consulta [Abilitazione e disabilitazione dei tipi di policy](#) nella Guida per l'utente di AWS Organizations .

- Crea quelle SCPs che ti serve. Per ulteriori informazioni sulla creazione SCPs, vedere [Creazione, aggiornamento ed eliminazione delle politiche di controllo del servizio](#) nella Guida per l'AWS Organizations utente.

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.

JSON

```
{
  "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.

JSON

```
{
```

```
"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 Supporto AWS identità e accesso

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

Argomenti

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

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 Supporto.

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 Supporto. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

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

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Desidero visualizzare le mie chiavi di accesso

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

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

Important

Non fornire le chiavi di accesso a terze parti, neppure per aiutare a [trovare l'ID utente canonico](#). In questo modo, potresti concedere a qualcuno l'accesso permanente al tuo Account AWS.

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

Sono un amministratore e desidero consentire ad altri di accedere Supporto

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

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

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

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

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Supporto supporta queste funzionalità, consulta. [Come Supporto AWS funziona con IAM](#)
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.

Risposta agli incidenti

La risposta agli incidenti Supporto è una AWS responsabilità. AWS ha una politica e un programma formali e documentati che regolano la risposta agli incidenti. Per ulteriori informazioni, consulta la Guida [AWS Security Incident Response tecnica](#).

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 [Health Dashboard](#). Ad esempio, eventi che influiscono sui servizi o sulle risorse del tuo account. Per ulteriori informazioni, consulta [Nozioni di base su Health Dashboard](#) nella Guida per l'utente di AWS Health .

Registrazione e monitoraggio in Supporto AWS e AWS Trusted Advisor

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Supporto AWS e AWS Trusted Advisor e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per osservare Supporto AWS 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. È possibile raccogliere e tenere traccia dei parametri, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi 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 CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon 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, consultare [Monitoraggio e registrazione per Supporto AWS](#) e [Monitoraggio e registrazione per AWS Trusted Advisor](#).

Convalida della conformità per Supporto AWS

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. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la [Documentazione AWS sulla sicurezza](#).

Resilienza in Supporto AWS

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 Supporto AWS

In quanto servizio gestito, Supporto AWS 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 Supporto 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. In alternativa è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Analisi della configurazione e delle vulnerabilità in Supporto

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 Supporto l'utilizzo AWS SDKs

I seguenti esempi di codice mostrano come utilizzarlo Supporto con un kit di sviluppo AWS software (SDK).

Nozioni di base: esempi di codice che mostrano come eseguire le operazioni essenziali all'interno di un servizio.

Le azioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le azioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica chiamando più funzioni all'interno dello stesso servizio o combinate con altri Servizi AWS.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- [Esempi di base per l' Supporto utilizzo AWS SDKs](#)
 - [Salve Supporto](#)
 - [Scopri le nozioni di base di Supporto con un SDK AWS](#)
 - [Azioni per l'utilizzo Supporto AWS SDKs](#)
 - [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](#)
 - [Utilizzare DescribeTrustedAdvisorCheckRefreshStatuses con una CLI](#)
 - [Utilizzare DescribeTrustedAdvisorCheckResult con una CLI](#)
 - [Utilizzare DescribeTrustedAdvisorCheckSummaries con una CLI](#)

- [Utilizzare DescribeTrustedAdvisorChecks con una CLI](#)
- [Utilizzare RefreshTrustedAdvisorCheck con una CLI](#)
- [Utilizzo ResolveCase con un AWS SDK o una CLI](#)
- [Scenari di utilizzo Supporto AWS SDKs](#)
 - [Guida introduttiva a Support](#)

Esempi di base per l' utilizzo Supporto AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di Supporto AWS with. AWS SDKs

Esempi

- [Salve Supporto](#)
- [Scopri le nozioni di base di Supporto con un SDK AWS](#)
- [Azioni per l'utilizzo Supporto AWS SDKs](#)
 - [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](#)
 - [Utilizzare DescribeTrustedAdvisorCheckRefreshStatuses con una CLI](#)
 - [Utilizzare DescribeTrustedAdvisorCheckResult con una CLI](#)
 - [Utilizzare DescribeTrustedAdvisorCheckSummaries con una CLI](#)
 - [Utilizzare DescribeTrustedAdvisorChecks con una CLI](#)
 - [Utilizzare RefreshTrustedAdvisorCheck con una CLI](#)
 - [Utilizzo ResolveCase con un AWS SDK o una CLI](#)

Salve Supporto

L'esempio di codice seguente mostra come iniziare a utilizzare Supporto.

.NET

SDK per .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](#).

```
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($"{response.Services.Count} services available.");
    }
}
```

```
}  
}
```

- Per i dettagli sull'API, consulta la [DescribeServices](#) sezione AWS SDK per .NET API Reference.

Java

SDK per Java 2.x

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 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 [DescribeServices](#) sezione 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](#).

Invocazione di `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.",
            );
        }
    }
}
```

```
    );  
  }  
  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 [DescribeServices](#) sezione AWS SDK per JavaScript API Reference.

Kotlin

SDK per Kotlin

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](#).

/**

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.fromEnvironment { 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, [DescribeServices](#) consulta 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 AWS](#) SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scopri le nozioni di base di Supporto con un SDK AWS

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

SDK per .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($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"  {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 Supporto 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 dell'API AWS SDK per .NET .
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

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](#).

Esegui varie Supporto 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 = "C:\\\\AWS\\test.txt" ; //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 dell'API AWS SDK for Java 2.x .
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [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.",
        );
      }
      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 getTodayOpenCases = async () => {
  const d = new Date();
  const startOfDay = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfDay.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 dell'API AWS SDK per JavaScript .
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Kotlin

SDK per Kotlin

Note

C'è dell'altro 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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 dell'API AWS SDK per Kotlin.
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)

- [DescribeAttachment](#)
- [DescribeCases](#)
- [DescribeCommunications](#)
- [DescribeServices](#)
- [DescribeSeverityLevels](#)
- [ResolveCase](#)

Python

SDK per Python (Boto3)

Note

C'è dell'altro 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 dell'API AWS SDK per Python (Boto3).
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Azioni per l'utilizzo Supporto AWS SDKs

I seguenti esempi di codice mostrano come eseguire singole Supporto azioni con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove sono disponibili le istruzioni per la configurazione e l'esecuzione del codice.

Questi estratti richiamano l' Supporto API e sono estratti di codice di programmi più grandi che devono essere eseguiti nel contesto. È possibile visualizzare le azioni nel contesto in [Scenari di utilizzo Supporto AWS SDKs](#).

Gli esempi seguenti includono solo le azioni più comunemente utilizzate. Per un elenco completo, consulta la [documentazione di riferimento dell'API Supporto AWS](#).

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](#)
- [Utilizzare DescribeTrustedAdvisorCheckRefreshStatuses con una CLI](#)
- [Utilizzare DescribeTrustedAdvisorCheckResult con una CLI](#)
- [Utilizzare DescribeTrustedAdvisorCheckSummaries con una CLI](#)
- [Utilizzare DescribeTrustedAdvisorChecks con una CLI](#)
- [Utilizzare RefreshTrustedAdvisorCheck con una CLI](#)
- [Utilizzo ResolveCase con un AWS SDK o una CLI](#)

Utilizzo **AddAttachmentsToSet** con un AWS SDK o una CLI

Gli esempi di codice seguenti 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:

- [Informazioni di base](#)

.NET

SDK per .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 [AddAttachmentsToSet](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come aggiungere un allegato a un set

L'add-attachments-to-set esempio seguente aggiunge un'immagine a un set che puoi quindi specificare per un caso di supporto nel tuo AWS account.

```

aws support add-attachments-to-set \
  --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQ1Br70-
  G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE" \
  --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string

```

Output:

```

{
  "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQ1Br70-
  G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE",
  "expiryTime": "2020-05-14T17:04:40.790+0000"
}

```

Per ulteriori informazioni, consulta [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [AddAttachmentsToSet 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 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 [AddAttachmentsToSet](#) sezione 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 [AddAttachmentsToSet](#) sezione AWS SDK per JavaScript API Reference.

Kotlin

SDK per Kotlin

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](#).

```
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.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- Per i dettagli sull'API, [AddAttachmentsToSet](#) consulta 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 AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 [AddCommunicationToCase](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come aggiungere una comunicazione a un caso

L'add-communication-to-caseesempio 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-  
G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE"
```

Output:

```
{  
  "result": true  
}
```

Per ulteriori informazioni, consulta [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [AddCommunicationToCase 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 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 [AddCommunicationToCase](#) sezione 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 [AddCommunicationToCase](#) sezione AWS SDK per JavaScript API Reference.

Kotlin

SDK per Kotlin

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](#).

```
suspend fun addAttachSupportCase(
  caseIdVal: String?,
  attachmentSetIdVal: String?,
) {
  val caseRequest =
    AddCommunicationToCaseRequest {
```



```
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient.fromEnvironment { 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, [AddCommunicationToCase](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 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 e 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 [AddCommunicationToCase](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 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 e 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 [AddCommunicationToCase](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

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_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 Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 [CreateCases](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come 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 [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [CreateCase 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 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 [CreateCase](#) sezione 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 [CreateCase](#) sezione AWS SDK per JavaScript API Reference.

Kotlin

SDK per Kotlin

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](#).

```
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.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```



```
}  
}
```

- Per i dettagli sull'API, [CreateCase](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 PowerShell

Esempio 1: crea un nuovo caso nel AWS Support Center. I valori per i CategoryCode parametri - ServiceCode e - possono essere ottenuti utilizzando il Get-ASAService cmdlet. Il valore per il SeverityCode parametro - può essere ottenuto utilizzando il Get-ASASeverityLevel cmdlet. 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 utilizzare 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 [CreateCase](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: crea un nuovo caso nel AWS Support Center. I valori per i CategoryCode parametri - ServiceCode e - possono essere ottenuti utilizzando il Get-ASAService cmdlet. Il valore per il SeverityCode parametro - può essere ottenuto utilizzando il Get-ASASeverityLevel cmdlet. 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 utilizzare 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 [CreateCase](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

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 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 AWS](#) SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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:

- [Informazioni di base](#)

.NET

SDK per .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 [DescribeAttachment](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come descrivere un allegato

L'esempio `describe-attachment` seguente restituisce le 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 [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeAttachment 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 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 [DescribeAttachment](#) sezione 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.
            })
        );
    } catch (error) {
        console.error(error);
    }
}
```

```
        attachmentId: "ATTACHMENT_ID",
    })),
    );
    console.log(response.attachment?.fileName);
    return response;
} catch (err) {
    console.error(err);
}
};
```

- Per i dettagli sull'API, consulta la [DescribeAttachment](#) sezione AWS SDK per JavaScript API Reference.

Kotlin

SDK per Kotlin

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](#).

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient.fromEnvironment { 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, [DescribeAttachment](#) consulta 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 AWS](#) SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 [DescribeCases](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come 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 [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeCases 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 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 [DescribeCases](#) sezione 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 [DescribeCases](#) sezione AWS SDK per 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.fromEnvironment { 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, [DescribeCases](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 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 risolti.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Esempio 4: restituisce i dettagli del 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")
```

- Per i dettagli sull'API, vedere [DescribeCases](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 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 risolti.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Esempio 4: restituisce i dettagli del 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")
```

- Per i dettagli sull'API, vedere [DescribeCases](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

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_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 AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 [DescribeCommunications](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come descrivere la comunicazione più recente relativa a un caso

L'`describe-communications` esempio seguente restituisce la comunicazione più recente per il caso di supporto 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":
  "eyJhZG90VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Per ulteriori informazioni, consulta [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeCommunications 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 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 [DescribeCommunications](#) sezione 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 [DescribeCommunications](#) sezione AWS SDK per 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.fromEnvironment { 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, [DescribeCommunications](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 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"
```

- Per i dettagli sull'API, vedere [DescribeCommunications](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 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"
```

- Per i dettagli sull'API, vedere [DescribeCommunications](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

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_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 AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 [DescribeServices](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Per elencare AWS i servizi e le categorie di servizi

L'esempio `describe-services` seguente elenca le categorie dei 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 [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeServices 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](#).

```
// 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 [DescribeServices](#) sezione 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.fromEnvironment { 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, [DescribeServices](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 PowerShell

Esempio 1: restituisce tutti i codici, i nomi e le categorie disponibili per il servizio.

```
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 dei codici del servizio specificato.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Esempio 4: restituisce il nome e le categorie (in giapponese) dei codici del servizio specificato. 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 [DescribeServices](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce tutti i codici, i nomi e le categorie disponibili per il servizio.

```
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 dei codici del servizio specificato.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Esempio 4: restituisce il nome e le categorie (in giapponese) dei codici del servizio specificato. 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 [DescribeServices](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

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_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 AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 la [DescribeSeverityLevels](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come elencare i livelli di gravità disponibili

L'esempio `describe-severity-levels` 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 [Selezione di una gravità](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeSeverityLevels 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 la [DescribeSeverityLevels](#) sezione 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 la [DescribeSeverityLevels](#) sezione AWS SDK per 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.fromEnvironment { 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, [DescribeSeverityLevels](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 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 Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 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 Strumenti per PowerShell Cmdlet Reference (V5).

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_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 AWS](#) SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **DescribeTrustedAdvisorCheckRefreshStatuses** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare **DescribeTrustedAdvisorCheckRefreshStatuses**.

CLI

AWS CLI

Per elencare gli stati di aggiornamento dei controlli di AWS Trusted Advisor

L'esempio `describe-trusted-advisor-check-refresh-statuses` seguente elenca gli stati di aggiornamento per due controlli di Trusted Advisor, ovvero Autorizzazioni bucket di Amazon S3 e Uso IAM.

```
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 Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta AWS CLI Command [DescribeTrustedAdvisorCheckRefreshStatuses](#)Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce lo stato corrente delle richieste di aggiornamento per i controlli specificati. Richiesta- ASATrusted AdvisorCheckRefresh può essere utilizzato per richiedere l'aggiornamento delle informazioni sullo stato dei controlli.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Per i dettagli sull'API, vedere [DescribeTrustedAdvisorCheckRefreshStatuses](#)in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce lo stato corrente delle richieste di aggiornamento per i controlli specificati. Richiesta- ASATrusted AdvisorCheckRefresh può essere utilizzato per richiedere l'aggiornamento delle informazioni sullo stato dei controlli.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Per i dettagli sull'API, vedere [DescribeTrustedAdvisorCheckRefreshStatuses](#)in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **DescribeTrustedAdvisorCheckResult** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Per elencare i risultati di un controllo di AWS Trusted Advisor

L'esempio `describe-trusted-advisor-check-result` seguente elenca i risultati del controllo `Uso IAM`.

```
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 Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeTrustedAdvisorCheckResult AWS CLI Command Reference](#).

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce i risultati di un controllo di Trusted Advisor. L'elenco dei controlli Trusted Advisor disponibili può essere ottenuto utilizzando Get-ASATrustedAdvisorChecks. L'output include lo stato generale del controllo, il timestamp dell'ultimo controllo eseguito e l'ID univoco del 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 Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce i risultati di un controllo di Trusted Advisor. L'elenco dei controlli Trusted Advisor disponibili può essere ottenuto utilizzando Get-ASATrustedAdvisorChecks. L'output include lo stato generale del controllo, il timestamp dell'ultimo controllo eseguito e l'ID univoco del 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 Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **DescribeTrustedAdvisorCheckSummaries** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Per elencare i riepiloghi dei controlli di AWS Trusted Advisor

L'esempio `describe-trusted-advisor-check-summaries` seguente elenca i risultati di due controlli di Trusted Advisor, ovvero Autorizzazioni bucket di Amazon S3 e Uso IAM.

```
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 Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeTrustedAdvisorCheckSummaries AWS CLI](#) Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce il riepilogo più recente del controllo di Trusted Advisor specificato.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Esempio 2: restituisce i riepiloghi più recenti dei controlli di Trusted Advisor specificati.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Per i dettagli sull'API, vedere [DescribeTrustedAdvisorCheckSummaries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce il riepilogo più recente del controllo di Trusted Advisor specificato.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Esempio 2: restituisce i riepiloghi più recenti dei controlli di Trusted Advisor specificati.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @"checkid1", "checkid2")
```

- Per i dettagli sull'API, vedere [DescribeTrustedAdvisorCheckSummaries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **DescribeTrustedAdvisorChecks** con una CLI

Gli esempi di codice seguenti 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 nel tuo AWS account. Queste informazioni includono il nome, l'ID, la descrizione, la categoria e i metadati del controllo. 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 Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [DescribeTrustedAdvisorChecks AWS CLI Command Reference](#).

PowerShell

Strumenti per PowerShell V4

Esempio 1: restituisce la raccolta dei controlli di 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 [DescribeTrustedAdvisorChecks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: restituisce la raccolta dei controlli di 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 [DescribeTrustedAdvisorChecks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **RefreshTrustedAdvisorCheck** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare RefreshTrustedAdvisorCheck.

CLI

AWS CLI

Per aggiornare un controllo di AWS Trusted Advisor

L'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 Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta [RefreshTrustedAdvisorCheck](#) Command Reference.AWS CLI

PowerShell

Strumenti per PowerShell V4

Esempio 1: richiede un aggiornamento del controllo di Trusted Advisor specificato.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Per i dettagli sull'API, vedere [RefreshTrustedAdvisorCheck](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: richiede un aggiornamento del controllo di Trusted Advisor specificato.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Per i dettagli sull'API, vedere [RefreshTrustedAdvisorCheck](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS 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

Gli esempi di codice seguenti 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 nei seguenti esempi di codice:

- [Informazioni di base](#)
- [Guida introduttiva a Support](#)

.NET

SDK per .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 [ResolveCase](#) sezione AWS SDK per .NET API Reference.

CLI

AWS CLI

Come risolvere un caso di supporto

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 [Gestione dei casi](#) nella Guida per l'utente del Supporto AWS .

- Per i dettagli sull'API, consulta AWS CLI Command [ResolveCase](#) 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 [ResolveCase](#) sezione 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 [ResolveCase](#) sezione AWS SDK per 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.fromEnvironment { 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, [ResolveCase](#) consulta AWS SDK for Kotlin API reference.

PowerShell

Strumenti per V4 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 [ResolveCase](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 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 [ResolveCase](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

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 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 AWS](#) SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo Supporto AWS con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari di utilizzo Supporto AWS SDKs

I seguenti esempi di codice mostrano come implementare scenari comuni in Supporto with AWS SDKs. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno Supporto o combinandole con altre Servizi AWS. Ogni scenario include un collegamento al codice sorgente completo, dove è possibile trovare le istruzioni su come configurare ed eseguire il codice.

Gli scenari sono relativi a un livello intermedio di esperienza per aiutarti a comprendere le azioni di servizio nel contesto.

Esempi

- [Guida introduttiva a Support](#)

Guida introduttiva a Support

L'esempio di codice seguente mostra come:

- Verifica i servizi disponibili e i livelli di gravità
- Creazione di un caso di supporto
- Aggiungi comunicazioni a un caso

Bash

AWS CLI con lo script Bash

Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri come eseguire la configurazione e l'esecuzione nel [repository dei tutorial sugli esempi di codice per gli sviluppatori](#).

```
#!/bin/bash

# AWS Support CLI Tutorial Script
# This script demonstrates how to use AWS Support API through AWS CLI

# Set up logging
LOG_FILE="aws-support-tutorial.log"
echo "Starting AWS Support Tutorial at $(date)" > "$LOG_FILE"

# Function to log commands and their outputs
log_cmd() {
    echo "$(date): Running command: $1" >> "$LOG_FILE"
    eval "$1" 2>&1 | tee -a "$LOG_FILE"
    return ${PIPESTATUS[0]}
}

# Function to check for errors in command output
check_error() {
    local cmd_output="$1"
    local cmd_status="$2"
    local error_msg="$3"
    local is_fatal="${4:-true}"

    if [[ $cmd_status -ne 0 || "$cmd_output" =~ [Ee][Rr][Rr][Oo][Rr] ]]; then
        echo "ERROR: $error_msg" | tee -a "$LOG_FILE"
        echo "Command output: $cmd_output" | tee -a "$LOG_FILE"

        # Check for subscription error
        if [[ "$cmd_output" =~ "SubscriptionRequiredException" ]]; then
            echo "" | tee -a "$LOG_FILE"
        fi
    fi
}
```

```

        echo "===== " | tee -a
"$LOG_FILE"
        echo "IMPORTANT: This account does not have the required AWS Support
plan." | tee -a "$LOG_FILE"
        echo "You need a Business, Enterprise On-Ramp, or Enterprise Support
plan" | tee -a "$LOG_FILE"
        echo "to use the AWS Support API." | tee -a "$LOG_FILE"
        echo "" | tee -a "$LOG_FILE"
        echo "This script will now demonstrate the commands that would be
run" | tee -a "$LOG_FILE"
        echo "if you had the appropriate support plan, but will not execute
them." | tee -a "$LOG_FILE"
        echo "===== " | tee -a
"$LOG_FILE"

        # Switch to demo mode
        DEMO_MODE=true
        return 0
    fi

    if [[ "$is_fatal" == "true" ]]; then
        cleanup_resources
        exit 1
    fi
fi

}

# Function to clean up resources
cleanup_resources() {
    echo "No persistent resources were created that need cleanup." | tee -a
"$LOG_FILE"
}

# Function to run a command in demo mode
demo_cmd() {
    local cmd="$1"
    local description="$2"

    echo "" | tee -a "$LOG_FILE"
    echo "DEMO: $description" | tee -a "$LOG_FILE"
    echo "Command that would be executed:" | tee -a "$LOG_FILE"
    echo "$cmd" | tee -a "$LOG_FILE"
    echo "" | tee -a "$LOG_FILE"
}

```

```
# Array to track created resources
declare -a CREATED_RESOURCES

# Initialize demo mode flag
DEMO_MODE=false

echo "=====
echo "AWS Support CLI Tutorial"
echo "=====
echo "This script demonstrates how to use AWS Support API"
echo "Note: You must have a Business, Enterprise On-Ramp,"
echo "or Enterprise Support plan to use the AWS Support API."
echo "=====
echo ""

# Step 1: Check available services
echo "Step 1: Checking available AWS Support services..."
SERVICES_OUTPUT=$(log_cmd "aws support describe-services --language en")
check_error "$SERVICES_OUTPUT" $? "Failed to retrieve AWS Support services"

# If we're in demo mode, set default values
if [[ "$DEMO_MODE" == "true" ]]; then
    SERVICE_CODE="general-info"
    echo "Using demo service code: $SERVICE_CODE" | tee -a "$LOG_FILE"
else
    # Extract a service code for demonstration
    SERVICE_CODE=$(echo "$SERVICES_OUTPUT" | grep -o '"code": "[^"]*"' | head -1
    | cut -d'"' -f4)
    if [[ -z "$SERVICE_CODE" ]]; then
        SERVICE_CODE="general-info"
        echo "Using default service code: $SERVICE_CODE" | tee -a "$LOG_FILE"
    else
        echo "Found service code: $SERVICE_CODE" | tee -a "$LOG_FILE"
    fi
fi

# Step 2: Check available severity levels
echo "Step 2: Checking available severity levels..."
if [[ "$DEMO_MODE" == "true" ]]; then
    demo_cmd "aws support describe-severity-levels --language en" "Check
    available severity levels"
    SEVERITY_CODE="low"
    echo "Using demo severity code: $SEVERITY_CODE" | tee -a "$LOG_FILE"
```

```

else
    SEVERITY_OUTPUT=$(log_cmd "aws support describe-severity-levels --language
en")
    check_error "$SEVERITY_OUTPUT" $? "Failed to retrieve severity levels"

    # Extract a severity code for demonstration
    SEVERITY_CODE=$(echo "$SEVERITY_OUTPUT" | grep -o '"code": "[^"]*"' | head -1
| cut -d'"' -f4)
    if [[ -z "$SEVERITY_CODE" ]]; then
        SEVERITY_CODE="low"
        echo "Using default severity code: $SEVERITY_CODE" | tee -a "$LOG_FILE"
    else
        echo "Found severity code: $SEVERITY_CODE" | tee -a "$LOG_FILE"
    fi
fi

# Step 3: Create a test support case
echo ""
echo "=====
echo "SUPPORT CASE CREATION"
echo "=====
if [[ "$DEMO_MODE" == "true" ]]; then
    echo "DEMO MODE: The following steps would create and manage a support case"
    echo "if you had a Business, Enterprise On-Ramp, or Enterprise Support plan."
    echo ""

    # Get user email for demo
    echo "Enter your email address for the demo (leave blank to use
example@example.com): "
    read -r USER_EMAIL

    if [[ -z "$USER_EMAIL" ]]; then
        USER_EMAIL="example@example.com"
    fi

    # Demo create case command
    demo_cmd "aws support create-case \
        --subject \"AWS CLI Tutorial Test Case\" \
        --service-code \"$SERVICE_CODE\" \
        --category-code \"using-aws\" \
        --communication-body \"This is a test case created as part of an AWS CLI
tutorial.\" \
        --severity-code \"$SEVERITY_CODE\" \
        --language \"en\" \

```

```

        --cc-email-addresses \"${USER_EMAIL}\" \"Create a support case\"

# Use a fake case ID for demo
CASE_ID=\"case-12345678910-2013-c4c1d2bf33c5cf47\"
echo \"Demo case ID: $CASE_ID\" | tee -a \"$LOG_FILE\"

# Demo list cases command
demo_cmd \"aws support describe-cases \
    --case-id-list \"${CASE_ID}\" \
    --include-resolved-cases false \
    --language \"en\" \"List support cases\"

# Demo add communication command
demo_cmd \"aws support add-communication-to-case \
    --case-id \"${CASE_ID}\" \
    --communication-body \"This is an additional communication for the test
case.\" \
    --cc-email-addresses \"${USER_EMAIL}\" \"Add communication to case\"

# Demo view communications command
demo_cmd \"aws support describe-communications \
    --case-id \"${CASE_ID}\" \
    --language \"en\" \"View case communications\"

# Demo resolve case command
demo_cmd \"aws support resolve-case \
    --case-id \"${CASE_ID}\" \"Resolve the support case\"

else
    echo \"This will create a test support case in your account.\"
    echo \"Do you want to continue? (y/n): \"
    read -r CREATE_CASE_CHOICE

    if [[ \"$CREATE_CASE_CHOICE\" =~ ^[Yy]$ ]]; then
        echo \"Creating a test support case...\"

        # Get user email for CC
        echo \"Enter your email address for case notifications (leave blank to
skip): \"
        read -r USER_EMAIL

        CC_EMAIL_PARAM=\"\"
        if [[ -n \"$USER_EMAIL\" ]]; then
            CC_EMAIL_PARAM=\"--cc-email-addresses $USER_EMAIL\"

```

```

fi

# Create the case
CASE_OUTPUT=$(log_cmd "aws support create-case \
  --subject \"AWS CLI Tutorial Test Case\" \
  --service-code \"$SERVICE_CODE\" \
  --category-code \"using-aws\" \
  --communication-body \"This is a test case created as part of an AWS
CLI tutorial.\" \
  --severity-code \"$SEVERITY_CODE\" \
  --language \"en\" \
  $CC_EMAIL_PARAM")

check_error "$CASE_OUTPUT" $? "Failed to create support case"

# Extract the case ID
CASE_ID=$(echo "$CASE_OUTPUT" | grep -o '"caseId": "[^"]*"' | cut -d'"' -
f4)

if [[ -n "$CASE_ID" ]]; then
  echo "Successfully created support case with ID: $CASE_ID" | tee -a
"$LOG_FILE"
  CREATED_RESOURCES+=("Support Case: $CASE_ID")

# Step 4: List the case we just created
echo ""
echo "Step 4: Listing the support case we just created..."
CASES_OUTPUT=$(log_cmd "aws support describe-cases \
  --case-id-list \"$CASE_ID\" \
  --include-resolved-cases false \
  --language \"en\"")

check_error "$CASES_OUTPUT" $? "Failed to retrieve case details"

# Step 5: Add a communication to the case
echo ""
echo "Step 5: Adding a communication to the support case..."
COMM_OUTPUT=$(log_cmd "aws support add-communication-to-case \
  --case-id \"$CASE_ID\" \
  --communication-body \"This is an additional communication for
the test case.\" \
  $CC_EMAIL_PARAM")

check_error "$COMM_OUTPUT" $? "Failed to add communication to case"

```

```

# Step 6: View communications for the case
echo ""
echo "Step 6: Viewing communications for the support case..."
COMMS_OUTPUT=$(log_cmd "aws support describe-communications \
    --case-id \"$CASE_ID\" \
    --language \"en\"")

check_error "$COMMS_OUTPUT" $? "Failed to retrieve case
communications"

# Step 7: Resolve the case
echo ""
echo "====="
echo "CASE RESOLUTION"
echo "====="
echo "Do you want to resolve the test support case? (y/n): "
read -r RESOLVE_CASE_CHOICE

if [[ "$RESOLVE_CASE_CHOICE" =~ ^[Yy]$ ]]; then
    echo "Resolving the support case..."
    RESOLVE_OUTPUT=$(log_cmd "aws support resolve-case \
        --case-id \"$CASE_ID\"")

    check_error "$RESOLVE_OUTPUT" $? "Failed to resolve case"
    echo "Successfully resolved support case: $CASE_ID" | tee -a
"$LOG_FILE"
else
    echo "Skipping case resolution. The case will remain open." | tee
-a "$LOG_FILE"
fi
else
    echo "Could not extract case ID from the response." | tee -a
"$LOG_FILE"
fi
else
    echo "Skipping support case creation." | tee -a "$LOG_FILE"
fi
fi

# Display summary of created resources
echo ""
echo "====="
echo "TUTORIAL SUMMARY"

```

```
echo "=====
if [[ "$DEMO_MODE" == "true" ]]; then
    echo "This was a demonstration in DEMO MODE."
    echo "No actual AWS Support cases were created."
    echo "To use the AWS Support API, you need a Business, Enterprise On-Ramp,"
    echo "or Enterprise Support plan."
else
    echo "Resources created during this tutorial:"
    if [[ ${#CREATED_RESOURCES[@]} -eq 0 ]]; then
        echo "No resources were created."
    else
        for resource in "${CREATED_RESOURCES[@}"; do
            echo "- $resource"
        done
    fi
fi

echo ""
echo "Tutorial completed successfully!"
echo "Log file: $LOG_FILE"
echo "=====
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dei comandi della AWS CLI .
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo Supporto AWS con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Monitoraggio e registrazione per Supporto AWS

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle Supporto altre AWS soluzioni esistenti. AWS fornisce i seguenti strumenti di monitoraggio per osservare Supporto, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

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

Argomenti

- [Integrazione Supporto AWS in applicazioni basate sugli eventi tramite Amazon EventBridge](#)
- [Registrazione delle chiamate Supporto AWS API con AWS CloudTrail](#)
- [Registrazione Supporto AWS dell'app nelle chiamate dell'API Slack utilizzando AWS CloudTrail](#)

Integrazione Supporto AWS in applicazioni basate sugli eventi tramite Amazon EventBridge

È possibile Supporto AWS incorporarle in applicazioni basate sugli eventi (EDAs) che utilizzano eventi che si verificano in Supporto AWS per comunicare tra i componenti dell'applicazione e avviare processi a valle.

Ad esempio, puoi ricevere una notifica ogni volta che si verificano i seguenti Supporto AWS eventi nel tuo account:

- Viene creato, risolto o riaperto un caso di assistenza
- Una corrispondenza viene aggiunta a un caso di supporto esistente

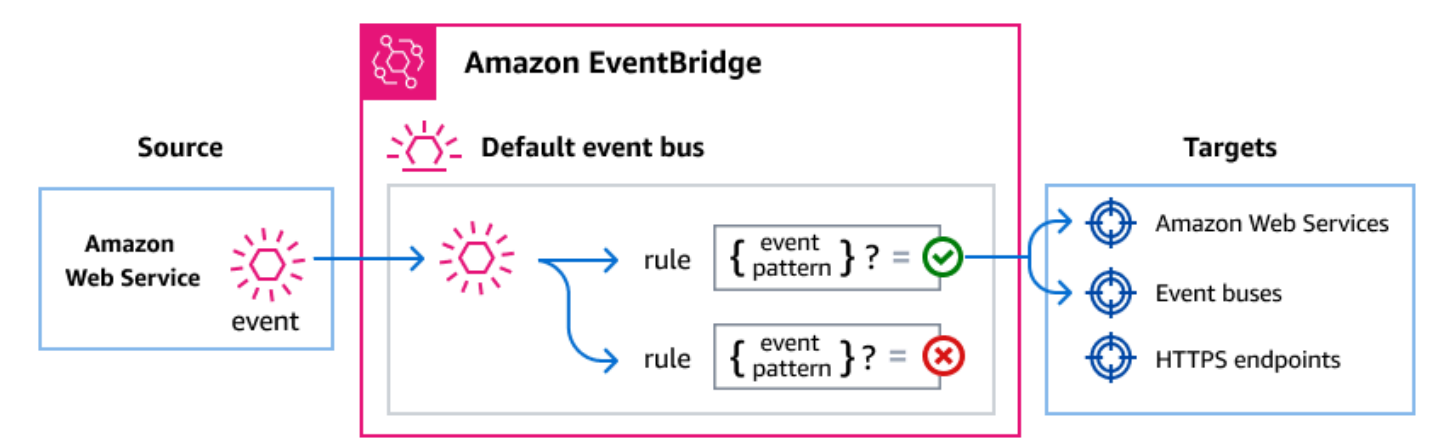
A tale scopo, puoi utilizzare Amazon EventBridge per indirizzare gli eventi da Supporto AWS altri componenti software. Amazon EventBridge è un servizio serverless che utilizza gli eventi per connettere tra loro i componenti delle applicazioni, semplificando l'integrazione AWS dei servizi, ad esempio Supporto AWS in architetture basate sugli eventi, senza codice e operazioni aggiuntivi.

Come indirizza gli eventi EventBridge Supporto AWS

Ecco come EventBridge funziona con Supporto AWS gli eventi:

Come molti AWS servizi, Supporto AWS genera e invia eventi al bus eventi EventBridge predefinito. Un bus di eventi è un router che riceve gli eventi e li indirizza verso le destinazioni, o destinazioni, specificate dall'utente. Gli obiettivi possono includere altri AWS servizi, applicazioni personalizzate e applicazioni partner SaaS.

EventBridge indirizza gli eventi in base alle regole create sull'event bus. Per ogni regola, specificate un filtro, o modello di eventi, per selezionare solo gli eventi desiderati. Ogni volta che un evento viene inviato al bus degli eventi, lo EventBridge confronta con ogni regola. Se l'evento corrisponde alla regola, EventBridge indirizza l'evento ai target specificati.



Supporto AWS eventi

Supporto AWS invia automaticamente i seguenti eventi al bus EventBridge eventi predefinito.

Tipo di dettaglio dell'evento	Description
Support Case Update	Rappresenta una modifica in un caso di supporto.

Struttura degli eventi

Tutti gli eventi dei AWS servizi contengono due tipi di dati:

- Un insieme comune di campi contenenti metadati sull'evento, ad esempio il AWS servizio che è l'origine dell'evento, l'ora in cui l'evento è stato generato, l'account e la regione in cui si è verificato l'evento e altri. Per le definizioni di questi campi generali, consulta la [struttura degli eventi](#) in Amazon EventBridge Events Reference.
- Un `detail` campo che contiene dati specifici per quel particolare evento di servizio.

Supporto AWS consegna dell'evento tramite AWS CloudTrail

AWS i servizi possono inviare eventi direttamente al bus eventi EventBridge predefinito. Inoltre, AWS CloudTrail invia anche eventi provenienti da numerosi AWS servizi. EventBridge Questi eventi possono includere chiamate API, accessi e azioni alla console, eventi di servizio e CloudTrail Insights. Per ulteriori informazioni, consulta [gli eventi AWS di servizio forniti tramite AWS CloudTrail](#) nella Guida per l'EventBridge utente.

Per un elenco degli Supporto AWS eventi inviati a EventBridge, consultate l' Supporto AWS argomento nella [Guida EventBridge agli eventi](#).

Creazione di modelli di eventi che corrispondano Supporto AWS agli eventi

I modelli di eventi sono filtri che consentono di specificare i dati che devono contenere gli eventi che si desidera selezionare.

Ogni modello di eventi è un oggetto in formato JSON che contiene:

- Un attributo `source` che identifica il servizio che invia l'evento. Per Supporto AWS gli eventi, la fonte è `aws.support`.
- (Facoltativo): Un `detail-type` attributo che contiene una matrice dei nomi degli eventi da abbinare.
- (Facoltativo): Un attributo `detail` contenente qualsiasi altro dato relativo all'evento da abbinare.

Ad esempio, il seguente schema di eventi selezionerebbe tutti gli eventi Support Case Update da Supporto AWS:

```
{
```

```
"source": ["aws.support"],
"detail-type": ["Support Case Update"]
}
```

È possibile specificare meglio la selezione degli eventi includendo dei valori nell'evento stesso. Ad esempio, il seguente modello di eventi corrisponde agli eventi Support Case Update che rappresentano la riapertura di un caso:

```
{
  "source": ["aws.support"],
  "detail-type": ["Support Case Update"],
  "detail": {
    "event-name": "ReopenCase"
  }
}
```

Per ulteriori informazioni sulla scrittura di modelli di eventi, consultate [Event patterns](#) nella Guida per l'EventBridge utente.

Consulta anche

Per ulteriori informazioni su come utilizzare EventBridge con Supporto AWS, consultate le seguenti risorse:

- [Come automatizzare le Supporto AWS API con Amazon EventBridge](#)
- [Supporto AWS case activity notificador attivo](#) GitHub

Evento Support Case Update

Di seguito sono riportati i campi di dettaglio dell'Support Case Update evento.

I `detail-type` campi `source` e sono inclusi di seguito perché contengono valori specifici per Supporto AWS gli eventi. Per le definizioni degli altri campi di metadati inclusi in tutti gli eventi, consulta la [struttura degli eventi in Amazon EventBridge Events](#) Reference.

```
{
  . . . ,
  "detail-type": "Support Case Update",
  "source": "aws.support",
```

```
. . .,  
"detail": {  
  "case-id" : "string",  
  "display-id" : "string",  
  "communication-id" : "string",  
  "event-name" : "string",  
  "origin" : "string"  
}  
}
```

detail-type

Identifica il tipo di evento.

Per questo evento, questo valore è `Support Case Update`.

source

Identifica il servizio che ha generato l'evento. Per Supporto AWS gli eventi, questo valore è `aws.support`.

detail

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per questo evento, questi dati includono:

case-id

L'ID del caso di supporto. L'ID del caso è una stringa alfanumerica nel seguente formato: `case-12345678910-2013-c4c1d2bf33c5cf47`.

display-id

L'identificatore Supporto AWS del caso nelle pagine del Centro.

communication-id

L'ID di comunicazione.

event-name

Valori validi: `CreateCase` | `AddCommunicationToCase` | `ResolveCase` | `ReopenCase`

Specifica il tipo di evento relativo alla richiesta di assistenza.

origin

Valori validi: AWS | CUSTOMER

Specifica se l'utente o un Supporto AWS agente ha aggiunto una corrispondenza tra un caso a un caso di supporto.

Attualmente, solo gli eventi con un o event-name AddCommunicationToCase conterranno questo valore.

Example Esempio di evento Support Case Update: richiesta di assistenza creata

```
{
  "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 Esempio di evento Support Case Update: Supporto AWS 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 Esempio di evento Support Case Update: caso di supporto risolto

```
{
  "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 Esempio di evento Support Case Update: richiesta di assistenza riaperta

```
{
  "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": ""  
  }  
}
```

Registrazione delle chiamate Supporto AWS API con AWS CloudTrail

Supporto AWS è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Supporto AWS. CloudTrail acquisisce le chiamate API Supporto AWS come eventi. Le chiamate acquisite includono chiamate dalla Supporto AWS console e chiamate di codice alle operazioni Supporto AWS API.

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. Supporto AWS 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 Supporto AWS, 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](#).

Supporto AWS informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in Supporto AWS, 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 cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di Supporto AWS, 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 log CloudTrail da più regioni](#) e [Ricezione di file di log CloudTrail da più account](#)

[Tutte le operazioni Supporto AWS API vengono registrate CloudTrail e documentate nell'API Reference.Supporto AWS](#)

Ad esempio, le chiamate alle CreateCase ResolveCase operazioni DescribeCases e generano voci nei file di CloudTrail registro.

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, consulta [Elemento CloudTrail userIdentity](#).

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

AWS Trusted Advisor informazioni relative alla registrazione CloudTrail

Trusted Advisor è un Supporto AWS servizio che consente di controllare il AWS proprio account alla ricerca di modi per risparmiare sui costi, migliorare la sicurezza e ottimizzare l'account.

Tutte le operazioni Trusted Advisor API vengono registrate CloudTrail e sono documentate nell'[Supporto AWS API](#) Reference.

Ad esempio, le chiamate alle `DescribeTrustedAdvisorCheckRefreshStatuses` `RefreshTrustedAdvisorCheck` operazioni `DescribeTrustedAdvisorCheckResult` e generano voci nei file di CloudTrail registro.

Note

CloudTrail registra anche le azioni Trusted Advisor della console. Per informazioni, consulta [Registrazione delle azioni AWS Trusted Advisor della console con AWS CloudTrail](#).

Comprensione delle Supporto AWS voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta 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: Inserimento del registro per `CreateCase`

L'esempio seguente mostra una voce di CloudTrail registro relativa all'[CreateCase](#) operazione.

```
{
  "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 registro per RefreshTrustedAdvisorCheck

L'esempio seguente mostra una voce di CloudTrail registro relativa all'[RefreshTrustedAdvisorCheck](#) operazione.

```

{
  "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 Supporto AWS dell'app nelle chiamate dell'API Slack utilizzando AWS CloudTrail

L' Supporto AWS app in Slack è integrata con. AWS CloudTrail CloudTrail fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS nell' Supporto AWS App. Per creare questo record, CloudTrail acquisisce tutte le chiamate API pubbliche per Supporto AWS l'App come eventi. Queste chiamate acquisite includono le chiamate dalla console dell' Supporto AWS App e le chiamate in codice alle operazioni dell'API pubblica Supporto AWS dell'App. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3. Questi includono eventi per Supporto AWS App. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Puoi utilizzare le informazioni CloudTrail raccolte per determinare la richiesta che è stata fatta ad Supporto AWS App. 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 CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#).

Supporto AWS Informazioni sull'app in CloudTrail

Quando crei il tuo Account AWS, questo si attiva CloudTrail sull'account. Quando si verifica un'attività API pubblica nell' Supporto AWS App, tale attività viene registrata in un CloudTrail evento, insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nella tua app Account AWS, inclusi gli eventi per Supporto AWS App, crea un percorso. 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 configurarne altri Servizi AWS per analizzare ulteriormente i dati sugli eventi raccolti nei CloudTrail log e agire in base ai dati. 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](#)

CloudTrail registra tutte le azioni pubbliche Supporto AWS dell'app. Queste operazioni sono documentate anche nella [documentazione di riferimento sull'API dell'app Supporto AWS in Slack](#). Ad esempio, le chiamate a `GetAccountAlias` e `UpdateSlackChannelConfiguration` le azioni generano voci nei file di CloudTrail registro. `CreateSlackChannelConfiguration`

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](#).

Comprensione delle Supporto AWS voci dei file di registro dell'app

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. 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 CloudTrail registro per l'[CreateSlackChannelConfiguration](#) operazione.

```
{
  "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-c233-4fffb-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 CloudTrail registro per l'[ListSlackChannelConfigurations](#) operazione.

```
{
  "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 CloudTrail registro per l'[GetAccountAlias](#) operazione.

```

{
  "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 Supporto AWS

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni dei Support Plans e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare i piani di supporto, segnalare quando qualcosa non va e intraprendere azioni automatiche quando appropriato:

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

Argomenti

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

Registrazione delle chiamate API Supporto AWS Plans con AWS CloudTrail

Supporto AWS Plans è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce le chiamate API per Supporto AWS i piani come eventi. Le chiamate acquisite includono chiamate dalla console Supporto AWS Plans e chiamate in codice alle operazioni dell'API Supporto AWS Plans.

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 Plans. Supporto AWS 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 Supporto AWS Plans, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

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

Supporto AWS Informazioni sui piani in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività di evento supportata in Supporto AWS Plans, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account . Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo account, inclusi gli eventi per Supporto AWS Plans, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo 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 configurarne altri Servizi AWS 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 log CloudTrail da più regioni](#) e [Ricezione di file di log CloudTrail da più account](#)

Tutte le operazioni dell'API Supporto AWS Plans 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 Servizio AWS.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Puoi anche aggregare i file di log di Supporto AWS Plans da più o Regioni AWS più account in un unico bucket Amazon S3.

Informazioni sulle voci dei file di registro Supporto AWS di Plans

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 GetSupportPlan

L'esempio seguente mostra una voce di CloudTrail registro per l'GetSupportPlanoperazione.

```
{
  "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 CloudTrail registro per l'GetSupportPlanUpdateStatusoperazione.

```

{
  "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 CloudTrail registro per l'StartSupportPlanUpdate operazione.

```

{
  "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 CloudTrail registro per l>CreateSupportPlanScheduleoperazione.

```

{
  "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"  
}
```

Example: voce di registro per ListSupportPlanModifiers

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

```
{  
  "eventVersion": "1.09",  
  "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:sts::111122223333:user/janedoe",  
        "accountId": "111122223333",  
        "userName": "Admin"  
      },  
      "attributes": {  
        "creationDate": "2024-08-15T15:44:43Z",  
        "mfaAuthenticated": "false"  
      }  
    },  
  },  
  "eventTime": "2024-08-15T16:29:59Z",  
  "eventSource": "supportplans.amazonaws.com",  
  "eventName": "ListSupportPlanModifiers",  
  "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"  
}
```

Registrazione delle modifiche al piano Supporto

Important

A partire dal 3 agosto 2022, le seguenti operazioni sono obsolete e non verranno visualizzate nei nuovi registri. CloudTrail Per un elenco delle operazioni supportate, consulta [Informazioni sulle voci dei file di registro Supporto AWS di Plans](#).

- `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: Inserimento del registro per `DescribeSupportLevelSummary`

L'esempio seguente mostra una voce di CloudTrail registro per l'`DescribeSupportLevelSummary` azione.

```
{
```

```

"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 UpdateProbationAutoCancellation

L'esempio seguente mostra una voce di CloudTrail registro per l'UpdateProbationAutoCancellationazione.

```

{
  "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 CloudTrail registro per l'UpdateSupportLevelazione da passare a Developer Support.

```

{
  "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 registrazione per AWS Trusted Advisor

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

- 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.

Ad esempio, Trusted Advisor fornisce il controllo delle autorizzazioni dei bucket di Amazon S3. Questo controllo identifica se sono presenti bucket con autorizzazioni di accesso aperto o che consentono l'accesso a qualsiasi utente autenticato. AWS Se l'autorizzazione di un bucket cambia, lo stato del controllo cambia. Trusted Advisor EventBridge rileva questo evento e quindi ti invia una notifica in modo che tu possa intervenire. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

- AWS Trusted Advisor i controlli identificano modi per ridurre i costi, aumentare le prestazioni e migliorare la sicurezza del tuo AWS account. È possibile utilizzarli EventBridge per monitorare lo stato dei Trusted Advisor controlli. Puoi quindi utilizzare Amazon CloudWatch per creare allarmi sui Trusted Advisor parametri. Questi allarmi ti avvisano quando cambia lo stato di un Trusted Advisor controllo, ad esempio quando viene raggiunta una risorsa aggiornata o una quota di servizio.
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la [Guida per l'utente AWS CloudTrail](#).

Argomenti

- [Monitoraggio dei risultati dei AWS Trusted Advisor controlli con Amazon EventBridge](#)
- [Creazione di CloudWatch allarmi Amazon per monitorare i parametri AWS Trusted Advisor](#)
- [Registrazione delle azioni AWS Trusted Advisor della console con AWS CloudTrail](#)

Monitoraggio dei risultati dei AWS Trusted Advisor controlli con Amazon EventBridge

Important

Avviso di fine del supporto: il supporto per gli sviluppatori verrà interrotto il 1° gennaio 2027. I clienti con Developer Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il supporto aziendale verrà interrotto il 1° gennaio 2027. I clienti con Business Support possono continuare a utilizzare il piano esistente o scegliere di passare a Business Support+ in qualsiasi momento prima del 1° gennaio 2027. Business Support+ offre assistenza basata sull'intelligenza artificiale che comprende il contesto delle tue operazioni, con accesso 24 ore su 24, 7 giorni su 7 agli AWS esperti a un minimo di 29 dollari al mese per account. Per ulteriori informazioni, consulta i dettagli del [piano Business Support+](#)

Avviso di fine del supporto: il 1° gennaio 2027, Enterprise AWS On-Ramp interromperà. Nel corso del 2026, i clienti Enterprise On-Ramp verranno automaticamente aggiornati a Enterprise AWS Support durante il rinnovo del contratto o in batch periodici. I clienti riceveranno una notifica via e-mail un mese prima dell'aggiornamento. Non è richiesta alcuna operazione aggiuntiva. Enterprise Support fornisce l'assegnazione TAM designata, tempi di risposta di 15 minuti ed AWS Security Incident Response è disponibile senza costi aggiuntivi, il tutto a un minimo inferiore di 5.000 dollari (invece di 15.000 dollari). [Per ulteriori informazioni, consulta i dettagli del piano Enterprise.AWSSupporto](#)

Per ulteriori informazioni, consulta [Fine del supporto On-Ramp per sviluppatori, Business ed Enterprise](#).

Developer Support, Business Support ed Enterprise On-Ramp rimarranno disponibili nella AWS GovCloud (US) regione.

Puoi utilizzarlo 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).

- Usa una AWS Lambda funzione per passare 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 risposte Trusted Advisor, consulta Trusted Advisor gli strumenti in.](#) GitHub

Note

- Trusted Advisor organizza eventi con il massimo impegno possibile. Non è sempre garantito che gli eventi vengano consegnati a EventBridge.
- È necessario disporre di un piano AWS Business Support+, AWS Enterprise Support o AWS Unified Operations per creare una regola per i Trusted Advisor controlli. Per ulteriori informazioni, consulta [Piani di modifica Supporto AWS](#).
-
- Trusted Advisor Trattandosi 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. Mantieni 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 AWS eventi o eventi EventBridge partner.
8. Nel Modello di eventi, mantieni 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.
 - ERRORE: Trusted Advisor consiglia un'azione per il controllo.
 - INFORMAZIONI: Trusted Advisor impossibile determinare lo stato del controllo.
 - OK: Trusted Advisor non rileva alcun problema per il controllo.
 - AVVISO: Trusted Advisor rileva un possibile problema durante il controllo e consiglia 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. Scegliete una delle seguenti opzioni per AWS le risorse:
 - Scegli Any resource ID (Qualsiasi ID della risorsa) per creare una regola che monitora tutte le risorse.
 - Scegli ID di risorsa specifici in base all'ARN, quindi inserisci i nomi di risorsa Amazon (ARNs) che desideri.
14. Scegli Next (Successivo).

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. Scegli Next (Successivo).
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 Trusted Advisor controlli e quindi invierà l'evento all'obiettivo che hai specificato.

Creazione di CloudWatch allarmi Amazon per monitorare i parametri AWS Trusted Advisor

Quando AWS Trusted Advisor aggiorna i controlli, Trusted Advisor pubblica le metriche relative ai risultati del controllo su CloudWatch. Puoi visualizzare i parametri in CloudWatch. È inoltre possibile creare allarmi per rilevare le modifiche allo stato dei Trusted Advisor controlli e delle modifiche allo stato delle risorse e l'utilizzo delle quote di servizio (in precedenza denominate limiti).

Segui questa procedura per creare un CloudWatch allarme per una metrica specifica. Trusted Advisor

Argomenti

- [Prerequisiti](#)
- [CloudWatch metriche per Trusted Advisor](#)
- [Trusted Advisor metriche e dimensioni](#)

Prerequisiti

Prima di creare CloudWatch allarmi per le Trusted Advisor metriche, consulta le seguenti informazioni:

- Scopri come CloudWatch utilizza metriche e allarmi. Per ulteriori informazioni, consulta [How CloudWatch works](#) nella Amazon CloudWatch User Guide.
- Usa la Trusted Advisor console o l' API Supporto AWS per aggiornare i controlli e ottenere gli ultimi risultati dei controlli. Per ulteriori informazioni, consulta [Aggiorna i risultati di controllo](#).

Per creare un CloudWatch allarme per le metriche Trusted Advisor

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Usa il selettore della regione e scegli la regione Stati Uniti orientali (Virginia settentrionale) AWS .
3. Nel pannello di navigazione, seleziona Alarms (Allarmi).
4. Scegli Crea allarme.
5. Scegli Seleziona metrica.
6. Per Parametri, inserisci uno o più valori relativi alle dimensioni per filtrare l'elenco di parametri. Ad esempio, puoi inserire il nome della metrica ServiceLimitUsageo la dimensione, ad esempio il nome dell' Trusted Advisor assegno.

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 [Trusted Advisor metriche e dimensioni](#).

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 e il nome della metrica è. YellowResources

N. Virginia ▾		All > TrustedAdvisor > Check Metrics		Trusted ✕	Advisor ✕	IAM ✕	Access ✕	Key ✕
☐	CheckName (2)	Metric Name						
☐	IAM Access Key Rotation	RedResources						
☒	IAM Access Key Rotation	YellowResources						

8. Scegli Seleziona metrica.
9. Nella pagina Specificare la metrica e le condizioni, verifica che il nome della metrica e CheckNamequello che hai scelto compaiano nella 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 $\geq$ threshold (Maggiore/Uguale $\geq$ 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 le YellowResourcesmetriche GreenChecksRedChecksYellowChecks, RedResources,, e puoi specificare una soglia che è qualsiasi numero intero maggiore o uguale a zero.
- Trusted Advisor non invia metriche per GreenResources, che sono risorse per le quali non Trusted Advisor ha rilevato alcun problema.

12. Scegli Next (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.

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ **In alarm**
The metric or expression is outside of the defined threshold.

☐ **OK**
The metric or expression is within the defined threshold.

☐ **Insufficient data**
The alarm has just started or not enough data is available.

Remove

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ **Select an existing SNS topic**

☐ Create new topic

☐ Use topic ARN

Send a notification to...

Q Default_CloudWatch_Alarms_Topic X

Only email lists for this account are available.

Email (endpoints)

janedoe@example.com - [View in SNS Console](#)

Add notification

15. Scegli Next (Successivo).
16. Per Name and description (Nome e descrizione), inserisci un nome e una descrizione per il tuo allarme.
17. Scegli Next (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 "IAMAccessKeyRotationCheckAlarm" 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 Console di gestione AWS:

<https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#s=Alarms&alarm=IAMAccessKeyRotationCheckAlarm>

Alarm Details:

- Name: IAMAccessKeyRotationCheckAlarm
- 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:IAMAccessKeyRotationCheckAlarm

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:

CloudWatch metriche per Trusted Advisor

Puoi usare la CloudWatch console o il AWS Command Line Interface (AWS CLI) per trovare le metriche disponibili per. Trusted Advisor

Per un elenco dei namespace, delle metriche e delle dimensioni per tutti i servizi che pubblicano metriche, consulta i servizi che pubblicano [metriche CloudWatch nella AWS Amazon](#) User Guide. CloudWatch

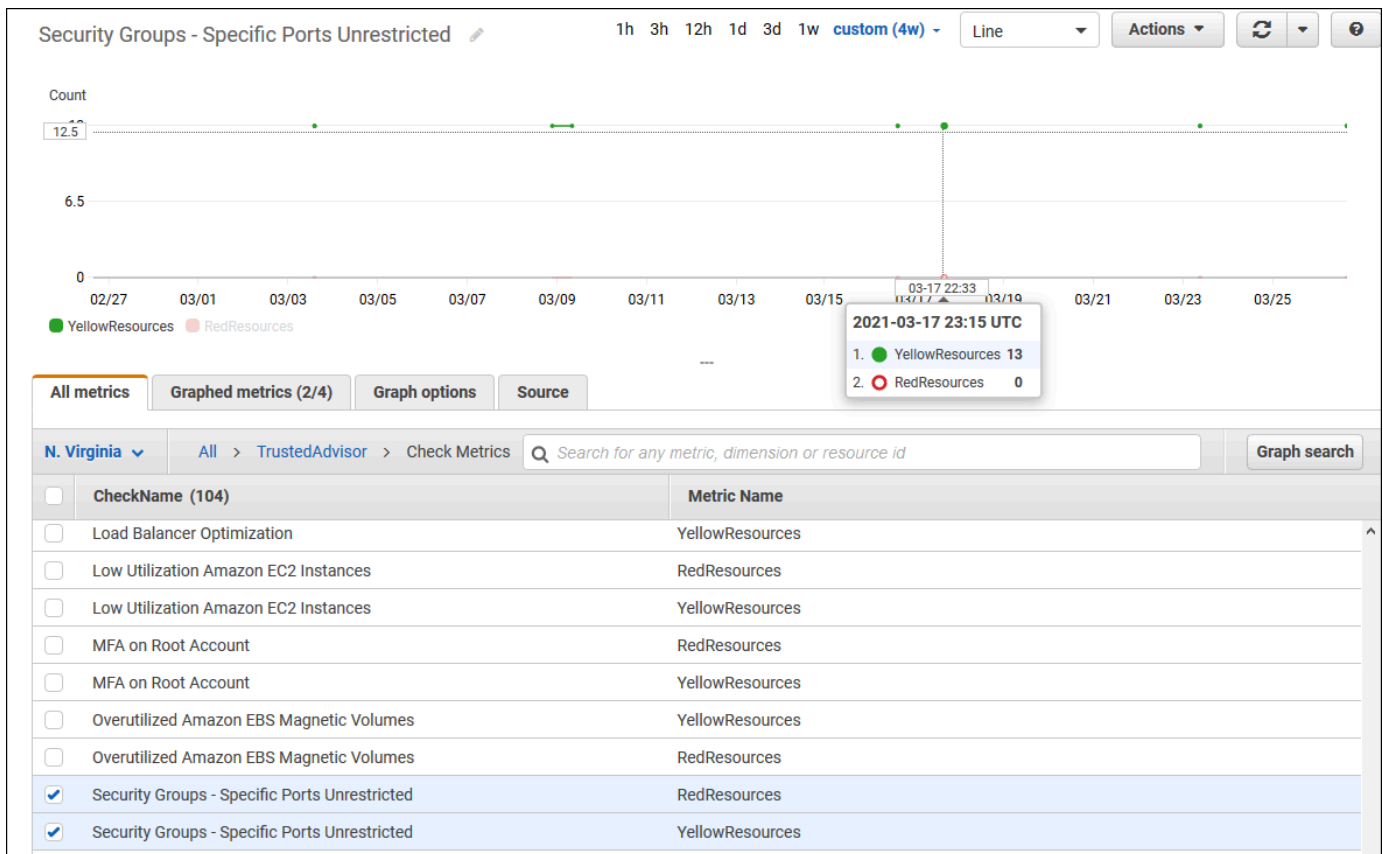
Visualizza i parametri (console) Trusted Advisor

Puoi accedere alla CloudWatch console e visualizzare le metriche disponibili per. Trusted Advisor

Per visualizzare le Trusted Advisor metriche disponibili (console)

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Usa il selettore della regione e scegli la regione Stati Uniti orientali (Virginia settentrionale) AWS .
3. Nel riquadro di navigazione, seleziona 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 fare quanto segue:
 - 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 segno di spunta identifica 13 risorse di colore giallo. Trusted Advisor consiglia di esaminare gli assegni gialli.



7. (Facoltativo) Per aggiungere questo grafico a una CloudWatch dashboard, scegli Azioni, quindi scegli Aggiungi alla dashboard.

Per ulteriori informazioni sulla creazione di un grafico per visualizzare le tue metriche, consulta [Graphing a metric](#) nella Amazon CloudWatch User Guide.

Visualizza le Trusted Advisor metriche (CLI)

È possibile utilizzare il AWS CLI comando [list-metrics per visualizzare le metriche](#) disponibili per Trusted Advisor

Example: elenca tutte le metriche per Trusted Advisor

L'esempio seguente specifica lo spazio dei nomi AWS/TrustedAdvisor nomi per cui visualizzare tutte le metriche. 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"
        }
    ],
    "MetricName": "ServiceLimitUsage"
}

```

```

        "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"
    },
    ...
]
```

Trusted Advisor metriche e dimensioni

Consulta le seguenti tabelle per le Trusted Advisor metriche e le dimensioni che puoi utilizzare per gli CloudWatch allarmi e i grafici.

Trusted Advisor metriche a livello di controllo

Puoi utilizzare le seguenti metriche per i controlli. Trusted Advisor

Metrica	Description
RedResources	Il numero di risorse in rosso (azione consigliata).
YellowResources	Il numero di risorse in giallo (indagine consigliata).

Trusted Advisor metriche a livello di quota di servizio

È possibile utilizzare le seguenti metriche per le quote. Servizio AWS

Mettrica	Description
ServiceLimitUsage	Percentuale di utilizzo delle risorse rispetto a una quota di servizio (precedentemente definita limiti).

Dimensioni per i parametri a livello di controllo

È possibile utilizzare la seguente dimensione per Trusted Advisor i controlli.

Dimensione	Description
CheckName	Il nome dell' Trusted Advisor assegno. Puoi trovare tutti i nomi dei controlli nella console Trusted Advisor o in AWS Trusted Advisor verifica riferimento .

Dimensioni per i parametri della quota di servizio

È possibile utilizzare le seguenti dimensioni per le metriche delle quote di Trusted Advisor servizio.

Dimensione	Description
Region	Il 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, vedere [Trusted Advisor azioni](#).

Note

CloudTrail registra anche le operazioni dell' Trusted Advisor API nell'[Supporto AWS API Reference](#). Per ulteriori informazioni, consulta [Registrazione delle chiamate Supporto AWS API 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'RefreshCheckazione 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'UpdateNotificationPreferencesazione.

```
{
  "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'GenerateReportazione. 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 Supporto AWS](#).

Per le istanze Windows di Amazon EC2, puoi utilizzare EC2 Rescue per esaminare le istanze per identificare problemi comuni, raccogliere file di registro e risolvere i problemi. Puoi anche usare EC2 Rescue per analizzare i volumi di avvio da istanze non funzionanti. 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 Supporto AWS. 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
Gateway Amazon API	Risoluzione dei problemi relativi a HTTP APIs
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
Amazon EC2 Auto Scaling	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 Amazon CloudSearch
AWS CodeDeploy	Risoluzione dei problemi di AWS CodeDeploy
Amazon CloudWatch	Risoluzione dei problemi di
AWS Database Migration Service	Risoluzione dei problemi 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 relativi alla creazione della SSL/TLS connessione
AWS Elastic Beanstalk	Risoluzione dei problemi
Amazon Elastic Compute Cloud (Amazon EC2)	Risoluzione dei problemi delle istanze Risoluzione dei problemi delle istanze di Windows Risoluzione dei problemi di importazione/esportazione delle macchine virtuali Risoluzione degli errori di richiesta API

Servizio	Link
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
Elastic Load Balancing	Risoluzione dei problemi di Application Load Balancer Risoluzione dei problemi di Classic Load Balancer
Amazon ElastiCache (Memcached)	Risoluzione dei problemi delle applicazioni
Amazon ElastiCache (sistema operativo 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
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	Link
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 Amazon OpenSearch Service
Amazon Personalize	Risoluzione dei problemi
Amazon Quick	Risoluzione dei problemi di Amazon Quick 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
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 AI	Risoluzione degli errori Risoluzione dei problemi di Amazon SageMaker AI Studio
Amazon Silk	Risoluzione dei problemi
Amazon Simple Email Service (Amazon SES)	Risoluzione dei problemi di Amazon SES

Servizio	Link
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
Gateway di archiviazione AWS	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 (Site-to-Site 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 Supporto AWS servizio.

- Supporto AWS Versione API: 15-04-2013
- Supporto AWS Versione dell'API dell'app: 2021-08-20

La tabella seguente descrive gli aggiornamenti importanti della AWS Trusted Advisor documentazione Supporto AWS e, a partire dal 10 maggio 2021. Puoi ora iscriverti a un feed RSS per ricevere notifiche sugli aggiornamenti.

Modifica	Descrizione	Data
Sono state aggiunte informazioni di supporto in lingua turca	Sono state aggiunte informazioni sulla disponibilità del supporto in lingua turca per i casi di assistenza. Per ulteriori informazioni, consulta Comprendere i tempi di Supporto AWS risposta .	14 aprile 2026
Scadenza aggiornata per le policy IAM dell'API Support Center Console	È stata aggiornata la scadenza dal 1 giugno 2026 al 2 novembre 2026 per l'aggiunta delle operazioni della console di Support Center alle politiche IAM. Per ulteriori informazioni, consulta Aggiungere le politiche IAM per le operazioni dell'API della console di Support Center .	27 marzo 2026
Titolo aggiornato del ruolo del team AWS Unified Operations	È stato aggiornato il titolo da Migration Specialist a Migrations and Events	19 marzo 2026

Engineer nella sezione del team Unified Operations. Per ulteriori informazioni, consulta [Migrations and Events Engineer](#).

[Documentazione aggiornata Supporto AWS dell'app per l'autorizzazione di più account](#)

Sono stati aggiornati i passaggi manuali per l'autorizzazione di più account senza utilizzare CloudFormation modelli. Per ulteriori informazioni, consulta [Autorizzare più account](#) e [Creazione di risorse con CloudFormation](#)

27 febbraio 2026

[Nuovo controllo dei gateway NAT inattivi](#)

È stato aggiunto un nuovo controllo per identificare i gateway NAT inattivi o sottoutilizzati che potrebbero essere candidati all'ottimizzazione dei costi. [Per ulteriori informazioni, vedere Registro delle modifiche per i controlli. AWS Trusted Advisor](#)

19 febbraio 2026

[Aggiornamento Gestisci l'accesso al Centro Supporto AWS](#)

È stato aggiunto un riferimento all'argomento sulle operazioni dell'API della console di Support Center per aiutare i clienti a trovare informazioni su operazioni aggiuntive per le loro politiche. Per ulteriori informazioni, consulta [Gestire l'accesso al Supporto AWS Centro](#).

13 febbraio 2026

[Nota aggiornata sull'aggiunta di politiche IAM per le operazioni dell'API della console di Support Center](#)

È stata aggiornata la nota relativa all'utilizzo di una configurazione VPN personalizzata. Per ulteriori informazioni, consulta [Aggiungere le politiche IAM per le operazioni dell'API della console di Support Center](#).

11 febbraio 2026

[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](#).

29 gennaio 2026

[Sono state aggiunte le migliori pratiche e i tempi di risposta previsti per i casi di Enterprise Support in Creare un caso di supporto da un'interazione di supporto](#)

È stata aggiunta una nuova sezione a discesa che descrive in dettaglio le best practice per i clienti di Enterprise Support durante la creazione di casi per Supporto AWS. Per ulteriori informazioni, consulta [Creare una richiesta di supporto da un'interazione di supporto](#).

12 gennaio 2026

[5 controlli di ottimizzazione dei costi obsoleti Trusted Advisor](#)

Per i dettagli, consulta il [registro delle modifiche](#) per i controlli. AWS Trusted Advisor

9 gennaio 2026

Piani di modifica Supporto AWS aggiornati	È stata aggiunta una nota che descrive in dettaglio cosa succede se un account viene aggiunto o rimosso da un'organizzazione iscritta a AWS Business Support+. Per ulteriori informazioni, consulta Change Plans. Supporto AWS	8 gennaio 2026
Nuova sezione Configura le autorizzazioni per utilizzare la risoluzione dei problemi basata sull'intelligenza artificiale	È stata aggiunta una nuova sezione che descrive come configurare le autorizzazioni richieste per la risoluzione dei problemi ottimizzata dall'intelligenza artificiale in Service Catalog. Per ulteriori informazioni, consulta Configurare le autorizzazioni per utilizzare la risoluzione dei problemi basata sull'intelligenza artificiale .	22 dicembre 2025
Riferimento di Trusted Advisor controllo aggiornato	Per i dettagli, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli .	18 dicembre 2025
Riferimento di Trusted Advisor controllo aggiornato	Per i dettagli, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli .	17 dicembre 2025
Sono state aggiunte informazioni relative alle riunioni virtuali con Supporto AWS	Per ulteriori informazioni, consulta Riunioni virtuali con Supporto AWS .	9 dicembre 2025

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 .	8 dicembre 2025
Sono state aggiunte informazioni relative ai nuovi piani Supporto AWS	Per ulteriori informazioni, consulta Supporto AWS Piani .	2 dicembre 2025
Sono state aggiunte informazioni sulla risoluzione dei problemi con intelligenza artificiale	Per ulteriori informazioni, consulta Risoluzione dei problemi con intelligenza artificiale nella console di Support Center .	2 dicembre 2025
Informazioni aggiunte: una nuova sezione per AWS Unified Operations	Per ulteriori informazioni, consulta Che cos'è AWS Unified Operations .	2 dicembre 2025
Aggiunta descrizione per Support Assistant APIs	Sono state aggiunte azioni Supporto AWS API per Support Assistant: ListInteractions ListInteractionEntries, e ResolveInteraction in Gestisci l'accesso al Supporto AWS Centro .	2 dicembre 2025
Riferimento di Trusted Advisor controllo aggiornato	Per i dettagli, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli .	21 novembre 2025

Riferimento di Trusted Advisor controllo aggiornato	Per i dettagli, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli .	17 novembre 2025
Aggiornato Modifica ed eliminazione di un ruolo collegato al servizio per Supporto	I clienti che hanno sottoscritto un piano AWS Organizations Enterprise Support possono eliminare il ruolo collegato al AWSServiceRoleForSupport servizio. Per ulteriori informazioni, vedere Modifica ed eliminazione di un ruolo collegato al servizio per Supporto	31 ottobre 2025
Riferimento di Trusted Advisor controllo aggiornato	Per i dettagli, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli .	15 ottobre 2025
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 .	30 settembre 2025

Nuovo argomento	È stato aggiunto un nuovo argomento con informazioni su come abilitare le notifiche di scadenza del piano promozionale. Per ulteriori informazioni, consulta Configurare le notifiche di scadenza del piano promozionale .	12 settembre 2025
Trusted Advisor Assegno aggiornato	Per i dettagli, consulta il registro delle modifiche per AWS Trusted Advisor i controlli .	11 settembre 2025
Chiamate API della console Testing Support Center aggiornate	La fase 3 è stata aggiornata per indicare la fonte corretta dell'evento, support-console.amazonaws.com. Per ulteriori informazioni, consulta Testing Support Center Console API call .	2 settembre 2025
Supporto AWS Piani di modifica aggiornati	I passaggi per l'upgrade o il downgrade Supporto AWS dell'abbonamento sono stati aggiornati. Per ulteriori informazioni, consulta Modifica Supporto AWS dei piani .	27 agosto 2025
Trusted Advisor Controllo aggiornato	Per i dettagli, consulta il registro delle modifiche per AWS Trusted Advisor i controlli .	19 agosto 2025
Sezione Trusted Advisor Engage rimossa	Rimossa la sezione Get started with AWS Trusted Advisor Engage (Preview).	7 agosto 2025

Aggiornato come aggiungere e l' Supporto AWS app a un canale Slack	Per i dettagli, consulta Configurazione di un canale Slack .	6 agosto 2025
Due controlli sono obsoleti	Per i dettagli, consulta il Registro delle modifiche per i controlli. AWS Trusted Advisor	22 luglio 2025
Politiche gestite aggiornate: AWSSupportAccess	Per i dettagli, consulta Supporto AWS gli aggiornamenti alle politiche AWS gestite .	18 luglio 2025
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 .	15 luglio 2025
Verifica aggiornata: fine del supporto standard per le istanze Amazon EC2 con Ubuntu LTS	Per i dettagli, consulta il registro delle modifiche per i controlli. AWS Trusted Advisor	3 luglio 2025
Trusted Advisor Controllo aggiornato: autorizzazioni Amazon S3 Bucket	Per i dettagli, consulta il registro delle modifiche per i controlli. AWS Trusted Advisor	3 luglio 2025
Controllo aggiornato: MFA sull'account root	Per i dettagli, consulta il Registro delle modifiche per i AWS Trusted Advisor controlli .	2 luglio 2025
Controllo aggiornato: driver Amazon ECS AWS Logs in modalità di blocco.	Per i dettagli, consulta il registro delle modifiche per i AWS Trusted Advisor controlli .	2 luglio 2025

[Aggiornato Richiedi un aumento della quota di servizio](#)

Sono state aggiunte informazioni su come creare una richiesta di aumento della quota di servizio se Servizio AWS o Regione AWS non è supportata nella console Service Quotas. Per ulteriori informazioni, consulta [Richiedere un aumento della quota di servizio](#).

2 luglio 2025

[La creazione di una richiesta di aumento della quota di servizio nella console di Support Center non è più supportata.](#)

Per ulteriori informazioni, vedere [Creazione di un aumento della quota di servizio](#).

23 giugno 2025

[È stata aggiunta una descrizione per UpdateInteraction nell'API Supporto](#)

È stata aggiunta la descrizione UpdateInteraction delle azioni AWS Supporto API in [Gestisci l'accesso al Supporto AWS Centro](#).

23 giugno 2025

[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 giugno 2025

[Nuova sezione: Informazioni sull'API della console Support Center](#)

L'API Support Center Console migliora la tua esperienza con la console Support Center. Per i dettagli, consulta [Informazioni sull'API della console Support Center](#).

16 giugno 2025

[Introduzione al AWS Trusted Advisor capitolo aggiornato a per sottolineare che i piani Basic e Developer Support non supportano l'aggiornamento automatico dei controlli. È necessario aggiornare manualmente i controlli di sicurezza per visualizzare lo stato del controllo più recente.](#)

Per informazioni dettagliate, vedi [AWS Trusted Advisor](#).

11 giugno 2025

[Verifica aggiornata: l'utilizzo AWS STS globale degli endpoint Regioni AWS è ora disponibile a tutti i livelli del Supporto AWS piano.](#)

Per i dettagli, consulta il [registro delle modifiche per i AWS Trusted Advisor controlli](#).

9 giugno 2025

[Nuovo controllo: consigli per l'ottimizzazione dei costi di Amazon Aurora per lo storage in cluster DB](#)

Per i dettagli, consulta il [registro delle modifiche per i AWS Trusted Advisor controlli](#).

9 giugno 2025

[Nuovo controllo: utilizzo AWS STS globale degli endpoint in tutto il mondo Regioni AWS](#)

Per i dettagli, consulta il [registro delle modifiche per i AWS Trusted Advisor controlli](#).

2 giugno 2025

15 nuovi Centrale ottimizzazione costi AWS controlli si aggiungono a Trusted Advisor	Per i dettagli, consulta il Registro delle modifiche per AWS Trusted Advisor i controlli .	30 maggio 2025
Sono stati aggiornati tre Trusted Advisor controlli	Per i dettagli, consulta il registro delle modifiche per AWS Trusted Advisor i controlli .	21 maggio 2025
Nuova funzionalità: aggiorna la gravità dei casi di supporto	Per i dettagli, consulta la sezione Modifica del livello di gravità dei casi di supporto Creazione dei casi di supporto e gestione dei casi .	21 maggio 2025
Ora aggiornata è possibile visualizzare i dettagli del Supporto AWS caso.	Per i dettagli, consulta Sicurezza per i tuoi Supporto AWS casi .	29 aprile 2025
Sono stati aggiornati due Trusted Advisor controlli	Per i dettagli, consulta il registro delle modifiche per AWS Trusted Advisor i controlli .	2 aprile 2025
È stata aggiunta una descrizione per l' Supporto API	È stata aggiunta la descrizione delle azioni AWS Supporto API in Gestisci l'accesso al Supporto AWS Centro .	7 marzo 2025
6 controlli obsoleti AWS Security Hub CSPM	Per i dettagli, consulta il Registro delle modifiche per i controlli. AWS Trusted Advisor	5 marzo 2025

[Rimossi i riferimenti alle metriche a livello di categoria per Trusted Advisor](#)

Le metriche a livello di categoria per sono obsolete. Trusted Advisor I riferimenti alle metriche a livello di categoria vengono rimossi da Creazione di [CloudWatch allarmi Amazon](#) per monitorare i parametri. AWS Trusted Advisor

27 gennaio 2025

[Documentazione aggiornata per Trusted Advisor](#)

Sono stati aggiunti due nuovi controlli: AWS CloudTrail Management Events Logging e Amazon RDS Continuous Backups Not Enabled. Per ulteriori informazioni, consulta [Change log](#) for checks. AWS Trusted Advisor

23 dicembre 2024

[Documentazione aggiornata per Trusted Advisor](#)

Risorse aggiornate per Auto Scaling Group. Per ulteriori informazioni, consulta [Change log for AWS Trusted Advisor check](#).

23 dicembre 2024

[Documentazione aggiornata per Trusted Advisor](#)

Controllo dell'accesso esterno di IAM Access Analyzer aggiornato. Per ulteriori informazioni, consulta [Change log for AWS Trusted Advisor checks](#).

23 dicembre 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 .	25 novembre 2024
Documentazione aggiornata per Trusted Advisor	Aggiunto 1 nuovo Trusted Advisor controllo. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli .	22 novembre 2024
Documentazione aggiunta per le politiche AWS gestite per AWS Partner-Led Support	È stata aggiunta documentazione per una nuova politica AWS gestita. <code>AWSPartnerLedSupportReadOnlyAccess</code> Per ulteriori informazioni, consulta le politiche AWS gestite per AWS Partner-Led Support .	22 novembre 2024
Documentazione aggiornata per Trusted Advisor	3 Trusted Advisor controlli aggiornati. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli .	7 novembre 2024

[Documentazione aggiornata
per Supporto AWS i piani](#)

È stato aggiunto un nuovo esempio di registro per l'ListSupportPlanModifiers operazione alle [chiamate API Logging Supporto Plans con AWS CloudTrail](#) pagina.

6 novembre 2024

[Documentazione per
AWSTrustedAdvisorServiceRolePolicy
aggiornata](#)

Sono state aggiunte nuove azioni IAM elasticloadbalancing:DescribeListeners e elasticloadbalancing:DescribeRules , per effettuare l'onboard, un nuovo controllo di sicurezza. Per ulteriori informazioni, consulta l'argomento relativo alle [policy gestite da AWS : AWSTrustedAdvisorServiceRolePolicy](#).

30 ottobre 2024

[Documentazione aggiornata
per Trusted Advisor](#)

Aggiunti 4 nuovi Trusted Advisor controlli. Per ulteriori informazioni, consulta [Registro delle modifiche per AWS Trusted Advisor i controlli](#).

11 ottobre 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](#).

8 ottobre 2024

[Documentazione aggiornata
per Trusted Advisor](#)

È stato spostato 1 controllo di ottimizzazione dei costi nel pilastro Fault Tolerance. Sono stati aggiornati 1 controllo di sicurezza e 1 controllo di tolleranza agli errori. Per ulteriori informazioni, vedere [Registro delle modifiche per AWS Trusted Advisor i controlli](#).

2 ottobre 2024

[Sezione AWS Trusted Advisor Engage aggiornata](#)

È stata aggiornata la sezione AWS Trusted Advisor Engage in modo da fare riferimento a AWS Countdown. Per ulteriori informazioni, consulta [Introduzione a AWS Trusted Advisor Engage \(anteprima\)](#).

16 settembre 2024

[Documentazione aggiornata
per i piani Supporto AWS](#)

È stata aggiunta una nuova autorizzazione e CloudTrail I documentazione per la visualizzazione di un elenco di modificatori del piano di supporto. Per ulteriori informazioni, consulta [Gestire l'accesso ai Supporto AWS piani, politiche AWS gestite per Supporto AWS i piani e Registrazione delle chiamate API Supporto AWS dei piani con](#). AWS CloudTrail

9 settembre 2024

Documentazione aggiornata per Trusted Advisor	Trusted Advisor aggiunti 9 nuovi controlli il 23 agosto. Per ulteriori informazioni, consulta Registro delle modifiche per i AWS Trusted Advisor controlli .	23 agosto 2024
Documentazione aggiornata per Trusted Advisor	Aggiornato 1 controllo di eccellenza Trusted Advisor operativa e aggiunto 1 nuovo controllo Trusted Advisor di sicurezza. Per ulteriori informazioni, vedere Registro delle modifiche per AWS Trusted Advisor i controlli .	22 agosto 2024
Documentazione aggiornata per Trusted Advisor	6 controlli Trusted Advisor di sicurezza aggiornati. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli .	20 agosto 2024
Documentazione aggiornata per Trusted Advisor	2 Trusted Advisor controlli aggiornati. Per ulteriori informazioni, consulta Registro delle modifiche per AWS Trusted Advisor i controlli .	12 agosto 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 .	5 agosto 2024

[Documentazione aggiornata per Trusted Advisor](#)

9 Trusted Advisor controlli aggiornati. Per ulteriori informazioni, consulta [Registro delle modifiche per AWS Trusted Advisor i controlli](#).

21 luglio 2024

[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:ListServiceManagedPolicies ,kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFirewall e sqs:GetQueueAttributes nuovi controlli integrati. Per ulteriori informazioni, consulta l'argomento relativo alle [policy gestite da AWS : AWSTrustedAdvisorServiceRolePolicy](#).

11 giugno 2024

[Sono stati rimossi 5 AWS Trusted Advisor controlli 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 sui controlli 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 Supporto piano](#)

Aggiornamenti alle funzionalità dei Supporto piani. Per ulteriori informazioni, consulta [Supporto 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
AWSTrustedAdvisorS
erviceRolePolicy
aggiornata](#)

Sono state aggiunte nuove azioni IAM `cloudtrail:GetTrail`, `cloudtrail:ListTrails`, `cloudtrail:GetEventSelector`, `cloudtrail:Outposts:GetOutposts`, `cloudtrail:Outposts:ListAssets` e `cloudtrail: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	1 controllo di sicurezza aggiornato 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](#)

Politiche aggiornate AWSTrustedAdvisorPriorityFullAccess e AWSTrustedAdvisorPriorityReadOnlyAccess AWS gestite per includere la dichiarazione IDs. 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:ListResolveEndpointIpAddresses`, `route53resolver:ListResolveEndpointIpAddresses`, `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](#)

Documentazione Trusted Advisor Engage aggiornata con modifiche ai moduli per la creazione e la modifica delle interazioni. È stata aggiunta una pagina con [esempi di politiche 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 Supporto AWS 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 Supporto AWS piani, politiche AWS gestite per Supporto AWS i piani e Registrazione delle Supporto AWS chiamate API con AWS CloudTrail](#).

08 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 Supporto AWS 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 Introduzione a Engage. AWS Trusted Advisor

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:

16 febbraio 2023

- 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, consulta [Guida introduttiva a Trusted Advisor Priority](#).

[Esempi di codice aggiornati per Supporto](#)

Sono stati aggiunti esempi di codice.NET, Java e Kotlin che mostrano come utilizzarli Supporto con un kit di sviluppo AWS software (SDK). Per ulteriori informazioni, consulta [Esempi di codice](#) per l'utilizzo. Supporto AWS SDKs

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 Supporto AWS l'app](#)

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 Supporto AWS l'app](#)

Puoi anche usare Terraform per creare le tue risorse per l' Supporto AWS App. Per ulteriori informazioni, consulta [Creare risorse per Supporto AWS 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' Supporto AWS app in Slack](#)

Ora puoi richiedere l'assistenza tramite chat dal vivo per le seguenti opzioni:

14 dicembre 2022

- 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](#).

[Documentazione aggiornata per Supporto AWS](#)

È stata aggiunta la documentazione sui nuovi endpoint per l' Supporto API. Per ulteriori informazioni, consulta [Informazioni sull'API Supporto AWS](#).

14 dicembre 2022

[È stata aggiunta la documentazione per CloudFormation i modelli da utilizzare per l' Supporto AWS app in Slack](#)

Puoi utilizzare i CloudFormation modelli per creare aree di lavoro e canali di configurazione Slack per in. Account AWS Organizations Per ulteriori informazioni, consulta [Creazione di risorse Supporto AWS 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 CSPM risultati in Trusted Advisor	I risultati dei controlli CSPM di Security Hub vengono rimossi Trusted Advisor più rapidamente. Per ulteriori informazioni, consulta il registro delle modifiche per i AWS Trusted Advisor 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' Supporto AWS 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 Supporto AWS	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 .	09 novembre 2022

[Documentazione aggiornata per l' Supporto AWS app in Slack](#)

È stata aggiunta la documentazione per le autorizzazioni supportapp . Per ulteriori informazioni, consulta [Autorizzazioni necessarie per la connessione dell' Supporto AWS app a Slack](#).

1 novembre 2022

[Documentazione aggiornata per l' Supporto AWS 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 [Supporto AWS 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:

29 settembre 2022

- [Gestione dell'accesso per i piani Supporto AWS](#)
- [AWS politiche gestite per Supporto AWS Plans](#)
- [Modifica Supporto AWS dei piani](#)
- [Registrazione delle chiamate all'API Supporto AWS Plans con AWS CloudTrail](#)

[Documentazione aggiornata per l' Supporto AWS app in Slack](#)

È stata aggiunta documentazione su come configurare un canale pubblico o privato da utilizzare con l' Supporto AWS app. Per ulteriori informazioni, consulta la pagina [Configuring a Slack channel](#) (Configurazione di un canale Slack).

22 settembre 2022

[Documentazione aggiornata per Supporto AWS](#)

È stata aggiunta una nuova sezione sulla sicurezza per i casi di supporto. Per ulteriori informazioni, consulta [Sicurezza per i tuoi Supporto AWS 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' Supporto AWS app in
Slack](#)

Vedi gli argomenti seguenti:

24 agosto 2022

Puoi utilizzare l' Supporto AWS 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 Supporto AWS nella documentazione di Slack](#).

Puoi allegare policy AWS gestite ai tuoi ruoli IAM per utilizzare l' Supporto AWS App. Per ulteriori informazioni, consulta [le politiche AWS gestite per Supporto AWS l'app in Slack](#).

Nuovo riferimento API per l' Supporto AWS app. Consulta la [documentazione di riferimento sull'API dell'app Supporto AWS](#).

[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:

17 agosto 2022

- 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](#).

[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:

7 luglio 2022

- Criteri di avviso
- Operazione consigliata
- Risorse aggiuntive
- Colonne del report

Per ulteriori informazioni, consulta il [riferimento dei controlli AWS Trusted Advisor](#).

[Documentazione aggiornata per Supporto AWS](#)

Documentazione aggiunta che spiega come gestire i casi di supporto.

28 giugno 2022

- [Aggiornamento di un caso di supporto esistente](#)
- [Risoluzione dei problemi](#)

[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 ulteriori controlli standard di sicurezza AWS Foundational Security Best Practices provenienti da AWS Security Hub CSPM. Per ulteriori informazioni, 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 Supporto AWS](#)

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 informazioni, [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 prioritari forniti dal tuo Technical Account Manager (TAM). Per ulteriori informazioni, consulta Guida introduttiva a Priority. Trusted Advisor	28 febbraio 2022
Documentazione aggiornata per l'utilizzo di Amazon EventBridge per Trusted Advisor	Puoi creare una EventBridge 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 EventBridge per monitorare Supporto AWS i casi	Puoi creare una EventBridge regola per monitorare e ricevere notifiche sui tuoi casi di assistenza. Per ulteriori informazioni, consulta Monitoraggio Supporto dei casi con EventBridge .	21 febbraio 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 febbraio 2022

[Documentazione aggiunta
per l'integrazione con AWS
Security Hub CSPM](#)

Nella Trusted Advisor console, ora puoi visualizzare i risultati dei controlli CSPM del Security Hub che fanno parte dello standard di sicurezza AWS Foundational Security Best Practices. Per ulteriori informazioni, vedere [Visualizzazione dei controlli AWS Security Hub CSPM nella console](#).
AWS Trusted Advisor

18 gennaio 2022

[Documentazione aggiornata
per Trusted Advisor](#)

Sono stati aggiunti tre nuovi controlli per le istanze Amazon EC2 che eseguono Microsoft SQL Server.

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

Per ulteriori informazioni, consulta il [riferimento dei controlli AWS Trusted Advisor](#).

[Documentazione aggiornata
per Trusted Advisor](#)

Trusted Advisor ha aggiunto quattro nuovi controlli per AWS Well-Architected

20 dicembre 2021

- 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](#).

[Documentazione aggiornata](#)

Se disponi di un piano [Enterprise On-Ramp Support](#), hai accesso a tutti i Trusted Advisor controlli e all' Supporto AWS 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 Registro delle modifiche per AWS Trusted Advisor i controlli .	08 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 Supporto AWS 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 Supporto casi](#)

Aggiunta documentazione su come creare un caso di supporto correlato per i casi chiusi in modo permanent e. Per ulteriori informazioni, consulta la sezione [Riapertura di un caso chiuso](#) e [Creazione di un caso correlato](#).

08 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](#).

08 giugno 2021

[Documentazione aggiornata](#)

I seguenti argomenti sono stati aggiornati:

12 maggio 2021

- Procedure aggiornate e contenuti aggiunti all'argomento [Creazione di CloudWatch allarmi Amazon per monitorare le AWS Trusted Advisor metriche](#)
- È stata aggiunta la sezione [Quote di servizio per la sezione API Supporto AWS](#)

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 <code>AWSSupportServiceRolePolicy</code> AWS gestita. Per ulteriori informazioni, consulta Utilizzo dei ruoli collegati ai servizi per Supporto AWS.	16 marzo 2021
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 Supporto AWS piano. Per ulteriori informazioni, consulta Registrazione delle modifiche al piano Supporto.	09 febbraio 2021
Documentazione aggiornata per Trusted Advisor	Aggiornato l'argomento Inizia a usare i Trusted Advisor consigli.	29 gennaio 2021

Modifica	Descrizione	Data
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
Aggiunto il supporto per le unità organizzative	È ora possibile creare report per i Trusted Advisor controlli per le unità organizzative (OUs). Per ulteriori informazioni, consulta Creazione di report di visualizzazione organizzativa .	17 novembre 2020
È stata aggiornata la registrazione con l'argomento AWS CloudTrail	È stata aggiunta una voce di registro di esempio per un'operazione Trusted Advisor API. Per informazioni, consulta AWS Trusted Advisor informazioni relative alla registrazione CloudTrail .	22 ottobre 2020
Supporto AWS Quote aggiunte	Informazioni aggiunte sulle quote e le restrizioni correnti per Supporto. Consulta la sezione Endpoint e quote Supporto 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

Modifica	Descrizione	Data
Sicurezza e Supporto AWS	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di Supporto AWS e Trusted Advisor. Consulta Sicurezza in Supporto AWS	05 maggio 2020
Sicurezza e Supporto AWS	Aggiunte informazioni sulle considerazioni di sicurezza durante l'utilizzo di Supporto AWS.	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
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 Supporto AWS chiamate con AWS CloudTrail	Aggiunta una nuova sezione.	21 aprile 2016

Modifica	Descrizione	Data
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 Console di gestione AWS.	30 ottobre 2014
Programmare la durata di un caso Supporto AWS	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
Accedendo Supporto AWS	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 Supporto AWS un nuovo servizio.	30 aprile 2013

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.