Guida per l'utente

AWS Well-Architected Tool

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Well-Architected Tool: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

..... vii
Che cos'è AWS Well-Architected Tool? 1
Che cos'è AWS Well-Architected Framework? 2
AWS Well-Architected Tool glossario 2
Nozioni di base 4
Accesso allo AWS WA Tool 4
Attivazione delle integrazioni 5
Attivazione di AppRegistry 6
Attivazione di Trusted Advisor 6
Definizione di un carico di lavoro 14
Documentazione di un carico di lavoro 17
Revisione di un carico di lavoro 18
Visualizzazione dei controlli di Trusted Advisor 20
Salvataggio di un milestone 22
Tutorial: documenta un carico di lavoro 24
Fase 1: Definire un carico di lavoro 24
Fase 2: Documentare lo stato del carico di lavoro 25
Fase 3: Rivedi il piano di miglioramento 29
Fase 4: apportare miglioramenti e misurare i progressi 31
Carichi di lavoro in AWS Well-Architected Tool 33
Problemi ad alto rischio (HRIs) e problemi a rischio medio () MRIs 34
Definire un carico di lavoro 35
Visualizza un carico di lavoro 36
Modifica un carico di lavoro 36
Condividi un carico di lavoro 37
Considerazioni sulla condivisione 40
Eliminare l'accesso condiviso 41
Modifica l'accesso condiviso 41
Accetta e rifiuta gli inviti 42
Eliminare un carico di lavoro 43
Genera un rapporto sul carico di lavoro 43
Visualizzazione dei dettagli del carico di lavoro 44
Scheda Overview (Panoramica) 45
La scheda Milestones 45

Scheda Proprietà ... 45
Scheda Condivisioni ... 46
Approfondimenti ... 48
Aggiunta di un obiettivo ... 48
Rimozione di un obiettivo ... 49
Visualizzazione dei dettagli dell'obiettivo ... 50
Scheda Overview (Panoramica) ... 50
Scheda Piano di miglioramento ... 50
Scheda Condivisioni ... 50
Obiettivi personalizzati ... 50
Visualizzazione di obiettivi personalizzati ... 51
Creazione di un obiettivo personalizzato ... 52
Visualizzazione in anteprima di un obiettivo personalizzato ... 54
Pubblicazione di un obiettivo personalizzato ... 54
Pubblicazione di un obiettivo personalizzato ... 55
Condivisione di un obiettivo ... 57
Aggiunta di tag a un obiettivo personalizzato ... 58
Eliminazione di un obiettivo ... 58
Specificazione del formato dell'obiettivo ... 59
Aggiornamenti dell'obiettivo ... 66
Determinazione dell'obiettivo da aggiornare ... 67
Aggiornamento di un obiettivo ... 68
Catalogo Lens ... 69
Modelli di revisione ... 72
Creazione di un modello di recensione ... 72
Modificare un modello di recensione ... 73
Condivisione di un modello di recensione ... 74
Definizione di un carico di lavoro da un modello ... 75
Eliminazione di un modello di recensione ... 76
Profili ... 78
Creazione di un profilo ... 78
Modifica di un profilo ... 79
Condivisione di un profilo ... 79
Aggiungere un profilo a un carico di lavoro ... 80
Rimuovere un profilo da un carico di lavoro ... 80
Eliminazione di un profilo ... 81

Jira ... 83
Configurazione del connettore ... 84
Configurazione del connettore ... 85
Sincronizzazione di un carico di lavoro ... 87
Disinstallazione del connettore ... 88
Milestone ... 90
Salvataggio di un milestone ... 90
Visualizzazione di milestone ... 90
Generazione di un report milestone ... 91
Condividi gli inviti ... 92
Accettazione di un invito alla condivisione ... 93
Rifiutare un invito alla condivisione ... 94
Notifiche ... 95
Notifiche sull'obiettivo ... 95
Notifiche sul profilo ... 95
Dashboard (Pannello di controllo) ... 97
Riepilogo ... 97
Wellate Framework, problemi del Wellato Framework Framework, ... 97
Problemi del Well-Well-Framework Framework di Well-Well- ... 98
I problemi del Well-Framework Framework di Well-Well-Framework ... 99
Sicurezza ... 101
Protezione dei dati ... 102
Crittografia dei dati a riposo ... 103
Crittografia in transito ... 103
Come AWS utilizza i tuoi dati ... 103
Identity and Access Management ... 104
Destinatari ... 104
Autenticazione con identità ... 105
Gestione dell'accesso con policy ... 108
Funzionamento di AWS Well-Architected Tool con IAM ... 111
Esempi di policy basate su identità ... 119
Policy gestite da AWS ... 125
Risoluzione dei problemi ... 131
Risposta agli incidenti ... 132
Convalida della conformità ... 132
Resilienza ... 133

Sicurezza dell'infrastruttura 134
Analisi della configurazione e delle vulnerabilità 134
Prevenzione del confused deputy tra servizi 134
Condivisione delle tue risorse 137
Attiva la condivisione delle risorse all'interno AWS Organizations 137
Tagging delle risorse 140
Nozioni di base sui tag 140
Tagging delle risorse 141
Limitazioni applicate ai tag 142
Utilizzo di tag tramite la console 142
Aggiunta di tag a una singola risorsa alla creazione 142
Aggiunta ed eliminazione di tag in una singola risorsa 142
Lavorare con i tag utilizzando l'API 144
Registrazione 146
Informazioni su AWS WA Tool in CloudTrail 146
Comprensione delle voci dei file di log di AWS WA Tool 147
EventBridge 150
Eventi di AWS WA Tool di esempio 151
Cronologia dei documenti 155
Glossario per AWS 162

Abbiamo rilasciato una nuova versione del Framework Well-Architected. Abbiamo anche aggiunto obiettivi nuovi e aggiornati al Catalogo Lens. Scopri di più sulle modifiche.

Che cos'è AWS Well-Architected Tool?

AWS Well-Architected Tool (AWS WA Tool) è un servizio nel cloud che fornisce un processo coerente per misurare l'architettura utilizzando le AWS migliori pratiche. AWS WA Tool ti aiuta durante l'intero ciclo di vita del prodotto effettuando le seguenti operazioni:

- Mediante l’assistenza nella documentazione delle decisioni prese
- Fornendo suggerimenti per migliorare il carico di lavoro in base alle best practice
- Guidando l’utente nel rendere i carichi di lavoro più affidabili, sicuri, efficienti e convenienti

Puoi utilizzarlo AWS WA Tool per documentare e misurare il tuo carico di lavoro utilizzando le migliori pratiche del AWS Well-Architected Framework. Queste best practice sono state sviluppate da AWS Solutions Architects sulla base di anni di esperienza nella creazione di soluzioni per un'ampia varietà di aziende. Il canone offre un approccio coerente per la misurazione delle architetture e fornisce linee guida per l'implementazione di progetti dimensionabili nel tempo in base alle esigenze.

Oltre alle AWS best practice, puoi utilizzare obiettivi personalizzati per misurare il carico di lavoro utilizzando le tue best practice. È possibile personalizzare le domande in modo personalizzato in modo che siano specifiche per una particolare tecnologia o per aiutarvi a soddisfare le esigenze di governance all'interno della vostra organizzazione. Le lenti personalizzate estendono la guida fornita dalle AWS lenti.

Si integra AWS Trusted Advisore ti AWS Service Catalog AppRegistryaiuta a scoprire più facilmente le informazioni necessarie per rispondere alle domande di AWS Well-Architected Tool revisione.

Questo servizio è destinato a coloro che sono coinvolti nello sviluppo tecnico dei prodotti, come i Chief Technology Officer (CTOs), gli architetti, gli sviluppatori e i membri del team operativo. AWS i clienti AWS WA Tool lo utilizzano per documentare le proprie architetture, fornire la governance del lancio dei prodotti e comprendere e gestire i rischi del proprio portafoglio tecnologico.

Argomenti

- Che cos'è AWS Well-Architected Framework?
- AWS Well-Architected Tool glossario

Che cos'è AWS Well-Architected Framework?

Il AWS Well-Architected Framework documenta una serie di domande fondamentali che consentono di comprendere in che modo un'architettura specifica si allinea alle best practice del cloud. Il canone fornisce un approccio coerente per valutare i sistemi rispetto alle qualità previste dai moderni sistemi basati sul cloud. In base allo stato dell'architettura, il canone suggerisce miglioramenti che è possibile apportare per ottenere al meglio tali qualità.

Impiegando il canone, è possibile apprendere le best practice relative alla progettazione e all'esecuzione di sistemi sicuri, efficienti e convenienti nel cloud. Offre un metodo per misurare con coerenza le proprie architetture rispetto alle best practice e individuare le aree di miglioramento. Il framework si basa su sei pilastri: eccellenza operativa, sicurezza, affidabilità, efficienza delle prestazioni, ottimizzazione dei costi e sostenibilità.

Durante la progettazione di un carico di lavoro, i compromessi tra questi pilastri si basano sulle esigenze aziendali. Le decisioni aziendali possono stabilire le priorità di progettazione. Negli ambienti di sviluppo, puoi ottimizzare per ridurre i costi a discapito dell'affidabilità. In soluzioni mission-critical, puoi ottimizzare l'affidabilità ed essere disposto ad accettare costi aggiuntivi. In soluzioni di e-commerce, puoi assegnare la priorità alle prestazioni, poiché la soddisfazione dei clienti può accompagnare un aumento delle entrate. Solitamente, la sicurezza e l'eccellenza operativa non sono soggette a compromessi rispetto agli altri pilastri.

Per ulteriori informazioni sul framework, visita il sito Web AWS Well-Architected.

AWS Well-Architected Tool glossario

Di seguito vengono definiti i termini comuni utilizzati in AWS WA Tool AWS Well-Architected Framework.

- Un workload (carico di lavoro) identifica un set di componenti che garantiscono valore aziendale. Il carico di lavoro è in genere il livello di dettaglio sui cui responsabili aziendali e tecnologici comunicano. Esempi di carichi di lavoro includono siti Web di marketing, siti Web di e-commerce, il back-end per un'app per dispositivi mobili e piattaforme di analisi. Il livello di complessità dell'architettura dei carichi di lavoro varia. Possono essere semplici, ad esempio un sito Web statico, o complessi, ad esempio architetture a microservizi con più datastore e molti componenti.
- Le tappe fondamentali segnano i cambiamenti chiave nell'architettura man mano che si evolve durante l'intero ciclo di vita del prodotto: progettazione, test, messa in funzione e produzione.

- Gli approfondimenti offrono un metodo per misurare con coerenza le proprie architetture rispetto alle best practice e individuare le aree di miglioramento.

  Oltre alle lenti fornite da AWS, puoi anche creare e utilizzare obiettivi personalizzati o utilizzare obiettivi che sono stati condivisi con te.
- I problemi ad alto rischio (HRIs) sono scelte architettoniche e operative AWS che, secondo noi, potrebbero avere un impatto negativo significativo su un'azienda. Questi HRIs potrebbero influire sulle operazioni organizzative, sulle risorse e sugli individui.
- I problemi a rischio medio (MRIs) sono scelte architetturali e operative AWS che secondo noi potrebbero avere un impatto negativo sull'attività aziendale, ma in misura minore rispetto a. HRIs

  Per ulteriori informazioni, consulta Problemi ad alto rischio (HRIs) e problemi a rischio medio () MRIs.

Nozioni di base su AWS Well-Architected Tool

Per iniziare a utilizzare AWS Well-Architected Tool, devi prima fornire le autorizzazioni appropriate agli utenti, ai gruppi e ai ruoli, nonché attivare il supporto per i Servizi AWS che desideri utilizzare con AWS WA Tool. Successivamente, definisci e documenta un carico di lavoro. Puoi anche salvare una milestone dello stato corrente di un carico di lavoro.

I seguenti argomenti spiegano come iniziare a utilizzare lo AWS WA Tool. Per un tutorial dettagliato su come utilizzareAWS Well-Architected Tool, consulta Tutorial: Documentare un carico di lavoroAWS Well-Architected Tool.

Argomenti

- Concessione dell'accesso allo AWS WA Tool a utenti, gruppi o ruoli
- Attivazione del supporto nello AWS WA Tool per altri servizi AWS
- Definizione di un carico di lavoro in AWS WA Tool
- Documentazione di un carico di lavoro in AWS WA Tool
- Revisione di un carico di lavoro con il Framework AWS Well-Architected
- Visualizzazione dei controlli di Trusted Advisor per un carico di lavoro
- Salvataggio di un milestone per un carico di lavoro in AWS WA Tool

Concessione dell'accesso allo AWS WA Tool a utenti, gruppi o ruoli

Puoi concedere a utenti, gruppi o ruoli il controllo completo o l'accesso in sola lettura allo AWS Well-Architected Tool.

Accesso allo AWS WA Tool

1. Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

   - Utenti e gruppi in AWS IAM Identity Center:

     Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

   - Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

2. Per concedere il controllo completo, applica la policy gestita WellArchitectedConsoleFullAccess al set di autorizzazioni o al ruolo.

   L'accesso completo consente al principale di eseguire tutte le operazioni in AWS WA Tool. Questo accesso è necessario per definire, eliminare, visualizzare, aggiornare e condividere i carichi di lavoro, nonché per creare e condividere obiettivi personalizzati.
3. Per concedere l'accesso in sola lettura, applica la policy gestita WellArchitectedConsoleReadOnlyAccess al set di autorizzazioni o al ruolo. I principali con questo ruolo possono solo visualizzare le risorse.

Per ulteriori informazioni su questo tipo di policy, consulta Policy gestite da AWS per AWS Well-Architected Tool.

Attivazione del supporto nello AWS WA Tool per altri servizi AWS

L'attivazione dell'accesso per l'organizzazione consente allo AWS Well-Architected Tool di raccogliere informazioni sulla struttura dell'organizzazione per condividere le risorse più facilmente (per ulteriori informazioni, consulta the section called “Attiva la condivisione delle risorse all'interno AWS Organizations”). L'attivazione del supporto per l'identificazione consente di raccogliere informazioni da AWS Trusted Advisor, da AWS Service Catalog AppRegistry e dalle risorse correlate (come gli stack AWS CloudFormation nelle raccolte di risorse di AppRegistry) per aiutarti a scoprire più facilmente le informazioni necessarie per rispondere alle domande di revisione di Well-Architected e personalizzare i controlli di Trusted Advisor per un carico di lavoro.

L'attivazione del supporto per AWS Organizations o l'attivazione del supporto per l'identificazione crea automaticamente un ruolo collegato al servizio per il tuo account.

Per attivare il supporto per altri servizi con cui AWS WA Tool può interagire, vai alle Impostazioni.

1. Per raccogliere informazioni da AWS Organizations, attiva l'opzione Attiva il supporto di AWS Organizations.
2. Per raccogliere informazioni da altri servizi e risorse AWS, attiva l'opzione Attiva supporto all'individuazione.
3. Seleziona Visualizza le autorizzazioni del ruolo per visualizzare le autorizzazioni dei ruoli collegati ai servizi o le policy delle relazioni di attendibilità.
4. Seleziona Salva impostazioni.

Attivazione di AppRegistry per un carico di lavoro

L'utilizzo di AppRegistry è facoltativo e i clienti con supporto AWS Business ed Enterprise possono attivare questa applicazione singolarmente per ogni carico di lavoro.

Ogni volta che il supporto all'individuazione è attivato e che AppRegistry è associata a un carico di lavoro nuovo o esistente, AWS Well-Architected Tool crea un gruppo di attributi gestito dal servizio. Il gruppo di attributi Metadata in AppRegistry contiene l'ARN del carico di lavoro, il nome del carico di lavoro e i rischi associati al carico di lavoro.

- Quando il supporto all'individuazione è attivato, ogni volta che viene apportata una modifica al carico di lavoro, il gruppo di attributi viene aggiornato.
- Quando il supporto all'individuazione è disattivato o l'applicazione viene rimossa dal carico di lavoro, le informazioni sul carico di lavoro vengono rimosse da AWS Service Catalog.

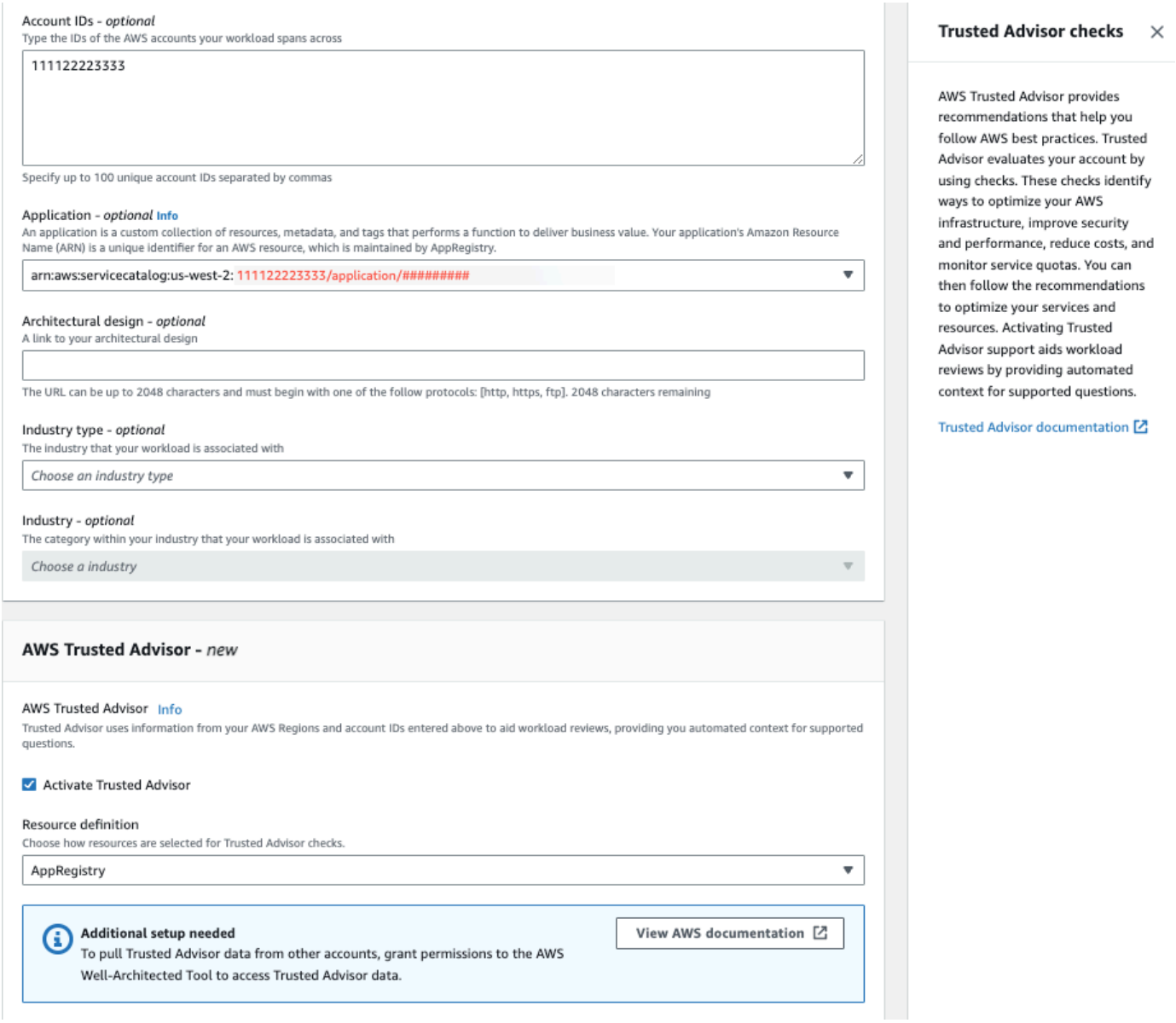
Se desideri che un'applicazione AppRegistry gestisca i dati recuperati da Trusted Advisor, imposta il campo Definizione della risorsa del carico di lavoro su AppRegistry o su Tutti. Crea ruoli per tutti gli account che possiedono le risorse nella tua applicazione seguendo le linee guida in the section called “Attivazione di Trusted Advisor in IAM”.

Attivazione di AWS Trusted Advisor per un carico di lavoro

È inoltre possibile integrare AWS Trusted Advisor ed eseguirne l'attivazione singolarmente per ogni carico di lavoro per i clienti con supporto AWS Business ed Enterprise. L'integrazione di Trusted Advisor con lo AWS WA Tool non comporta costi; per i dettagli sui prezzi di Trusted Advisor, consulta Piani di supporto AWS. L'attivazione di Trusted Advisor per i carichi di lavoro può fornirti un approccio più completo, automatizzato e monitorato alla revisione e all'ottimizzazione dei carichi di lavoro di AWS. In questo modo, è possibile migliorare l'affidabilità, la sicurezza, le prestazioni e l'ottimizzazione dei costi per i carichi di lavoro.

Per attivare Trusted Advisor per un carico di lavoro

1. Per attivare Trusted Advisor, i proprietari del carico di lavoro possono utilizzare AWS WA Tool per aggiornare un carico di lavoro esistente o crearne uno nuovo scegliendo Definisci carico di lavoro.
2. Inserisci un ID account utilizzato da Trusted Advisor nel campo ID account o seleziona l'ARN di un'applicazione nel campo Applicazione oppure entrambi per attivare Trusted Advisor.
3. Nella sezione AWS Trusted Advisor, seleziona Attiva Trusted Advisor.



4. Una notifica che indica che il ruolo di servizio IAM verrà creato viene visualizzata in occasione della prima attivazione di Trusted Advisor per un carico di lavoro. Scegliendo Visualizza autorizzazioni vengono visualizzate le autorizzazioni del ruolo IAM. Puoi visualizzare il nome del

ruolo, nonché le autorizzazioni e le relazioni di attendibilità create automaticamente da JSON in IAM. Dopo la creazione del ruolo, per i successivi carichi di lavoro che attivano Trusted Advisor, viene visualizzata solo la notifica Configurazione aggiuntiva necessaria.

5. Nel menu a discesa Definizione della risorsa, puoi selezionare Metadati del carico di lavoro, AppRegistry o Tutti. La selezione effettuata nel campo Definizione della risorsa determina quali dati AWS WA Tool recupera da Trusted Advisor per fornire i controlli di stato nella revisione del carico di lavoro che corrispondono alle best practice di Well-Architected.

   Metadati del carico di lavoro: il carico di lavoro è definito dagli ID account e dalle Regioni AWS specificati nel carico di lavoro.

   AppRegistry: il carico di lavoro è definito dalle risorse (come gli stack AWS CloudFormation) presenti nell'applicazione AppRegistry associata al carico di lavoro.

   Tutti: il carico di lavoro è definito sia dai metadati del carico di lavoro che dalle risorse AppRegistry.
6. Seleziona Successivo.
7. Applica il Framework AWS Well-Architected per il tuo carico di lavoro e scegli Definisci carico di lavoro. I controlli di Trusted Advisor sono collegati solo al Framework AWS Well-Architected e non ad altri obiettivi.

Lo AWS WA Tool recupera periodicamente i dati da Trusted Advisor utilizzando i ruoli creati in IAM. Il ruolo IAM viene creato automaticamente per il proprietario del carico di lavoro. Tuttavia, per visualizzare le informazioni di Trusted Advisor, i proprietari di qualsiasi account associato al carico di lavoro devono aprire IAM e creare un ruolo; per maggiori dettagli, consulta ???. Se il ruolo non esiste, lo AWS WA Tool non può ottenere le informazioni di Trusted Advisor per tale account e visualizza un errore.

Per ulteriori informazioni sulla creazione di un ruolo in AWS Identity and Access Management (IAM), consulta Creating a role for an AWS service (console) nella Guida per l'utente di IAM.

Attivazione di Trusted Advisor per un carico di lavoro in IAM

> **Note**
>
> I proprietari dei carichi di lavoro devono attivare l'opzione Attiva supporto all'individuazione per il relativo account prima di creare un carico di lavoro di Trusted Advisor. La scelta di

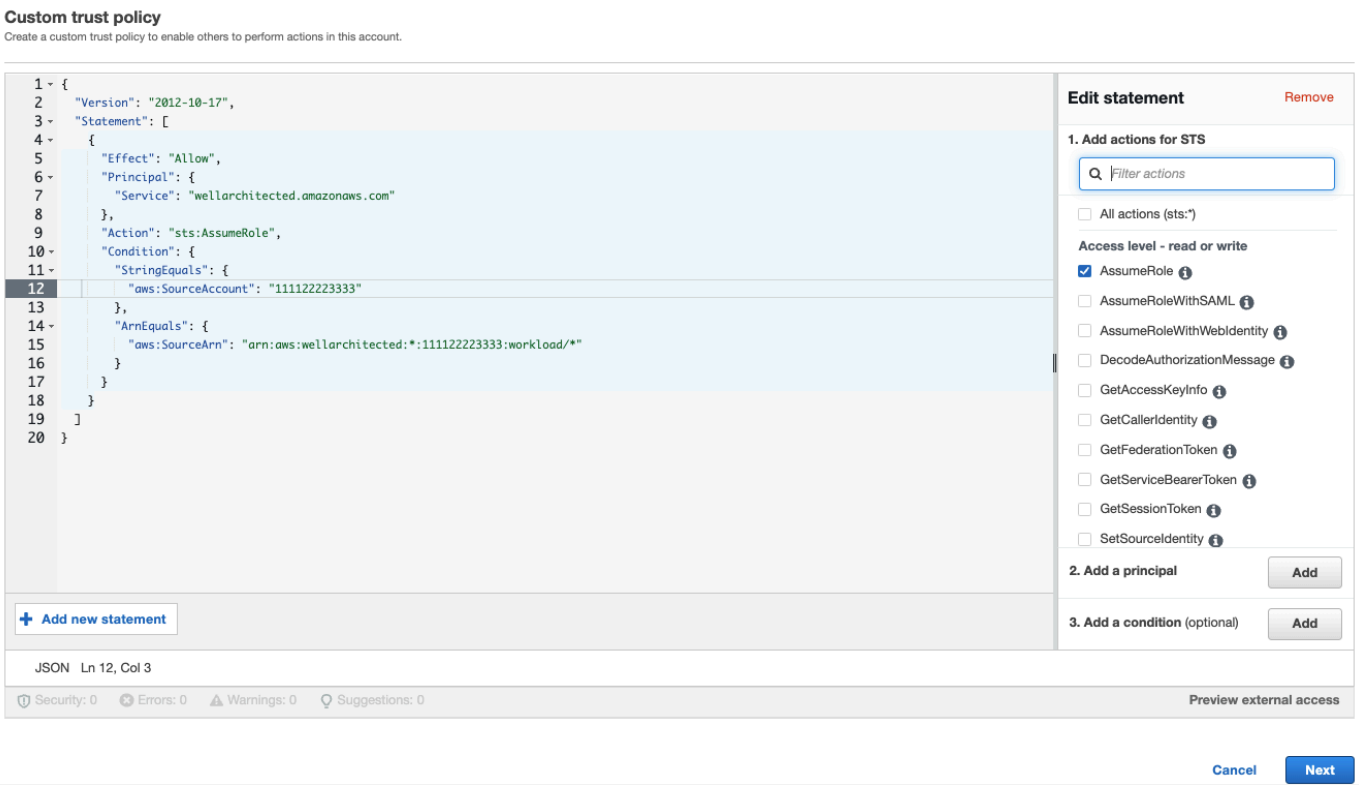
attivare l'opzione Attiva supporto all'individuazione crea il ruolo richiesto per il proprietario del carico di lavoro. Utilizza la seguente procedura per tutti gli altri account associati.

I proprietari degli account associati per i carichi di lavoro che hanno attivato Trusted Advisor devono creare un ruolo in IAM per visualizzare le informazioni di Trusted Advisor nello AWS Well-Architected Tool.

Per creare un ruolo in IAM affinché lo AWS WA Tool ottenga informazioni da Trusted Advisor

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegli Ruoli e poi Crea ruolo.
3. Sotto Tipo di entità attendibile scegli Policy di attendibilità personalizzata.
4. Copia e incolla la seguente policy di attendibilità personalizzata nel campo JSON della console IAM, come mostrato nell'immagine seguente. Sostituisci *WORKLOAD_OWNER_ACCOUNT_ID* con l'ID account del proprietario del carico di lavoro e scegli Avanti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "wellarchitected.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
        },
        "ArnEquals": {
          "aws:SourceArn":
 "arn:aws:wellarchitected:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"
        }
      }
    }
  ]
}
```



Note

Il valore `aws:sourceArn` nel blocco condizione della precedente policy di attendibilità personalizzata corrisponde a `"arn:aws:wellarchitected:*:`*WORKLOAD_OWNER_ACCOUNT_ID*`:workload/*"`, che è una condizione generica che indica che il ruolo può essere utilizzato dallo AWS WA Tool per tutti i carichi di lavoro del proprietario del carico di lavoro in questione. Tuttavia, l'accesso può essere limitato a uno specifico ARN del carico di lavoro o a un set di ARN del carico di lavoro. Per specificare più ARN, vedi la seguente policy di attendibilità di esempio.

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

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn": [

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_1",

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. Nella pagina Aggiungi autorizzazioni, per Policy di autorizzazione scegli Crea policy per concedere allo AWS WA Tool l'accesso ai dati in lettura da Trusted Advisor. Selezionando Crea policy si apre una nuova finestra.

> **Note**
>
> Inoltre, è possibile ignorare la creazione delle autorizzazioni durante la creazione del ruolo e creare una policy inline dopo la creazione del ruolo. Scegli Visualizza ruolo nel messaggio relativo alla corretta creazione del ruolo e seleziona Crea policy inline nel menu a discesa Aggiungi autorizzazioni della scheda Autorizzazioni.

6. Copia e incolla la seguente policy di autorizzazione nel campo JSON. Nell'ARN di `Resource`, sostituisci *YOUR_ACCOUNT_ID* con il tuo ID account, specifica la Regione o un asterisco (*) e scegli Prossimo:Tag.

   Per maggiori dettagli sui formati ARN, consulta Amazon Resource Name (ARN) in Riferimenti generali di AWS.

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

```
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeCheckRefreshStatuses",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeRiskResources",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeRisk",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeRisks",
                "trustedadvisor:DescribeCheckItems"
            ],
            "Resource": [
              "arn:aws:trustedadvisor:*:YOUR_ACCOUNT_ID:checks/*"
            ]
        }
    ]
}
```

7. Se Trusted Advisor è attivato per un carico di lavoro e nel campo Definizione della risorsa è stato selezionato AppRegistry o Tutti, tutti gli account che possiedono una risorsa nell'applicazione AppRegistry collegate al carico di lavoro devono aggiungere la seguente autorizzazione alla policy di autorizzazione del proprio ruolo Trusted Advisor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListAssociatedResources",
                "tag:GetResources",
                "servicecatalog:GetApplication",
                "resource-groups:ListGroupResources",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources"
            ],
            "Resource": "*"
        }
    ]
}
```

8. (Facoltativo) Aggiungi tag. Scegli Prossimo: Rivedi.

9. Controlla la policy, assegnale un nome e seleziona Crea policy.
10. Nella pagina Aggiungi autorizzazioni del ruolo, seleziona il nome della policy che hai appena creato, quindi seleziona Avanti.
11. Inserisci il nome del ruolo, che deve utilizzare la seguente sintassi: `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*. Quindi scegli Crea ruolo. Sostituisci *`WORKLOAD_OWNER_ACCOUNT_ID`* con l'ID account del proprietario del carico di lavoro.

    Nella parte superiore della pagina dovrebbe comparire un messaggio di operazione riuscita che indica che il ruolo è stato creato.
12. Per visualizzare il ruolo e la policy di autorizzazione associata, nel pannello di navigazione sinistro sotto Gestione degli accessi, scegli Ruoli e cerca il nome di `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*. Seleziona il nome del ruolo per verificare che le autorizzazioni e le relazioni di attendibilità siano corrette.

Disattivazione di Trusted Advisor per un carico di lavoro

Per disattivare Trusted Advisor per un carico di lavoro

Puoi disattivare Trusted Advisor per qualsiasi carico di lavoro dallo AWS Well-Architected Tool modificando il carico di lavoro e deselezionando Attiva Trusted Advisor. Per ulteriori informazioni sulla modifica dei carichi di lavoro, consulta the section called “Modifica un carico di lavoro”.

La disattivazione di Trusted Advisor dallo AWS WA Tool non comporta l'eliminazione dei ruoli creati in IAM. L'eliminazione dei ruoli da IAM richiede una misura di pulizia separata. I proprietari dei carichi di lavoro o i proprietari degli account associati devono eliminare i ruoli IAM creati quando Trusted Advisor è disattivato nello AWS WA Tool o arrestare la raccolta dei dati di Trusted Advisor dati per il carico di lavoro da parte di AWS WA Tool.

Per eliminare **`WellArchitectedRoleForTrustedAdvisor`** in IAM

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegli Ruoli.
3. Cerca `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* e seleziona il nome del ruolo.

4. Scegli Elimina. Nella finestra pop-up, digita il nome del ruolo per confermare l'eliminazione e seleziona nuovamente Elimina.

Per ulteriori informazioni sull'eliminazione di un ruolo da IAM, consulta Deleting an IAM role (console) nella Guida per l'utente di IAM.

Definizione di un carico di lavoro in AWS WA Tool

Un carico di lavoro è un set di componenti che garantiscono valore aziendale. Esempi di carichi di lavoro includono siti web di marketing, siti web di e-commerce, il backend per un'app per dispositivi mobili e piattaforme di analisi. La definizione accurata di un carico di lavoro aiuta a garantire una revisione completa rispetto ai pilastri del Framework AWS Well-Architected.

Per definire un carico di lavoro

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Se si utilizza AWS WA Tool per la prima volta, verrà visualizzata una pagina che presenta le caratteristiche del servizio. Nella sezione Define a workload (Definisci un carico di lavoro), scegliere Define workload (Definisci carico di lavoro).

   In alternativa, nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro) e selezionare Define workload (Definisci carico di lavoro).

   Per informazioni dettagliate su come AWS utilizza i dati dei carichi di lavoro, scegli Why does AWS need this data, and how will it be used? (Perché AWS ha bisogno di questi dati e come verranno utilizzati?).
3. Nella casella Name (Nome), immettere un nome per il carico di lavoro.

   > **Note**
   >
   > Il nome deve contenere da 3 a 100 caratteri. Almeno tre caratteri non devono essere costituiti da spazi. I nomi dei carichi di lavoro devono essere univoci. Spazi e maiuscole vengono ignorati durante la verifica dell'unicità.

4. Nella casella Description (Descrizione), immettere una descrizione del carico di lavoro. La descrizione deve contenere da 3 a 250 caratteri.

5. Nella casella Review owner (Proprietario revisione), immettere il nome, l'indirizzo di posta elettronica o l'identificatore del gruppo primario o del singolo a cui appartiene il processo di revisione del carico di lavoro.
6. Nella casella Environment (Ambiente), scegliere l'ambiente per il carico di lavoro:
   - Production (Produzione): il carico di lavoro viene eseguito in un ambiente di produzione.
   - Pre-production (Pre-produzione): il carico di lavoro viene eseguito in un ambiente di pre-produzione.
7. Nella sezione Regions (Regioni), scegliere le regioni per il carico di lavoro:
   - Regioni AWS (Regioni AWS): scegli le Regioni AWS in cui viene eseguito il carico di lavoro, una alla volta.
   - Non-AWS regions (Regioni non AWS): inserisci i nomi delle Regioni al di fuori di AWS in cui viene eseguito il carico di lavoro. È possibile specificare fino a 5 Regioni univoche, separate da virgole.

   Utilizzare entrambe le opzioni se appropriato per il carico di lavoro.
8. (Facoltativo) Nella casella ID account, inserisci gli ID degli Account AWS associati al carico di lavoro. È possibile specificare fino a 100 ID account univoci, separati da virgole.

   Se Trusted Advisor è attivato, tutti gli ID account specificati vengono utilizzati per ottenere dati da Trusted Advisor. Consulta Attivazione di AWS Trusted Advisor per un carico di lavoro per concedere allo AWS WA Tool le autorizzazioni per recuperare i dati di Trusted Advisor per tuo conto all'interno di IAM.
9. (Facoltativo) Nella casella Applicazione, inserisci l'ARN di un'applicazione dal AWS Service Catalog AppRegistry che desideri associare al carico di lavoro. È possibile specificare un solo ARN per ogni carico di lavoro; l'applicazione e il carico di lavoro devono trovarsi nella stessa Regione.
10. (Facoltativo) Nella casella Architectural design (Progettazione dell'architettura) immettere l'URL della progettazione dell'architettura.
11. (Opzionale) Nella casella Industry type (Tipo di settore), scegliere il tipo di settore associato al carico di lavoro.
12. (Opzionale) Nella casella Industry (Settore), scegliere il settore corrispondente al carico di lavoro.
13. (Facoltativo) Nella sezione Trusted Advisor, per attivare i controlli di Trusted Advisor per il tuo carico di lavoro, seleziona Attiva Trusted Advisor. Potrebbe essere necessaria una configurazione aggiuntiva per gli account associati al carico di lavoro. Consulta the section called “Attivazione di Trusted Advisor” per concedere allo AWS WA Tool le autorizzazioni per ottenere i

dati di Trusted Advisor per tuo conto. Seleziona Metadati del carico di lavoro, AppRegistry o Tutti sotto Definizione della risorsa per definire le risorse utilizzate dallo AWS WA Tool per eseguire i controlli di Trusted Advisor.

14. (Facoltativo) Nella sezione Jira, per attivare le impostazioni di sincronizzazione di Jira a livello di carico di lavoro, seleziona Sostituisci le impostazioni a livello di account. Potrebbe essere necessaria una configurazione aggiuntiva per gli account associati al carico di lavoro. Consulta AWS Well-Architected Tool Connector for Jira per iniziare l'impostazione e configurare il connettore. Seleziona Non sincronizzare il carico di lavoro, Sincronizza il carico di lavoro - Manuale o Sincronizza il carico di lavoro - Automatico e (facoltativamente) inserisci una chiave di progetto Jira con cui eseguire la sincronizzazione.

> **Note**
>
> Se le impostazioni a livello di account non vengono sovrascritte, i carichi di lavoro utilizzeranno per impostazione predefinita l'impostazione di sincronizzazione di Jira a livello di account.

15. (Facoltativo) Nella sezione Tag aggiungi eventuali tag che desideri associare al carico di lavoro.

    Per ulteriori informazioni sui tag, consulta Tagging delle risorse AWS WA Tool.

16. Seleziona Next (Successivo).

    Se una casella obbligatoria è vuota o se un valore specificato non è valido, è necessario correggere il problema prima di continuare.

17. (Facoltativo) Nel passaggio Applica profilo, associa un profilo al carico di lavoro selezionando un profilo esistente, cercando il nome del profilo o scegliendo Crea profilo per creare un profilo. Seleziona Next (Successivo).

18. Scegliere l'approfondimento che si applica a questo carico di lavoro. È possibile aggiungere fino a 20 obiettivi a un carico di lavoro. Per le descrizioni degli obiettivi AWS ufficiali, consulta Lenses.

    È possibile selezionare Obiettivi personalizzati (obiettivi creati da te o condivisi con il tuo Account AWS) o Catalogo Lens (obiettivi AWS ufficiali disponibili per tutti gli utenti) oppure entrambi.

> **Note**
>
> La sezione Obiettivi personalizzati è vuota se non hai creato un obiettivo personalizzato o se non ne è stato condiviso uno con te.

> **Dichiarazione di non responsabilità**
>
> Consultando e/o applicando gli obiettivi personalizzati creati da un altro utente o account AWS, accetti che gli obiettivi personalizzati creati da altri utenti e condivisi con te sono Contenuti di terze parti come definiti nel Contratto clienti AWS.

19. Scegliere Define workload (Definisci carico di lavoro).

    Se una casella obbligatoria è vuota o se un valore specificato non è valido, è necessario correggere il problema prima che il carico di lavoro sia definito.

Documentazione di un carico di lavoro in AWS WA Tool

Dopo aver definito un carico di lavoro in AWS Well-Architected Tool, puoi documentarne lo stato aprendo la pagina Carico di lavoro analizzato. Questo ti aiuta a valutare il carico di lavoro e a monitorarne lo stato di avanzamento nel tempo.

Per documentare lo stato di un carico di lavoro

1. Dopo aver definito inizialmente il carico di lavoro, viene visualizzata una pagina che mostra i dettagli correnti del carico di lavoro. Scegli Start reviewing (Inizia la revisione) per iniziare.

   In alternativa, nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro) e selezionare il nome del carico di lavoro per aprire la pagina dei dettagli del carico di lavoro. Scegli Continue reviewing (Continua la revisione).

   (Facoltativo) Se al carico di lavoro è associato un profilo, il pannello di navigazione a sinistra contiene un elenco di domande prioritarie per la revisione dei carichi di lavoro, che puoi utilizzare per velocizzare il processo di revisione del tuo carico di lavoro.
2. Ora viene visualizzata la prima domanda. Per ogni domanda:

   a. Leggere la domanda e determinare se è valida per il carico di lavoro in esame.

      Per ulteriori informazioni, scegliere Info (Informazioni) e visualizzare le informazioni nel pannello di aiuto.

      - Se la domanda non è valida per il carico di lavoro in uso, scegliere Question does not apply to this workload (Domanda non valida per questo carico di lavoro).

- In caso contrario, selezionare le best practice che si stanno attualmente seguendo dall'elenco.

  Se attualmente non viene seguita alcuna best practice, scegliere None of these (Nessuna di queste).

Per ulteriori informazioni su qualsiasi voce, scegliere Info (Informazioni) e visualizzare le informazioni nel pannello di aiuto.

b. (Facoltativo) Se una o più best practice non si applicano a un determinato carico di lavoro, scegliere Mark best practice(s) that don't apply to this workload (Contrassegna best practice non applicabili al carico di lavoro) e selezionarle. Per ogni best practice selezionata, è facoltativamente possibile selezionare un motivo e fornire ulteriori dettagli.

c. (Facoltativo) Utilizzare la casella Notes (Note) per registrare informazioni correlate alla domanda.

   Ad esempio, è possibile descrivere il motivo per cui la domanda non è applicabile o fornire ulteriori dettagli sulle best practice selezionate.

d. Scegliere Next (Successivo) per passare alla domanda successiva.

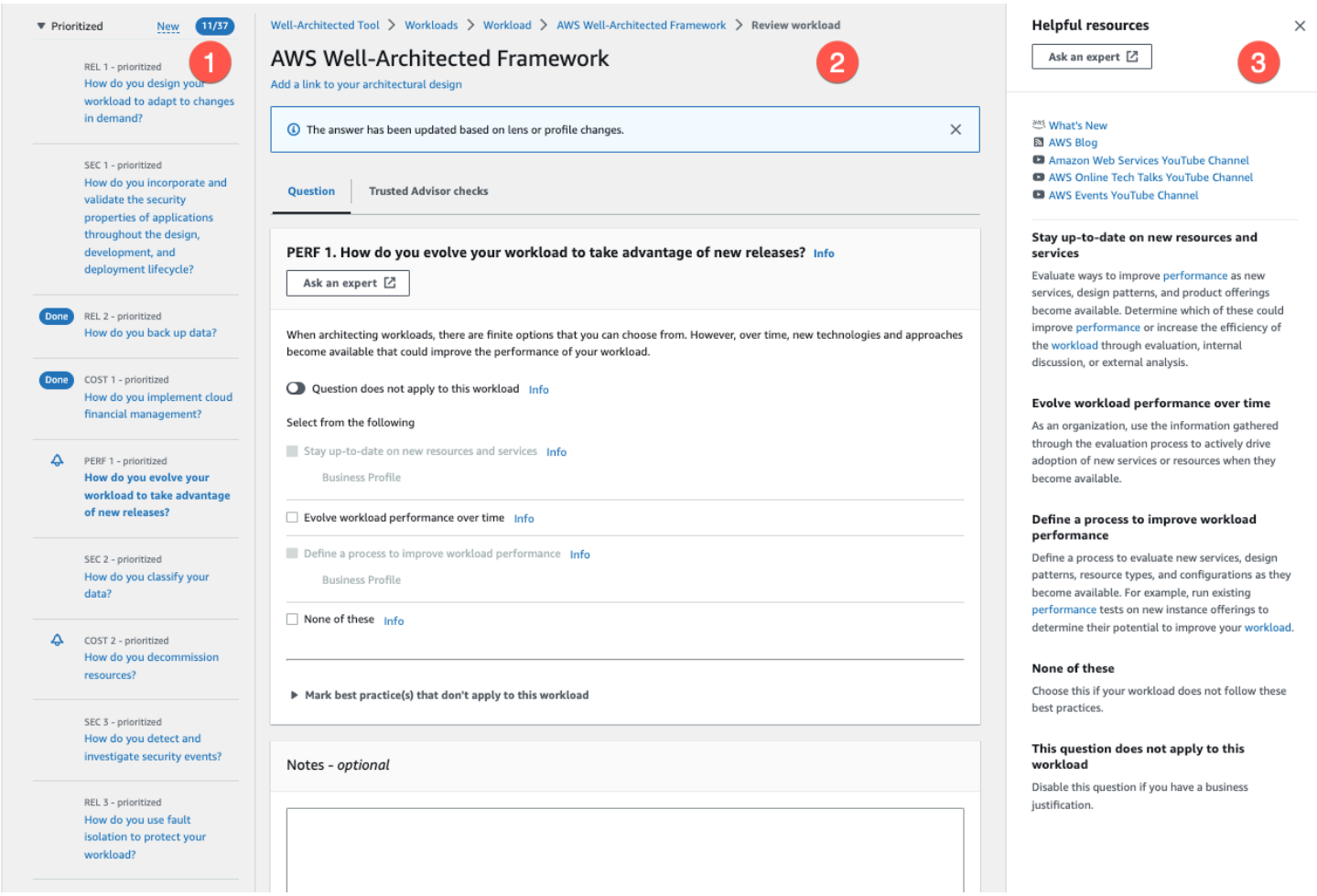
Ripeti questi passaggi per ogni domanda in ogni pilastro.

3. Scegliere Save and exit (Salva ed esci) in qualsiasi momento per salvare le modifiche e sospendere la documentazione del carico di lavoro.

Dopo aver documentato il carico di lavoro desiderato, è possibile tornare alle domande per continuare a rivederlo in qualsiasi momento. Per ulteriori informazioni, consulta Revisione di un carico di lavoro con il Framework AWS Well-Architected.

Revisione di un carico di lavoro con il Framework AWS Well-Architected

Puoi rivedere il tuo carico di lavoro nella pagina Carico di lavoro analizzato della Console. Questa pagina illustra le best practice e offre risorse utili per le prestazioni del carico di lavoro.



1. Per aprire la pagina Carico di lavoro analizzato, dalla pagina dei dettagli del carico di lavoro, scegli Continua l'analisi. Il pannello di navigazione a sinistra mostra le domande per ogni pilastro. Le domande a cui hai risposto sono contrassegnate come Fatto. Il numero di domande con risposta in ciascun pilastro viene visualizzato accanto al nome del pilastro.

   Puoi passare alle domande in altri pilastri scegliendo il nome del pilastro e quindi la domanda cui desideri rispondere.

   (Facoltativo) Se al carico di lavoro è associato un profilo, lo AWS WA Tool utilizza le informazioni del profilo per determinare quali domande di revisione del carico di lavoro sono prioritarie e quali invece non sono applicabili alla tua azienda. Nel pannello di navigazione a sinistra puoi utilizzare le domande prioritarie per velocizzare il processo di revisione del carico di lavoro. Un'icona di notifica viene visualizzata accanto alle domande che sono state appena aggiunte all'elenco delle domande prioritarie.
2. Nel pannello centrale, viene visualizzata la domanda corrente. Seleziona le best practice che stai seguendo. Scegli Info (Informazioni) per ottenere ulteriori informazioni sulla domanda o una

best practice. Scegli Chiedi a un esperto per accedere alla community AWS re:Post dedicata a AWS Well-Architected. AWS re:Post è una community con domande e risposte raggruppate per argomento che sostituisce i forum AWS. Con re:POST puoi trovare risposte, rispondere a domande, unirti a un gruppo, seguire argomenti popolari e votare le tue domande e risposte preferite.

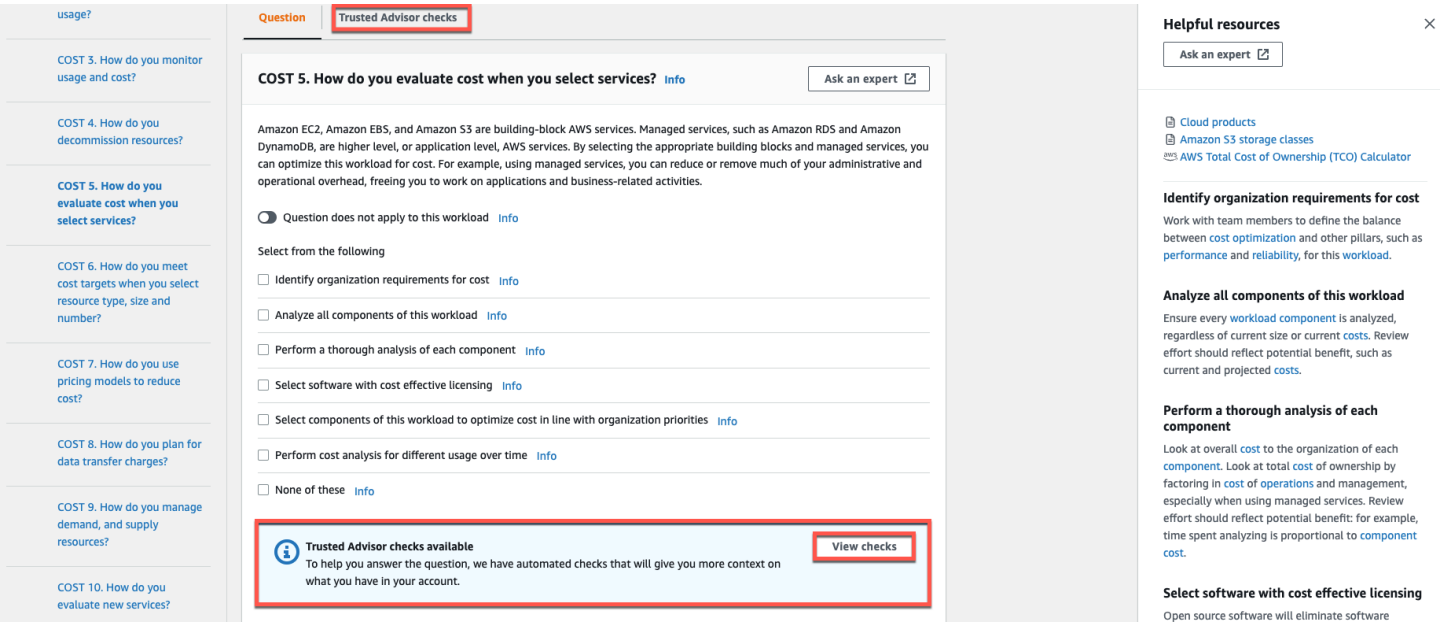
(Facoltativo) Per contrassegnare una o più best practice come non applicabili, scegli Mark best practice(s) that don't apply to this workload (Contrassegna best practice non applicabili al carico di lavoro) e seleziona le best practice desiderate.

Utilizza i pulsanti nella parte inferiore di questo pannello per passare alla domanda successiva, tornare alla domanda precedente o salvare le modifiche e uscire.

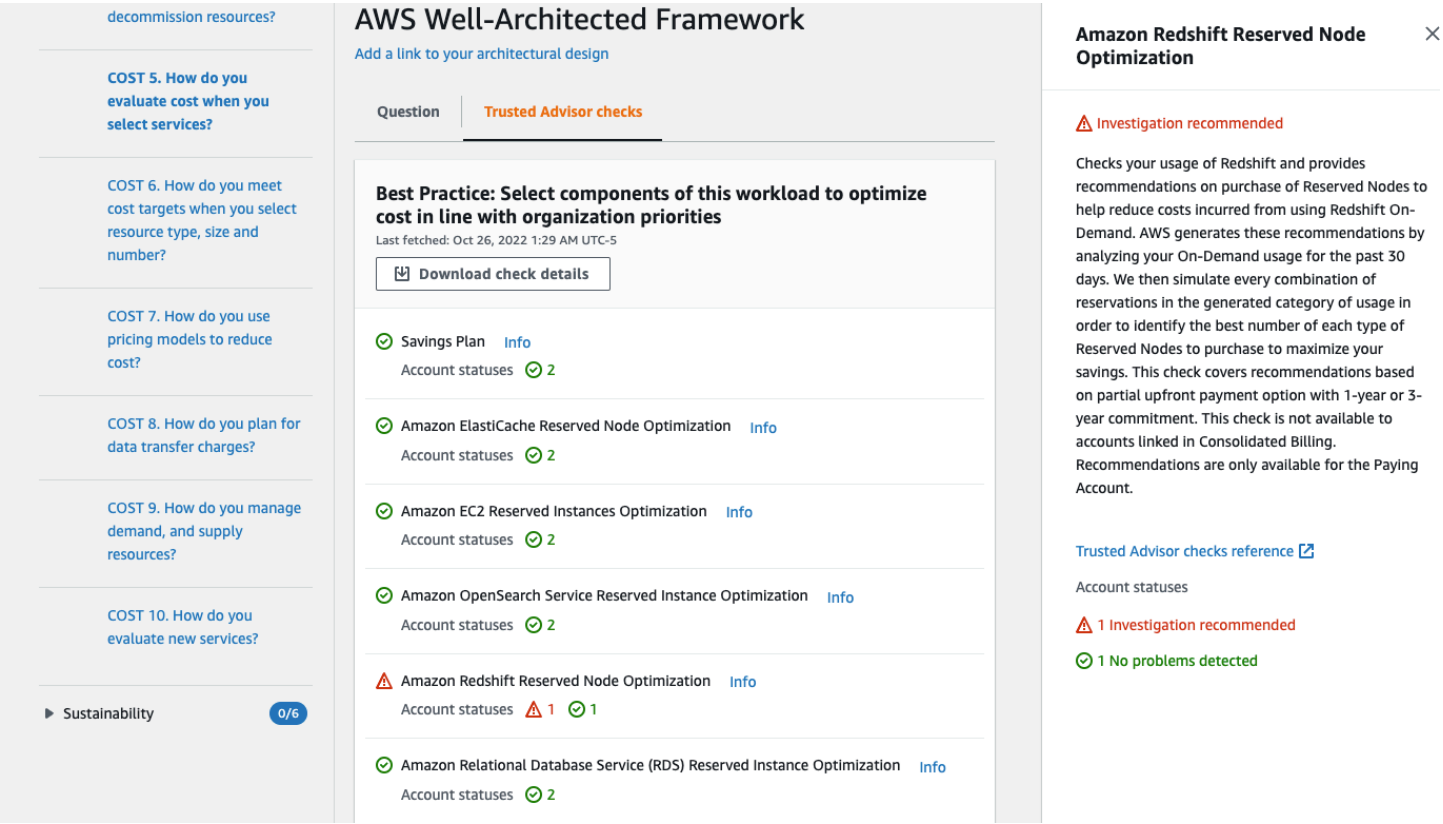
3. Nel pannello a destra, vengono visualizzate ulteriori informazioni e risorse utili. Scegli Chiedi a un esperto per accedere alla community AWS re:POST dedicata a AWS Well-Architected. In questa community puoi porre domande relative alla progettazione, alla creazione, all'implementazione e alla gestione dei carichi di lavoro su AWS.

Visualizzazione dei controlli di Trusted Advisor per un carico di lavoro

Se Trusted Advisor è attivato per il tuo carico di lavoro, viene visualizzata una scheda dei controlli di Trusted Advisor accanto a Domanda. Se per la best practice sono disponibili dei controlli, dopo la selezione della domanda viene visualizzata una notifica che indica che sono disponibili dei controlli di Trusted Advisor. Selezionando Visualizza i controlli si passa alla scheda dei controlli di Trusted Advisor.



Nella scheda dei controlli di Trusted Advisor, puoi visualizzare informazioni più dettagliate sui controlli relativi alle best practice di Trusted Advisor, visualizzare i collegamenti alla documentazione di Trusted Advisor nel pannello delle risorse di aiuto oppure scegliere Scarica i dettagli dei controlli per scaricare un report dei controlli di Trusted Advisor e degli stati di ciascuna best practice sotto forma di file CSV.



Le categorie dei controlli di Trusted Advisor sono visualizzate come icone colorate e il numero accanto a ciascuna icona indica il numero di account che hanno tale stato.

- Operazione 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 un 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.

Per ulteriori informazioni sui controlli di Trusted Advisor, consulta View check categories nella Guida per l'utente di Supporto.

Selezionando il collegamento Informazioni accanto a ciascun controllo di Trusted Advisor vengono visualizzate le informazioni relative al controllo nel pannello delle risorse di aiuto. Per ulteriori informazioni, consulta AWS Trusted Advisor check reference nella Guida per l'utente di Supporto.

Salvataggio di un milestone per un carico di lavoro in AWS WA Tool

È possibile salvare un milestone per un carico di lavoro in qualsiasi momento. Un milestone registra lo stato corrente del carico di lavoro.

Per salvare un milestone

1. Nella pagina dei dettagli del carico di lavoro, scegliere Save milestone (Salva milestone).
2. Nella casella Milestone name (Nome del milestone), immettere un nome per il milestone.

   > **Note**
   >
   > Il nome deve contenere da 3 a 100 caratteri. Almeno tre caratteri non devono essere costituiti da spazi. I nomi milestone associati a un carico di lavoro devono essere univoci. Spazi e maiuscole vengono ignorati durante la verifica dell'unicità.

3. Seleziona Salva.

Dopo il salvataggio di un milestone, non è possibile modificare i dati del carico di lavoro acquisiti in tale milestone.

Per ulteriori informazioni, consultare Milestone.

Tutorial: Documentazione e carico di AWS Well-Architected Tool lavoro

Questo tutorial descrive come AWS Well-Architected Tool documentare e misurare un carico di lavoro. Questo esempio illustra nel dettaglio come definire e documentare un carico di lavoro per un sito Web di vendita al dettaglio.

Argomenti

- Fase 1: Definire un carico di lavoro
- Fase 2: Documentare lo stato del carico di lavoro
- Fase 3: Rivedi il piano di miglioramento
- Fase 4: apportare miglioramenti e misurare i progressi

Fase 1: Definire un carico di lavoro

Per iniziare, definisci un carico di lavoro. Esistono due modi per definire un carico di lavoro. In questo tutorial, non definiamo un carico di lavoro a partire da un modello di recensione. Per maggiori dettagli sulla definizione di un carico di lavoro a partire da un modello di revisione, consulta. the section called “Definire un carico di lavoro”

Per definire un carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.

   > **Note**
   >
   > L'utente che documenta lo stato del carico di lavoro deve disporre delle autorizzazioni di accesso complete per. AWS WA Tool

2. Nella sezione Define a workload (Definisci un carico di lavoro), scegliere Define workload (Definisci carico di lavoro).
3. Nella casella Name (Nome), immettere **`Retail Website - North America`** come nome del carico di lavoro.
4. Nella casella Description (Descrizione), immettere una descrizione del carico di lavoro.

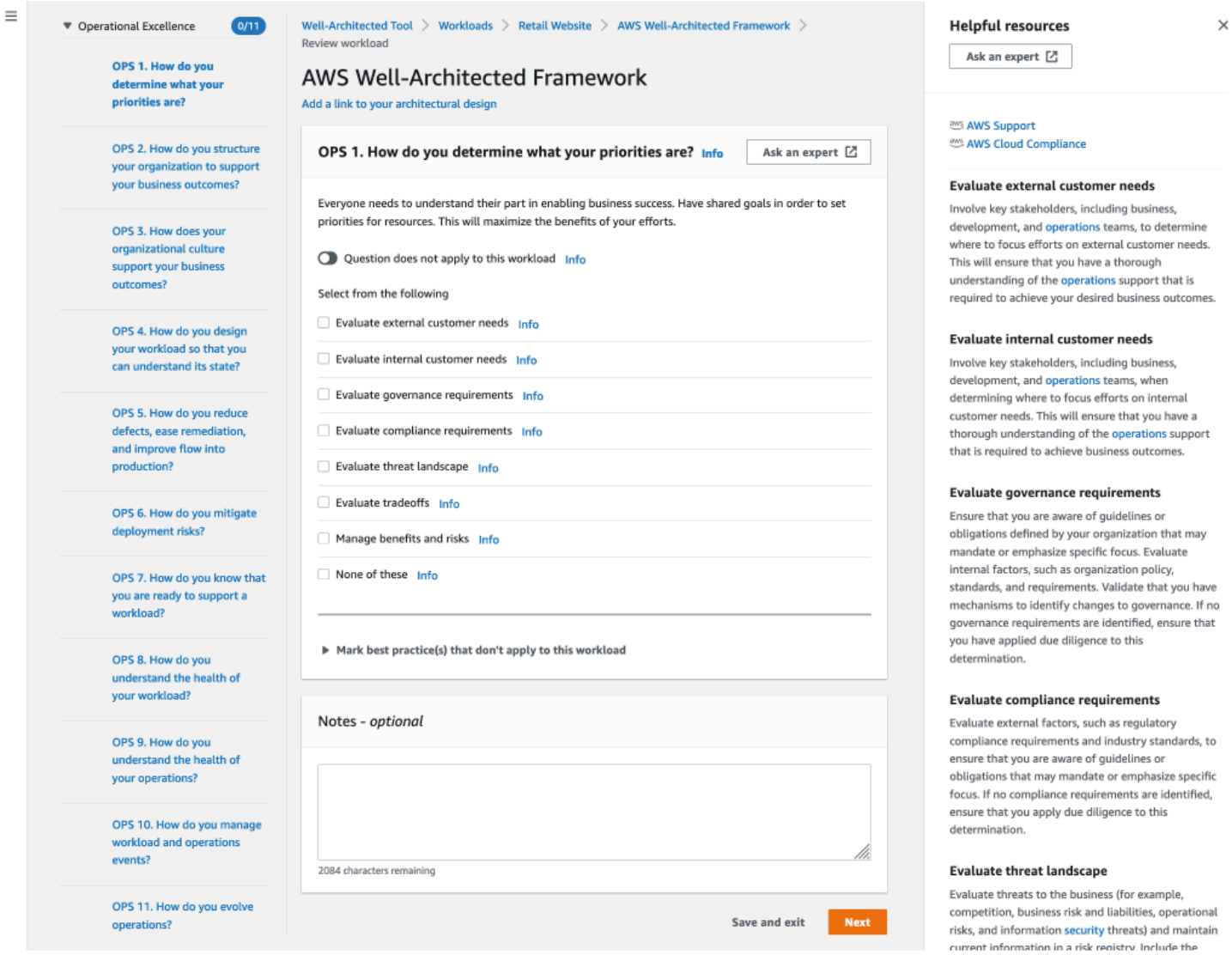
5. Nella casella Titolare della revisione, inserisci il nome della persona responsabile del processo di revisione del carico di lavoro.
6. Nella casella Ambiente, indica che il carico di lavoro si trova in un ambiente di produzione.
7. Il nostro carico di lavoro viene eseguito su entrambi AWS e presso il nostro data center locale:
    a. Seleziona Regioni AWSe scegli le due regioni del Nord America in cui viene eseguito il carico di lavoro.
    b. Seleziona anche aree non AWS geografiche e inserisci un nome per il data center locale.
8. La IDs casella Account è facoltativa. Non associarne alcuna Account AWS a questo carico di lavoro.
9. La casella Applicazione è facoltativa. Non inserire un'applicazione ARN per questo carico di lavoro.
10. La casella Diagramma architettonico è facoltativa. Non associare un diagramma architettonico a questo carico di lavoro.
11. Le caselle Industry type (Tipo di settore) e Industry (Settore) sono opzionali e non sono specificate per questo carico di lavoro.
12. La sezione Trusted Advisor è facoltativa. Non attivare il Trusted Advisor supporto per questo carico di lavoro.
13. La sezione Jira è facoltativa. Non sovrascrivere le impostazioni a livello di account nella sezione Jira per questo carico di lavoro.
14. Per questo esempio, non applicare alcun tag al carico di lavoro. Scegli Next (Successivo).
15. Il passaggio Applica profilo è facoltativo. Non applicare un profilo per questo carico di lavoro. Scegli Next (Successivo).
16. Per questo esempio, applicate l'obiettivo AWS Well-Architected Framework, che viene selezionato automaticamente. Scegliere Define workload (Definisci carico di lavoro) per salvare questi valori e definire il carico di lavoro.
17. Una volta definito il carico di lavoro, scegliere Start review (Avvia revisione) per iniziare a documentare lo stato del carico di lavoro.

Fase 2: Documentare lo stato del carico di lavoro

Per documentare lo stato del carico di lavoro, vengono poste domande per l'obiettivo selezionato che abbracciano i pilastri del AWS Well-Architected Framework: eccellenza operativa, sicurezza, affidabilità, efficienza delle prestazioni, ottimizzazione dei costi e sostenibilità.

Per ogni domanda, scegli le best practice che stai seguendo dall'elenco fornito. Se hai bisogno di ulteriori dettagli su una best practice, scegli Info (Informazioni) e visualizza ulteriori informazioni e risorse nel pannello a destra.

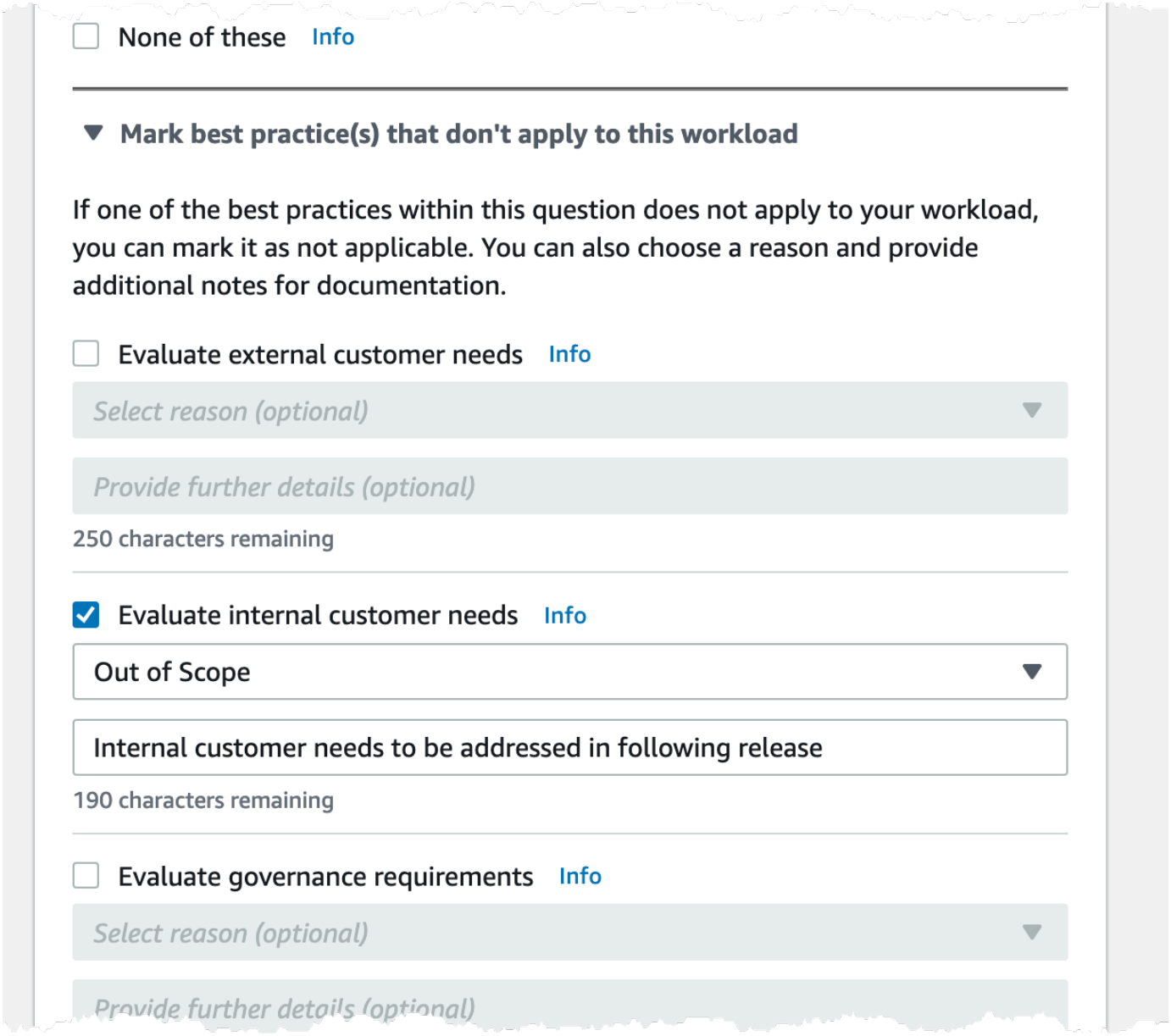
Scegli Chiedi a un esperto per accedere alla community di AWS re:POST dedicata a Well-Architected AWS . In questa community puoi porre domande relative alla progettazione, alla creazione, all'implementazione e al funzionamento dei carichi di lavoro. AWS



1. Scegliere Next (Avanti) per passare alla domanda successiva. Puoi utilizzare il pannello a sinistra per passare a un'altra domanda nello stesso pilastro o a una domanda in un altro pilastro.
2. Se scegli La domanda non si applica a questo carico di lavoro o Nessuno di questi, ti AWS consiglia di includere il motivo nella casella Note. Queste note sono incluse come parte del report

del carico di lavoro e possono essere utili in futuro quando vengono apportate modifiche al carico di lavoro.

> **Note**
>
> Facoltativamente, puoi contrassegnare una o più best practice individuali come non applicabili. Scegli Contrassegna le migliori pratiche che non si applicano a questo carico di lavoro e seleziona le migliori pratiche che non si applicano. Facoltativamente, puoi selezionare un motivo e fornire dettagli aggiuntivi. Ripetere l'operazione per ogni best practice non applicabile.



> **Note**
>
> Puoi mettere in pausa questo processo in qualsiasi momento scegliendo Salva ed esci. Per riprenderlo in un secondo momento, apri la AWS WA Tool console e scegli Carichi di lavoro nel riquadro di navigazione a sinistra.

3. Selezionare il nome del carico di lavoro per aprire la pagina dei dettagli del carico di lavoro.
4. Scegli Continue reviewing (Continua revisione) e quindi naviga fino al punto in cui la revisione è stata sospesa.

5. Dopo aver completato tutte le domande, viene visualizzata una pagina di panoramica del carico di lavoro. Puoi rivedere i dettagli ora o accedervi in seguito scegliendo Workloads (Carichi di lavoro) nel riquadro di navigazione a sinistra e selezionando il nome del carico di lavoro.

Dopo aver documentato lo stato del carico di lavoro per la prima volta, è necessario salvare un milestone e generare un report relativo al carico di lavoro.

Un milestone acquisisce lo stato corrente del carico di lavoro e consente di misurarne lo stato di avanzamento quando si apportano modifiche in base al piano di miglioramento.

Dalla pagina dei dettagli del carico di lavoro:

1. Nella sezione Panoramica del carico di lavoro, scegli il pulsante Salva traguardo.
2. Inserisci **`Version 1.0 - initial review`** come nome della pietra miliare.
3. Seleziona Salva.
4. Per generare un rapporto sul carico di lavoro, seleziona l'obiettivo desiderato e scegli Genera rapporto e viene creato un PDF file. Questo file contiene lo stato del carico di lavoro, il numero di rischi identificati e un elenco di miglioramenti suggeriti.

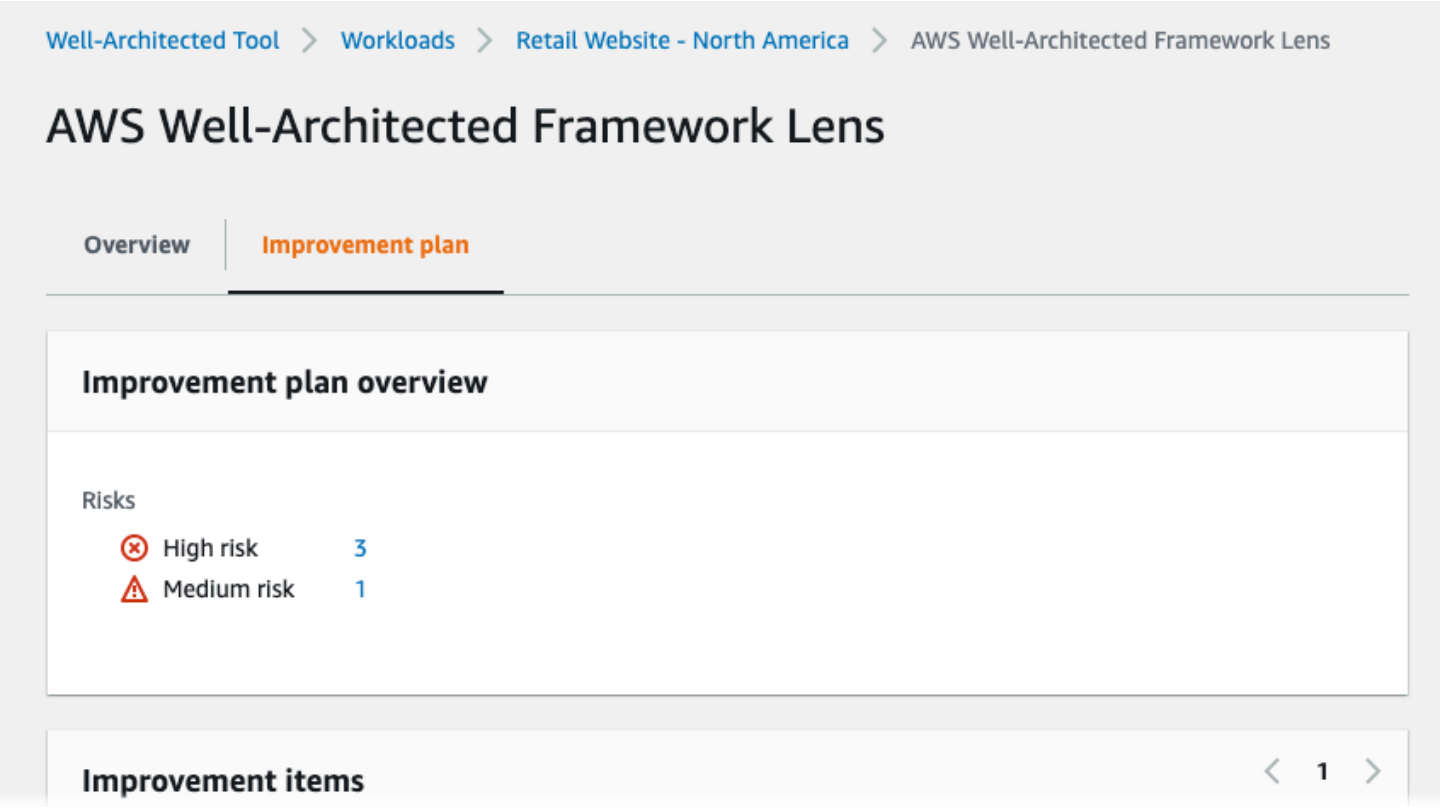
Fase 3: Rivedi il piano di miglioramento

Sulla base delle migliori pratiche selezionate, AWS WA Tool identifica le aree ad alto e medio rischio misurate rispetto allo standard AWS Well-Architected Framework Lens.

Per rivedere il piano di miglioramento:

1. Scegliete AWS Well-Architected Framework dalla sezione Lenti della pagina Panoramica.
2. Quindi scegli Improvement plan (Piano di miglioramento).

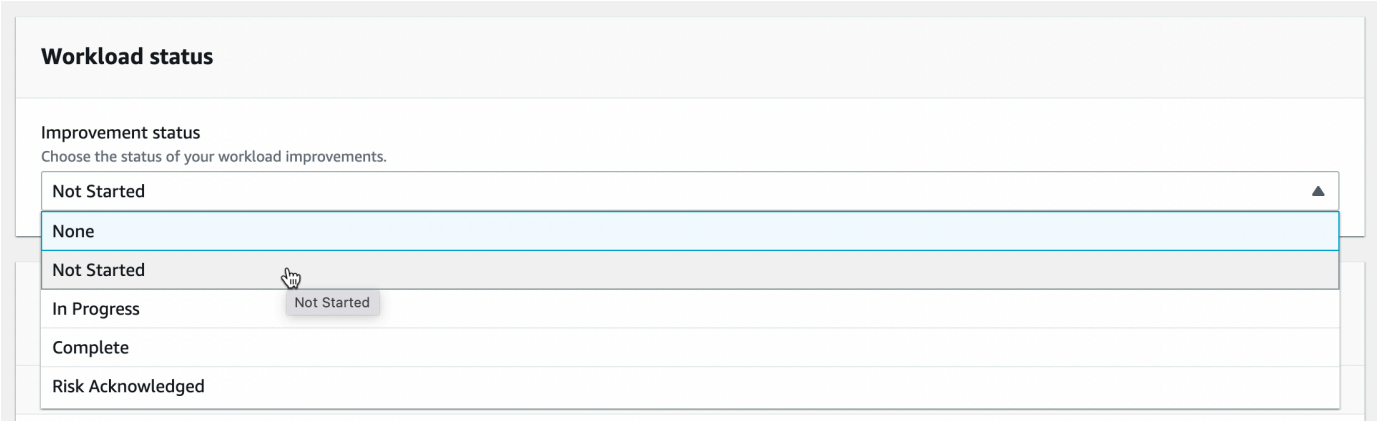
Per questo particolare esempio di carico di lavoro, il AWS Well-Architected Framework Lens ha identificato tre problemi ad alto rischio e uno a rischio medio.



Aggiorna lo stato di miglioramento del carico di lavoro per indicare che non sono stati avviati miglioramenti al carico di lavoro.

Per modificare lo stato di miglioramento:

1. Dal piano di miglioramento, fai clic sul nome del carico di lavoro (**`Retail Website - North America`**) nella barra di navigazione nella parte superiore della pagina.
2. Fate clic sulla scheda Proprietà.
3. Vai alla sezione Stato del carico di lavoro e seleziona Non avviato dall'elenco a discesa.



4. Torna al piano di miglioramento dalla scheda Proprietà facendo clic sulla scheda Panoramica e quindi facendo clic sul collegamento AWS Well-Architected Framework nella sezione Lenses. Quindi fai clic sulla scheda Piano di miglioramento nella parte superiore della pagina.

La sezione Improvement items (Elementi di miglioramento) mostra gli elementi di miglioramento consigliati identificati nel carico di lavoro. Le domande sono ordinate in base alla priorità dei pilastri impostata, con gli eventuali problemi a rischio elevato visualizzati per primi seguiti dagli eventuali problemi a rischio medio.

Espandi Recommended improvement items (Elementi di miglioramento consigliati) per mostrare le best practice relative a una domanda. Ogni operazione di miglioramento consigliato si collega a una guida esperta dettagliata per consentire di eliminare, o almeno mitigare, i rischi identificati.

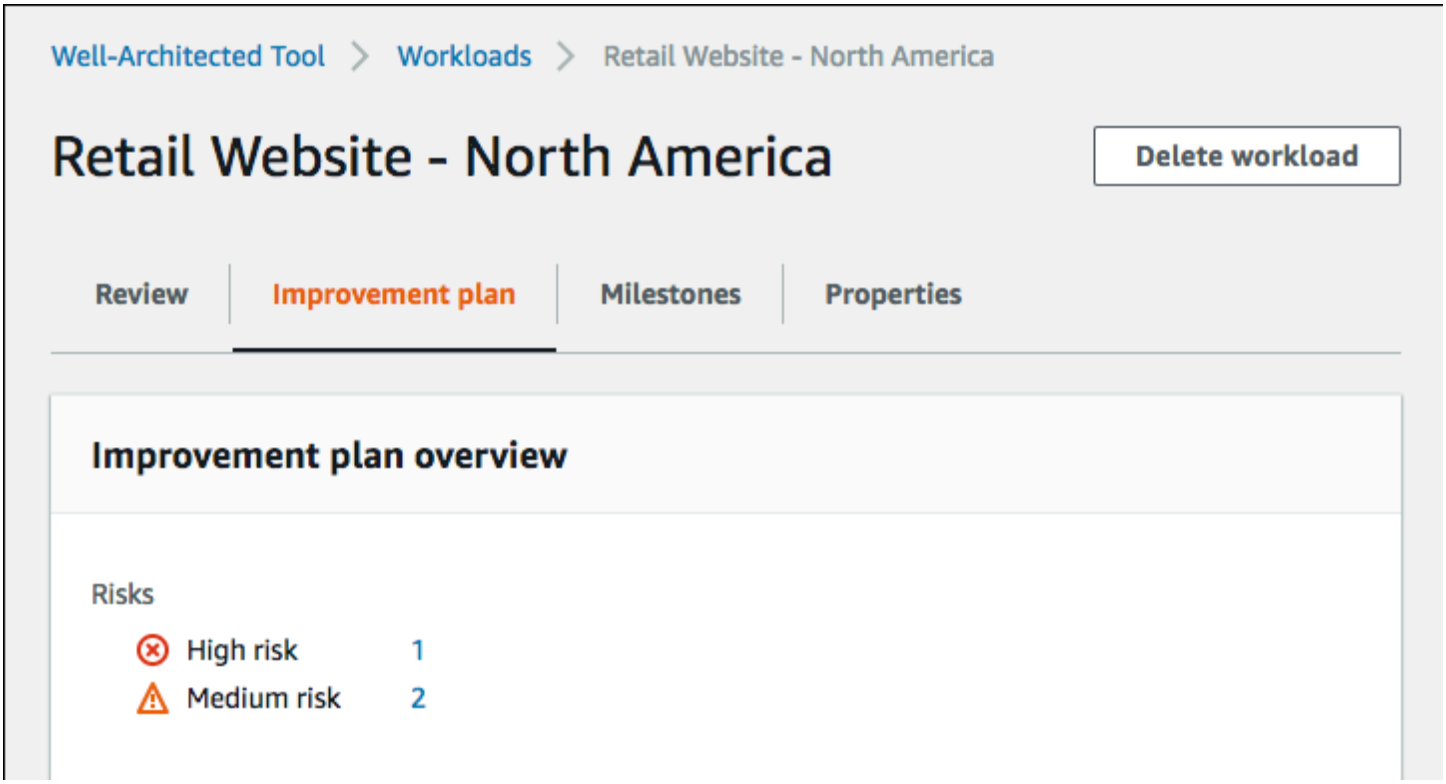
Se al carico di lavoro è associato un profilo, nella sezione Panoramica del piano di miglioramento viene visualizzato un conteggio dei rischi con priorità ed è possibile filtrare l'elenco degli elementi di miglioramento selezionando Assegna priorità per profilo. L'elenco degli elementi di miglioramento mostra un'etichetta con priorità.

Fase 4: apportare miglioramenti e misurare i progressi

Nell'ambito di questo piano di miglioramento, uno dei problemi ad alto rischio è stato risolto aggiungendo Amazon CloudWatch e AWS Auto Scaling supporto al carico di lavoro.

Dalla sezione Articoli di miglioramento:

1. Scegli la domanda pertinente e aggiorna le migliori pratiche selezionate per riflettere le modifiche. Vengono aggiunte delle note per registrare i miglioramenti.
2. Quindi scegli Salva ed esci per aggiornare lo stato del carico di lavoro.
3. Dopo aver apportato le modifiche, puoi tornare a Improvement plan (Piano di miglioramento) e vedere l'effetto delle modifiche sul carico di lavoro. In questo esempio, tali azioni hanno migliorato il profilo di rischio, riducendo il numero di problemi ad alto rischio da tre a uno solo.



A questo punto, è possibile salvare un milestone e quindi passare a Milestones (Milestone) per vedere come è stato migliorato il carico di lavoro.

Carichi di lavoro

Un carico di lavoro è una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

Un carico di lavoro può essere costituito da un sottoinsieme di risorse in un'unica risorsa Account AWS o essere una raccolta di più risorse distribuite su più risorse. Account AWS Un'azienda di piccole dimensioni potrebbe avere solo pochi carichi di lavoro mentre un'azienda di grandi dimensioni potrebbe averne migliaia.

La pagina Carichi di lavoro disponibile nella navigazione a sinistra, fornisce informazioni sui carichi di lavoro e sui carichi di lavoro condivisi con l'utente.

Le seguenti informazioni vengono visualizzate per ogni carico di lavoro:

Nome

Il nome del carico di lavoro.

Owner

L' Account AWS ID che possiede il carico di lavoro.

Le domande con risposta

Il numero di domande che hanno ricevuto una risposta.

Rischi elevati

Il numero di problemi ad alto rischio (HRIs) identificati.

Rischi medi

Il numero di problemi a rischio medio (MRIs) identificati.

Stato miglioramento

Lo stato di miglioramento impostato per il carico di lavoro:

- Nessuno
- Non avviato
- In Progress (In corso)

- Completa
- Rischio confermato

Ultimo aggiornamento

Data e ora dell'ultimo aggiornamento del carico di lavoro.

Dopo aver scelto un carico di lavoro dall'elenco:

- Per rivedere i dettagli del carico di lavoro, scegliere View details (Visualizza dettagli).
- Per modificare le proprietà del carico di lavoro, scegliere Edit (Modifica).
- Per gestire la condivisione del carico di lavoro con altri Account AWS utenti o unità organizzative (OUs), scegli Visualizza dettagli e quindi Condivisioni. AWS Organizations
- Per eliminare il carico di lavoro e tutti i relativi milestone, scegliere Delete (Elimina). Solo il proprietario del carico di lavoro può eliminarlo.

> **Warning**
>
> L'eliminazione di un carico di lavoro non può essere annullata. Tutti i dati associati al carico di lavoro vengono eliminati.

Problemi ad alto rischio (HRIs) e problemi a rischio medio () MRIs

I problemi ad alto rischio (HRIs) identificati nelle scelte architettoniche e operative che AWS Well-Architected Tool sono AWS stati rilevati potrebbero avere un impatto negativo significativo su un'azienda. Questi HRIs potrebbero influire sulle operazioni organizzative, sugli asset e sugli individui. Anche i problemi a rischio medio (MRIs) potrebbero avere un impatto negativo sull'attività, ma in misura minore. Questi problemi si basano sulle risposte fornite in AWS Well-Architected Tool. Le migliori pratiche corrispondenti sono ampiamente applicate dai clienti AWS e AWS dai clienti. Queste best practice sono le linee guida definite dal AWS Well-Architected Framework e dagli obiettivi.

> **Note**
>
> Queste sono solo linee guida e i clienti dovrebbero valutare e misurare l'impatto che la mancata implementazione potrebbe avere sulla loro attività. Se esistono ragioni tecniche

o aziendali specifiche che impediscono di applicare una best practice al carico di lavoro, il rischio potrebbe essere inferiore a quello indicato. AWS suggerisce ai clienti di documentare questi motivi e il modo in cui influiscono sulle best practice nelle note sul carico di lavoro. Per tutti i casi identificati HRIs eMRIs, AWS suggerisce ai clienti di implementare le migliori pratiche come definite nel AWS Well-Architected Tool. Se viene implementata la procedura consigliata, indicare che il problema è stato risolto contrassegnando la procedura consigliata come soddisfatta in AWS Well-Architected Tool. Se i clienti scelgono di non implementare la best practice, AWS suggerisce di documentare l'approvazione a livello aziendale applicabile e i motivi della mancata implementazione.

Definisci un carico di lavoro in AWS Well-Architected Tool

Esistono due modi per definire un carico di lavoro. Nella pagina Carichi di lavoro AWS WA Tool è possibile definire un carico di lavoro senza un modello. In alternativa, nella pagina Rivedi modelli, puoi utilizzare un modello di revisione esistente o creare un nuovo modello per definire un carico di lavoro.

Per definire un carico di lavoro dalla pagina Carichi di lavoro

1. Seleziona Carichi di lavoro nel riquadro di navigazione a sinistra.
2. Seleziona il menu a discesa Definisci carico di lavoro.
3. Scegliere Define workload (Definisci carico di lavoro). Oppure, se hai creato un modello di recensione e desideri definire un carico di lavoro in base a tale modello, scegli Definisci dal modello di revisione.
4. Segui le istruzioni the section called “Definizione di un carico di lavoro” per specificare le proprietà del carico di lavoro o (facoltativamente) applica profili e obiettivi.

Per definire un carico di lavoro dalla pagina Rivedi i modelli

1. Seleziona Rivedi modelli nel riquadro di navigazione a sinistra.
2. Seleziona il nome di un modello di recensione esistente o segui le istruzioni the section called “Creazione di un modello di recensione” per creare un nuovo modello di recensione.
3. Scegli Definisci carico di lavoro da modello.
4. Segui le istruzioni riportate the section called “Definizione di un carico di lavoro da un modello” per creare il carico di lavoro dal tuo modello di recensione.

Visualizza un carico di lavoro in AWS Well-Architected Tool

È possibile visualizzare i dettagli dei carichi di lavoro di proprietà e dei carichi di lavoro condivisi con l'utente.

Per visualizzare un carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare il carico di lavoro da visualizzare in uno dei seguenti modi:
   - Scegliere il nome del carico di lavoro.
   - Selezionare il carico di lavoro e scegliere View details (Visualizza dettagli).

Viene visualizzata la pagina dei dettagli del carico di lavoro.

> **Note**
>
> È stato aggiunto un campo obbligatorio, Review owner (Proprietario revisione), per consentire di identificare facilmente la persona o gruppo primario responsabile del processo di revisione. La prima volta che si visualizza un carico di lavoro definito prima dell'aggiunta di questo campo, si riceve una notifica di questa modifica. Scegliere Edit (Modifica) per impostare il campo Review owner (Proprietario revisione). Non sono richieste ulteriori operazioni. Scegliere Acknowledge (Conferma) per posticipare l'impostazione del campo Review owner (Proprietario revisione) . Per i prossimi 60 giorni, viene visualizzato un banner per ricordare che il campo è vuoto. Per rimuovere il banner, modificare il carico di lavoro e specificare un campo Review owner (Proprietario revisione).
> Se non imposti il campo entro la data specificata, l'accesso al carico di lavoro viene limitato. Puoi continuare a visualizzare il carico di lavoro ed eliminarlo, ma non puoi modificarlo, tranne che per impostare il campo Review owner (Proprietario revisione) . L'accesso condiviso al carico di lavoro non viene influenzato mentre l'accesso è limitato.

Modifica un carico di lavoro in AWS Well-Architected Tool

È possibile modificare i dettagli di un carico di lavoro di cui si è proprietari.

Per modificare un carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare il carico di lavoro da modificare e scegliere Edit (Modifica).
4. Apportare le modifiche al carico di lavoro.

   Per una descrizione di ognuno dei campi, consulta Definizione di un carico di lavoro in AWS WA Tool.

   > **Note**
   >
   > Quando aggiorni un carico di lavoro esistente, puoi attivare Trusted Advisor, che crea automaticamente il IAM ruolo per il proprietario del carico di lavoro. I proprietari degli account associati per i carichi di lavoro con carichi di lavoro Trusted Advisor attivati devono creare un ruolo in. IAM Per informazioni dettagliate, consultare the section called “Attivazione di Trusted Advisor in IAM”.

5. Scegliere Save (Salva) per salvare le modifiche al carico di lavoro.

   Se un campo richiesto è vuoto oppure se un valore specificato non è valido, è necessario correggere il problema prima che gli aggiornamenti al carico di lavoro vengano salvati.

Condividi un carico di lavoro in AWS Well-Architected Tool

Puoi condividere un carico di lavoro di tua proprietà con altri utenti Account AWS, un'organizzazione e le unità organizzative (OUs) all'interno della stessa Regione AWS.

> **Note**
>
> Puoi condividere i carichi di lavoro solo all'interno dello stesso. Regione AWS
> Quando condivide un carico di lavoro con un altro Account AWS, se il destinatario non dispone dell'`wellarchitected:UpdateShareInvitation`autorizzazione, non può accettare l'invito alla condivisione. the section called “Accesso allo AWS WA Tool”Per esempi di policy di autorizzazione, consulta la sezione.

Per condividere un carico di lavoro con altri Account AWS utenti

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare un carico di lavoro di cui si è proprietari in uno dei modi seguenti:
   - Scegliere il nome del carico di lavoro.
   - Selezionare il carico di lavoro e scegliere View details (Visualizza dettagli).
4. Scegli Condivisioni. Quindi scegli Crea e crea condivisioni per utenti o account per creare un invito per il carico di lavoro.
5. Inserisci l'ID a 12 cifre o l' Account AWS ID ARN dell'utente con cui desideri condividere il carico di lavoro.
6. Scegliere l'autorizzazione che si desidera concedere.

   Sola-lettura

   Fornisce l'accesso in sola lettura al carico di lavoro.

   Collaboratore

   Fornisce l'accesso di aggiornamento alle risposte e alle relative note e l'accesso di sola lettura al resto del carico di lavoro.
7. Scegli Crea per inviare un invito al carico di lavoro all'utente o all'utente specificato. Account AWS

Se l'invito al carico di lavoro non viene accettato entro sette giorni, l'invito scade automaticamente.

Se sia un utente che l'utente dispongono Account AWS entrambi di inviti per il carico di lavoro, all'utente viene applicato l'invito al carico di lavoro con l'autorizzazione di livello più alto.

> **Important**
>
> Prima di condividere un carico di lavoro con un'organizzazione o con delle unità organizzative (OUs), è necessario abilitare l'accesso. AWS Organizations

Per condividere un carico di lavoro con l'organizzazione o OUs

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare un carico di lavoro di cui si è proprietari in uno dei modi seguenti:
   - Scegliere il nome del carico di lavoro.
   - Selezionare il carico di lavoro e scegliere View details (Visualizza dettagli).
4. Scegli Condivisioni. Quindi scegli Crea e crea condivisioni per Organizations.
5. Nella pagina Crea condivisione del carico di lavoro, scegli se concedere le autorizzazioni all'intera organizzazione o a una o più. OUs
6. Scegliere l'autorizzazione che si desidera concedere.

   Sola-lettura

   Fornisce l'accesso in sola lettura al carico di lavoro.

   Collaboratore

   Fornisce l'accesso di aggiornamento alle risposte e alle relative note e l'accesso di sola lettura al resto del carico di lavoro.
7. Scegli Crea per condividere il carico di lavoro.

Per vedere chi ha condiviso l'accesso a un carico di lavoro, scegliere Condivisioni dalla pagina Visualizza i dettagli del carico di lavoro in AWS Well-Architected Tool.

Per impedire che un'entità condivida i carichi di lavoro, collegare una policy che non consenta le operazioni `wellarchitected:CreateWorkloadShare`.

Puoi anche condividere obiettivi personalizzati che possiedi con altri utenti Account AWS, con la tua organizzazione e OUs all'interno della stessa Regione AWS. Per i dettagli, fare riferimento aCondivisione di un obiettivo personalizzato in AWS WA Tool.

Considerazioni sulla condivisione AWS Well-Architected Tool dei carichi di lavoro

Un carico di lavoro può essere condiviso con un massimo di 20 diversi utenti Account AWS . Un carico di lavoro può essere condiviso solo con account e utenti che partecipano allo Regione AWS stesso carico di lavoro.

Per condividere un carico di lavoro in una regione introdotta dopo il 20 marzo 2019, sia tu che la persona condivisa Account AWS dovete abilitare la Regione in. AWS Management Console Per ulteriori informazioni, consulta AWS Global Infrastructure.

Puoi condividere un carico di lavoro con un Account AWS singolo utente in un account o entrambi. Quando condividi un carico di lavoro con un utente Account AWS, tutti gli utenti di quell'account hanno accesso al carico di lavoro. Se solo utenti specifici di un account richiedono l'accesso, segui la migliore pratica di concedere il privilegio minimo e condividi il carico di lavoro individualmente con tali utenti.

Se Account AWS sia un utente che un utente dell'account dispongono di inviti per il carico di lavoro, l'invito al carico di lavoro con le autorizzazioni di livello più elevato determina l'autorizzazione dell'utente al carico di lavoro. Se elimini l'invito al carico di lavoro per l'utente, l'accesso dell'utente è determinato dall'invito al carico di lavoro per. Account AWS Eliminare entrambi gli inviti ai carichi di lavoro per rimuovere l'accesso dell'utente al carico di lavoro.

Prima di condividere un carico di lavoro con un'organizzazione o una o più unità organizzative (OUs), è necessario abilitare l'accesso. AWS Organizations

Se condividi un carico di lavoro sia con un'organizzazione che con una o più organizzazioniOUs, l'invito al carico di lavoro con le autorizzazioni di massimo livello determina l'autorizzazione dell'account al carico di lavoro.

Per abilitare la AWS Organizations condivisione

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Scegli Abilita AWS Organizations supporto.
4. Scegliere Save settings (Salva impostazioni).

Elimina l'accesso condiviso in AWS Well-Architected Tool

È possibile eliminare un invito al carico di lavoro. L'eliminazione di un invito ai carichi di lavoro rimuove l'accesso condiviso al carico di lavoro.

Per eliminare l'accesso condiviso a un carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare il carico di lavoro in uno dei seguenti modi:
   - Scegliere il nome del carico di lavoro.
   - Selezionare il carico di lavoro e scegliere View details (Visualizza dettagli).
4. Scegli Condivisioni.
5. Selezionare l'invito al carico di lavoro da eliminare e scegliere Elimina.
6. Seleziona Elimina per confermare.

Se un utente e l'utente Account AWS hanno degli inviti al carico di lavoro, devi eliminare entrambi gli inviti al carico di lavoro per rimuovere l'autorizzazione dell'utente al carico di lavoro.

Modifica l'accesso condiviso in AWS Well-Architected Tool

È possibile modificare un invito a carichi di lavoro in sospeso o accettato.

Per modificare l'accesso condiviso a un carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo. https://console.aws.amazon.com/wellarchitected/
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare un carico di lavoro di cui si è proprietari in uno dei modi seguenti:
   - Scegliere il nome del carico di lavoro.
   - Selezionare il carico di lavoro e scegliere View details (Visualizza dettagli).
4. Scegli Condivisioni.
5. Selezionare l'invito al carico di lavoro da modificare e scegliere Modifica.
6. Scegli la nuova autorizzazione che desideri concedere all'utente Account AWS o.

Sola-lettura

Fornisce l'accesso in sola lettura al carico di lavoro.

Collaboratore

Fornisce l'accesso di aggiornamento alle risposte e alle relative note e l'accesso di sola lettura al resto del carico di lavoro.

7. Seleziona Salva.

Se l'invito al carico di lavoro modificato non viene accettato entro sette giorni, scadrà automaticamente.

Accetta e rifiuta gli inviti al carico di lavoro in AWS Well-Architected Tool

Un invito a un carico di lavoro è una richiesta di condivisione di un carico di lavoro di proprietà di un altro. Account AWS Se si accetta l'invito al carico di lavoro, il carico di lavoro viene aggiunto alle pagine Carichi di lavoro e Dashboard . Se si rifiuta l'invito al carico di lavoro, viene rimosso dall'elenco degli inviti al carico di lavoro.

Hai sette giorni per accettare un invito al carico di lavoro. Se non lo accetti entro sette giorni, l'invito scade automaticamente.

> **Note**
>
> I carichi di lavoro possono essere condivisi solo all'interno dello stesso. Regione AWS

Per accettare o rifiutare un invito al carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione sinistro scegliere Inviti ai carichi di lavoro.
3. Selezionare l'invito al carico di lavoro da accettare o rifiutare.
   - Per accettare l'invito al carico di lavoro, scegliere Accetta.

     Il carico di lavoro viene aggiunto alle pagine Carichi di lavoro e Dashboard .
   - Per rifiutare l'invito al carico di lavoro, scegliere Rifiuta.

L'invito al carico di lavoro viene rimosso dall'elenco.

Per rifiutare l'accesso condiviso dopo l'accettazione di un invito al carico di lavoro, scegliere Rifiuta condivisione dalla pagina Visualizza i dettagli del carico di lavoro in AWS Well-Architected Tool relativa al carico di lavoro.

Eliminare un carico di lavoro in AWS Well-Architected Tool

Puoi eliminare un carico di lavoro quando non è più necessario. L'eliminazione di un carico di lavoro consente di rimuovere tutti i dati associati al carico di lavoro, inclusi eventuali milestone e inviti alla condivisione del carico di lavoro. Solo il proprietario di un carico di lavoro può eliminarlo.

> **Warning**
>
> L'eliminazione di un carico di lavoro non può essere annullata. Tutti i dati associati al carico di lavoro vengono rimossi in modo permanente.

Per eliminare un carico di lavoro

1. Accedi a AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare il carico di lavoro da eliminare e scegliere Delete (Elimina).
4. Nella finestra Delete (Elimina), scegliere Delete (Elimina) per confermare l'eliminazione del carico di lavoro e dei suoi milestone.

Per impedire che un'entità elimini i carichi di lavoro, collegare una policy che non consenta le operazioni `wellarchitected:DeleteWorkload`.

Genera un rapporto sul carico di lavoro in AWS Well-Architected Tool

Puoi generare un report del carico di lavoro per un approfondimento. Il report contiene le risposte alle domande relative al carico di lavoro, le note e il numero corrente di rischi elevati e medi identificati.

Se una domanda ha uno o più rischi identificati, il piano di miglioramento associato alla domanda elenca le operazioni che è possibile effettuare per ridurre tali rischi.

Se al carico di lavoro è associato un profilo, le informazioni di panoramica del profilo e i rischi prioritari vengono visualizzati nel rapporto sul carico di lavoro.

Un report consente di condividere i dettagli relativi al carico di lavoro con altri utenti che non dispongono dell'accesso a AWS Well-Architected Tool.

Per generare un report del carico di lavoro

1. Accedi a AWS Management Console e apri la console all'indirizzo. AWS Well-Architected Tool https://console.aws.amazon.com/wellarchitected/
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare il carico di lavoro desiderato e scegliere View details (Visualizza dettagli).
4. Selezionare l'approfondimento per cui generare un report e scegliere Generate report (Genera report).

   Viene generato il report che può essere scaricato o visualizzato.

Visualizza i dettagli del carico di lavoro in AWS Well-Architected Tool

La pagina dei dettagli del carico di lavoro fornisce informazioni sul carico di lavoro, incluso i milestone, il piano di miglioramento e le condivisioni dei carichi di lavoro. Utilizza le schede nella parte superiore della pagina per raggiungere le diverse sezioni dei dettagli.

Per eliminare il carico di lavoro, scegliere Elimina carico di lavoro. Solo il proprietario di un carico di lavoro può eliminarlo.

Per rimuovere l'accesso a un carico di lavoro condiviso, scegliere Rifiuta condivisione.

Argomenti

- La scheda AWS Well-Architected Tool Panoramica
- La scheda AWS Well-Architected Tool Milestones
- La scheda AWS Well-Architected Tool Proprietà
- La scheda AWS Well-Architected Tool Condivisioni

La scheda AWS Well-Architected Tool Panoramica

Quando visualizzi inizialmente un carico di lavoro, la scheda Overview (Panoramica) è la prima informazione visualizzata. Questa scheda fornisce lo stato generale del carico di lavoro seguito dallo stato di ciascun approfondimento.

Se non hai completato tutte le domande, viene visualizzato un banner che ricorda di iniziare o continuare con la documentazione del carico di lavoro.

La sezione Workload overview (Panoramica del carico di lavoro) mostra lo stato generale corrente del carico di lavoro e le eventuali Workload notes (Note del carico di lavoro) immesse. Scegliere Edit (Modifica) per aggiornare lo stato o le note.

Per acquisire lo stato attuale del carico di lavoro, scegliere Save milestone (Salva milestone). I milestone sono immutabili e non possono essere modificati dopo che vengono salvati.

Per continuare a documentare lo stato del carico di lavoro, scegliere Start reviewing (Avvia revisione) e selezionare l'approfondimento desiderato.

La scheda AWS Well-Architected Tool Milestones

Per visualizzare i milestone per il carico di lavoro, scegliere la scheda Milestones (Milestone).

Dopo aver selezionato un milestone, scegli Generate report (Genera report) per creare il report del carico di lavoro associato al milestone. Il report contiene le risposte alle domande sul carico di lavoro, le note e il numero di rischi elevati e medi del carico di lavoro al momento del salvataggio del milestone.

Puoi visualizzare i dettagli relativi allo stato del carico di lavoro al momento di un determinato milestone in uno dei seguenti modi:

- Scegliendo il nome del milestone.
- Selezionando il milestone e scegliendo View milestone (Visualizza milestone).

La scheda AWS Well-Architected Tool Proprietà

Per visualizzare le proprietà del carico di lavoro, scegliere la scheda Properties (Proprietà). Inizialmente, queste proprietà sono i valori specificati quando è stato definito il carico di lavoro. Scegli Edit (Modifica) per apportare modifiche. Solo il proprietario del carico di lavoro può apportare modifiche.

Per le descrizioni delle proprietà, consulta Definizione di un carico di lavoro in AWS WA Tool.

La scheda AWS Well-Architected Tool Condivisioni

Per visualizzare o modificare gli inviti al carico di lavoro, scegliere la scheda Condivisioni . Questa scheda viene visualizzata solo dal proprietario di un carico di lavoro.

Le seguenti informazioni vengono visualizzate per ogni singolo Account AWS utente che ha accesso condiviso al carico di lavoro:

Principale

L' Account AWS ID o l'utente ARN con accesso condiviso al carico di lavoro.

Stato

Lo stato dell'invito al carico di lavoro.

- In attesa

  L'invito è in attesa di essere accettato o respinto. Se un invito al carico di lavoro non viene accettato entro sette giorni, scade automaticamente.
- Accettato

  L'invito è stato accettato.
- Rifiutato

  L'invito è stato respinto.
- Scaduto

  L'invito non è stato accettato o è stato respinto entro sette giorni.

Autorizzazione

L'autorizzazione concessa all'utente Account AWS o.

- Sola-lettura

  L'entità dispone di accesso in sola lettura al carico di lavoro.
- Collaboratore

  L'entità può aggiornare le risposte e le relative note e ha accesso in sola lettura al resto del carico di lavoro.

Dettagli dell'autorizzazione

Descrizione dettagliata dell’autorizzazione.

Per condividere il carico di lavoro con un altro utente Account AWS o con lo stesso utente Regione AWS, scegli Crea. Un carico di lavoro può essere condiviso con un massimo di 20 utenti EA diversi Account AWS .

Per eliminare un invito a carichi di lavoro, selezionare l'invito e scegliere Elimina.

Per modificare un invito a carichi di lavoro, selezionare l'invito e scegliere Modifica.

Utilizzo degli obiettivi in AWS WA Tool

In AWS Well-Architected Tool, gli obiettivi offrono un metodo per misurare con coerenza le proprie architetture rispetto alle best practice e individuare le aree di miglioramento. L'obiettivo Framework AWS Well-Architected viene applicato automaticamente quando viene definito un carico di lavoro.

Un carico di lavoro può avere uno o più approfondimenti applicati. Ogni approfondimento ha una propria serie di domande, best practice, note e piano di miglioramento.

Esistono due tipi di obiettivi che possono essere applicati ai carichi di lavoro: Catalogo Lens e Obiettivi personalizzati.

- Catalogo Lens: obiettivi ufficiali creati e gestiti da AWS. Il Catalogo Lens è disponibile per tutti gli utenti e non richiede alcuna installazione per essere utilizzato.
- Obiettivi personalizzati: obiettivi definiti dall'utente che non costituiscono contenuti AWS ufficiali. È possibile creare obiettivi personalizzati sulla base di propri pilastri, domande, best practice e piani di miglioramento, oltre a condividere obiettivi personalizzati con altri Account AWS.

È possibile aggiungere cinque obiettivi alla volta, con un massimo di 20 obiettivi applicati per carico di lavoro.

Se un approfondimento viene rimosso da un carico di lavoro, i dati associati all'approfondimento vengono mantenuti. I dati vengono ripristinati se si aggiunge nuovamente l'approfondimento al carico di lavoro.

Aggiunta di un obiettivo a un carico di lavoro in AWS WA Tool

L'aggiunta di un obiettivo a un carico di lavoro consente di comprendere meglio i punti di forza e di debolezza dell'architettura, determinare le aree di miglioramento e garantire che i carichi di lavoro seguano le best practice.

Per aggiungere un approfondimento a un carico di lavoro

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).

3. Selezionare il carico di lavoro desiderato e scegliere View details (Visualizza dettagli).
4. Selezionare l'obiettivo da aggiungere e scegliere Salva.

   Gli obiettivi possono essere selezionati in Obiettivi personalizzati, Catalogo Lens o entrambi.

È possibile aggiungere fino a 20 obiettivi a un carico di lavoro.

Per ulteriori informazioni sul Catalogo Lens AWS, consultare AWS Well-Architected Lenses. Non tutti i whitepaper sugli obiettivi vengono forniti come obiettivi nel Catalogo Lens.

> **Dichiarazione di non responsabilità**
>
> Consultando e/o applicando gli obiettivi personalizzati creati da un altro utente o account AWS, accetti che gli obiettivi personalizzati creati da altri utenti e condivisi con te sono Contenuti di terze parti come definiti nel Contratto clienti AWS.

Rimozione di un obiettivo da un carico di lavoro in AWS WA Tool

È possibile rimuovere un obiettivo quando non è più rilevante per il carico di lavoro.

Come rimuovere un approfondimento da un carico di lavoro

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Workloads (Carichi di lavoro).
3. Selezionare il carico di lavoro desiderato e scegliere View details (Visualizza dettagli).
4. Deselezionare l'obiettivo da rimuovere e scegliere Salva.

   L'obiettivo Framework AWS Well-Architected non può essere rimosso da un carico di lavoro.

I dati associati all'approfondimento vengono mantenuti. Se l'approfondimento viene aggiunto nuovamente al carico di lavoro, i dati vengono ripristinati.

Visualizzazione dei dettagli dell'obiettivo per un carico di lavoro in AWS WA Tool

È possibile visualizzare i dettagli dell'obiettivo nella console AWS Well-Architected Tool. Per visualizzare i dettagli su un approfondimento, selezionare l'approfondimento.

Scheda Overview (Panoramica)

La scheda Panoramica fornisce informazioni generali sull'approfondimento, ad esempio il numero di domande che hanno ricevuto una risposta. Da questa scheda è possibile continuare a rivedere un carico di lavoro, generare un report o modificare le note dell'approfondimento.

Scheda Piano di miglioramento

La scheda Piano di miglioramento fornisce un elenco di operazioni proposte per migliorare il carico di lavoro. È possibile filtrare le raccomandazioni in base al rischio e al pillar.

Scheda Condivisioni

Per un obiettivo personalizzato, la scheda Condivisioni fornisce l'elenco dei principali IAM con cui l'obiettivo è stato condiviso.

Obiettivi personalizzati per carichi di lavoro in AWS WA Tool

È possibile creare obiettivi personalizzati sulla base di propri pilastri, domande, best practice e piani di miglioramento. Gli obiettivi personalizzati vengono applicati a un carico di lavoro nello stesso modo in cui si utilizzano gli obiettivi forniti da AWS. È anche possibile condividere gli obiettivi personalizzati creati dall'utente con altri Account AWS e gli obiettivi personalizzati di proprietà di altri possono essere condivisi con l'utente.

Si possono modificare le domande per renderle personalizzate e specifiche per una particolare tecnologia, in modo da consentire di rispondere alle esigenze di governance dell'organizzazione o estendere le linee guida fornite da Framework Well-Architected e dagli obiettivi AWS. Analogamente agli obiettivi esistenti, è possibile monitorare i progressi nel tempo creando tappe fondamentali e fornire periodicamente lo stato generando report.

Argomenti

- Visualizzazione di obiettivi personalizzati in AWS WA Tool

- Creazione di un obiettivo personalizzato per un carico di lavoro in AWS WA Tool
- Visualizzazione in anteprima di un obiettivo personalizzato per un carico di lavoro in AWS WA Tool
- Pubblicazione di un obiettivo personalizzato in AWS WA Tool per la prima volta
- Pubblicazione di un aggiornamento di un obiettivo personalizzato in AWS WA Tool
- Condivisione di un obiettivo personalizzato in AWS WA Tool
- Aggiunta di tag a un obiettivo personalizzato in AWS WA Tool
- Eliminazione di un obiettivo personalizzato in AWS WA Tool
- Specificazione del formato dell'obiettivo in AWS WA Tool

Visualizzazione di obiettivi personalizzati in AWS WA Tool

È possibile visualizzare i dettagli degli obiettivi personalizzati di proprietà dell'utente e condivisi con l'utente.

Per visualizzare un obiettivo

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.

   > **Note**
   >
   > La sezione Obiettivi personalizzati è vuota se non hai creato un obiettivo personalizzato o se non ne è stato condiviso uno con te.

3. Scegliere l'obiettivo personalizzato da visualizzare:
   - Di mia proprietà: mostra gli obiettivi personalizzati creati dall'utente.
   - Condiviso con me: mostra gli obiettivi personalizzati condivisi con l'utente.
4. Selezionare l'obiettivo personalizzato da visualizzare in uno dei seguenti modi:
   - Scegliere il nome dell'obiettivo.
   - Selezionare l'obiettivo e scegliere Visualizza dettagli.

Viene visualizzata la pagina Visualizzazione dei dettagli dell'obiettivo per un carico di lavoro in AWS WA Tool.

La pagina Obiettivi personalizzati include i seguenti campi:

Nome

Nome dell'obiettivo.

Owner

L'ID dell'Account AWS proprietario dell'obiettivo personalizzato.

Stato

Lo stato PUBBLICATO indica che l'obiettivo personalizzato è stato pubblicato e può essere applicato ai carichi di lavoro o condiviso con altri Account AWS.

Lo stato BOZZA indica che l'obiettivo personalizzato è stato creato ma non è ancora stato pubblicato. Un obiettivo personalizzato deve essere pubblicato prima di poter essere applicato ai carichi di lavoro o condiviso.

Versione

Il nome della versione dell'obiettivo personalizzato.

Ultimo aggiornamento

Data e ora dell'ultimo aggiornamento dell'obiettivo personalizzato.

Creazione di un obiettivo personalizzato per un carico di lavoro in AWS WA Tool

Per creare un obiettivo personalizzato

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. Scegliere Crea obiettivo personalizzato.
4. Per scaricare il file di modello JSON scegliere Scarica file.
5. Aprire il file di modello JSON con l'editor di testo preferito e aggiungere i dati dell'obiettivo personalizzato. Questi dati includono pilastri, domande, best practice e link dei piani di miglioramento.

Fare riferimento a Specificazione del formato dell'obiettivo in AWS WA Tool per ulteriori dettagli. Un obiettivo personalizzato non può superare la dimensione di 500 KB.

6. Selezionare Scegli file per scegliere il file JSON.
7. (Facoltativo) Nella sezione Tag aggiungere eventuali tag da associare all'obiettivo personalizzato.
8. Scegliere Invia e anteprima per visualizzare l'anteprima dell'obiettivo personalizzato o Invia per inviare l'obiettivo personalizzato senza visualizzarlo in anteprima.

   Se si sceglie Invia e anteprima per l'obiettivo personalizzato, è possibile selezionare Avanti per visualizzare l'anteprima dell'obiettivo o selezionare Esci dall'anteprima per tornare a Obiettivi personalizzati.

Se la convalida non riesce, modificare il file JSON e provare a creare nuovamente l'obiettivo personalizzato.

Una volta che AWS WA Tool convalida il file JSON, l'obiettivo personalizzato viene visualizzato in Obiettivi personalizzati.

Una volta creato, l'obiettivo personalizzato è nello stato BOZZA. È necessario pubblicare l'obiettivo prima che possa essere applicato ai carichi di lavoro o condiviso con altri Account AWS.

È possibile creare fino a 15 obiettivi personalizzati in un Account AWS.

> **Dichiarazione di non responsabilità**
>
> Non includere o raccogliere informazioni di identificazione personale (PII) degli utenti finali o di altre persone all'interno o tramite gli obiettivi personalizzati. Se gli obiettivi personalizzati o quelli condivisi e utilizzati nell'account dell'utente includono o raccolgono informazioni di identificazione personale, è necessario garantire che tali informazioni incluse vengano trattate in conformità alla normativa applicabile, fornendo l'adeguata informativa sulla privacy e ottenendo il consenso necessario per il trattamento dei dati.

Visualizzazione in anteprima di un obiettivo personalizzato per un carico di lavoro in AWS WA Tool

Per visualizzare in anteprima un obiettivo personalizzato

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. È possibile visualizzare in anteprima solo gli obiettivi con lo stato BOZZA. Selezionare l'obiettivo personalizzato desiderato nello stato BOZZA e scegliere Anteprima esperienza.
4. Scegliere Avanti per visualizzare l'anteprima dell'obiettivo.
5. (Facoltativo) È possibile esaminare il Piano di miglioramento selezionando le best practice all'interno di ogni domanda dell'anteprima e scegliendo Aggiorna in base alle risposte per testare la logica di rischio. Se sono necessarie modifiche, è possibile aggiornare le regole di rischio nel modello JSON prima della pubblicazione.
6. Scegliere Esci dall'anteprima per tornare all'obiettivo personalizzato.

> **Note**
>
> È possibile visualizzare l'anteprima di un obiettivo personalizzato anche selezionando Invia e anteprima durante la creazione di un obiettivo personalizzato.

Pubblicazione di un obiettivo personalizzato in AWS WA Tool per la prima volta

Per pubblicare un obiettivo personalizzato

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. Selezionare l'obiettivo personalizzato desiderato e scegliere Pubblica obiettivo.
4. Nella casella Nome versione, inserire un identificatore univoco per la modifica della versione. Questo valore può contenere fino a 32 caratteri alfanumerici o punti (".").

5. Scegliere Pubblica obiettivo personalizzato.

   Dopo la pubblicazione, lo stato dell'obiettivo personalizzato diventa PUBBLICATO.

L'obiettivo personalizzato ora può essere applicato ai carichi di lavoro o condiviso con altri Account AWS o utenti.

Pubblicazione di un aggiornamento di un obiettivo personalizzato in AWS WA Tool

Per pubblicare un aggiornamento di un obiettivo personalizzato esistente

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. Selezionare l'obiettivo personalizzato desiderato e scegliere Modifica.
4. Se non è disponibile un file JSON aggiornato, scegliere Scarica file per scaricare una copia dell'obiettivo personalizzato corrente. Modificare il file JSON scaricato con l'editor di testo preferito e apportare le modifiche desiderate.
5. Selezionare Scegli file per selezionare il file JSON aggiornato e scegliere Invia e anteprima per visualizzare l'anteprima dell'obiettivo personalizzato oppure Invia per inviare l'obiettivo personalizzato senza visualizzarlo in anteprima.

   Un obiettivo personalizzato non può superare la dimensione di 500 KB.

   Una volta che AWS WA Tool convalida il file JSON, l'obiettivo personalizzato viene visualizzato in Obiettivi personalizzati nello stato BOZZA.
6. Selezionare nuovamente l'obiettivo personalizzato e scegliere Pubblica obiettivo.
7. Scegliere Esamina le modifiche prima della pubblicazione per verificare che le modifiche apportate all'obiettivo personalizzato siano corrette. È inclusa la convalida dei seguenti elementi:

   - Il nome dell'obiettivo personalizzato
   - I nomi dei pilastri
   - Le domande nuove, aggiornate ed eliminate

   Scegli Next (Successivo).

8. Specificare il tipo di modifica della versione.

   Versione principale

   Indica che sono state apportate modifiche sostanziali all'obiettivo. Si utilizza per le modifiche che influiscono sul significato dell'obiettivo personalizzato.

   A tutti i carichi di lavoro con l'obiettivo applicato verrà comunicato che è disponibile una nuova versione dell'obiettivo personalizzato.

   Le modifiche della versione principale non vengono applicate automaticamente ai carichi di lavoro che utilizzano l'obiettivo.

   Versione secondaria

   Indica che sono state apportate modifiche secondarie all'obiettivo. Si usa per piccole modifiche, come modifiche al testo o aggiornamenti dei link URL.

   Le modifiche della versione secondaria vengono applicate automaticamente ai carichi di lavoro che utilizzano l'obiettivo personalizzato.

   Scegli Next (Successivo).

9. Nella casella Nome versione, inserire un identificatore univoco per la modifica della versione. Questo valore può contenere fino a 32 caratteri alfanumerici o punti (".").
10. Scegliere Pubblica obiettivo personalizzato.

    Dopo la pubblicazione, lo stato dell'obiettivo personalizzato diventa PUBBLICATO.

L'obiettivo personalizzato aggiornato ora può essere applicato ai carichi di lavoro o condiviso con altri Account AWS o utenti.

Se l'aggiornamento è una modifica della versione principale, a tutti i carichi di lavoro a cui è stata applicata la versione precedente dell'obiettivo verrà notificata la disponibilità di una nuova versione con la possibilità di effettuare l'aggiornamento.

Gli aggiornamenti della versione secondaria vengono applicati automaticamente senza notifica.

È possibile creare fino a 100 versioni di un obiettivo personalizzato.

Condivisione di un obiettivo personalizzato in AWS WA Tool

È possibile condividere un obiettivo personalizzato con altri Account AWS, utenti, AWS Organizations e unità organizzative (UO).

Per condividere un obiettivo personalizzato con altri Account AWS e utenti

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. Selezionare l'obiettivo personalizzato da condividere e scegliere Visualizza dettagli.
4. Nella pagina Visualizzazione dei dettagli dell'obiettivo per un carico di lavoro in AWS WA Tool, scegliere Condivisioni. Quindi scegliere Crea e Creazione di condivisioni per utenti o account per creare un invito di condivisione dell'obiettivo.
5. Immettere l'ID Account AWS a 12 cifre o l'ARN dell'utente con cui si desidera condividere l'obiettivo personalizzato.
6. Scegliere Crea per inviare un invito di condivisione dell'obiettivo all'utente o all'Account AWS specificato.

È possibile condividere obiettivi personalizzati con un massimo di 300 Account AWS o utenti.

L'invito di condivisione dell'obiettivo scade automaticamente se non viene accettato entro sette giorni.

> **Important**
>
> Prima di condividere un obiettivo personalizzato con l'organizzazione o le unità organizzative (UO), è necessario abilitare l'accesso ad AWS Organizations.

Per condividere un obiettivo personalizzato con l'organizzazione o le unità organizzative

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. Selezionare l'obiettivo personalizzato da condividere.
4. Nella pagina Visualizzazione dei dettagli dell'obiettivo per un carico di lavoro in AWS WA Tool, scegliere Condivisioni. Quindi scegliere Crea e Creazione di condivisioni per le Organizzazioni.

5. Nella pagina Crea condivisione dell'obiettivo personalizzato, scegliere se concedere le autorizzazioni all'intera organizzazione oppure a una o più unità organizzative.
6. Scegliere Crea per condividere l'obiettivo personalizzato.

Per vedere chi ha condiviso l'accesso a un obiettivo personalizzato, scegliere Condivisioni dalla pagina Visualizzazione dei dettagli dell'obiettivo per un carico di lavoro in AWS WA Tool.

> **Dichiarazione di non responsabilità**
>
> Condividendo gli obiettivi personalizzati con altri Account AWS, si accetta che AWS li renda disponibili agli altri account. Questi altri account possono continuare ad accedere e utilizzare gli obiettivi personalizzati condivisi anche se si eliminano gli obiettivi personalizzati dal proprio Account AWS o si termina il proprio Account AWS.

Aggiunta di tag a un obiettivo personalizzato in AWS WA Tool

Per aggiungere tag a un obiettivo personalizzato

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.
3. Selezionare l'obiettivo personalizzato da aggiornare.
4. Nella sezione Tag scegliere Gestisci tag.
5. Selezionare Aggiungi nuovo tag e immettere la Chiave e il Valore per ogni tag da aggiungere.
6. Seleziona Salva.

Per rimuovere un tag, scegliere Rimuovi accanto al tag da eliminare.

Eliminazione di un obiettivo personalizzato in AWS WA Tool

Per eliminare un obiettivo personalizzato

1. Accedi alla AWS Management Console e apri la console dello AWS Well-Architected Tool all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegliere Obiettivi personalizzati.

3. Selezionare l'obiettivo personalizzato da eliminare e scegliere Elimina.
4. Scegliere Delete (Elimina).

   Ai carichi di lavoro esistenti con l'obiettivo applicato viene notificato che l'obiettivo personalizzato è stato eliminato, tuttavia possono continuare a utilizzarlo. L'obiettivo personalizzato non può più essere applicato a nuovi carichi di lavoro.

> **Dichiarazione di non responsabilità**
>
> Condividendo gli obiettivi personalizzati con altri Account AWS, si accetta che AWS li renda disponibili agli altri account. Questi altri account possono continuare ad accedere e utilizzare gli obiettivi personalizzati condivisi anche se si eliminano gli obiettivi personalizzati dal proprio Account AWS o si termina il proprio Account AWS.

Specificazione del formato dell'obiettivo in AWS WA Tool

Gli obiettivi sono definiti utilizzando un formato JSON specifico. Quando si inizia a creare un obiettivo personalizzato, si ha la possibilità di scaricare un file JSON modello. È possibile utilizzare questo file come fondamento per gli obiettivi personalizzati in quanto definisce la struttura di base per i pilastri, le domande, le best practice e il piano di miglioramento.

Sezione Obiettivi

Questa sezione definisce gli attributi per l'obiettivo personalizzato. Indica il nome e la descrizione.

- `schemaVersion`: la versione dello schema dell'obiettivo personalizzato da utilizzare. Impostata in base al modello, da non modificare.
- `name`: il nome dell'obiettivo. Il nome può contenere fino a 128 caratteri.
- `description`: la descrizione in formato testo dell'obiettivo. Questo testo viene visualizzato quando si selezionano gli obiettivi da aggiungere durante la creazione del carico di lavoro o quando si seleziona un obiettivo da applicare successivamente a un carico di lavoro esistente. La descrizione può contenere fino a 2048 caratteri.

```
    "schemaVersion": "2021-11-01",
    "name": "Company Policy ABC",
```

```
   "description": "This lens provides a set of specific questions to assess compliance
with company policy ABC-2021 as revised on 2021/09/01.",
```

Sezione Pilastri

Questa sezione definisce i pilastri associati all'obiettivo personalizzato. È possibile mappare le domande ai pilastri del Framework AWS Well-Architected, definire i pilastri o entrambe le attività.

Si possono definire fino a 10 pilastri per un obiettivo personalizzato.

- `id`: ID del pilastro. L'ID può contenere da 3 a 128 caratteri alfanumerici o di sottolineatura ("_"). Gli ID utilizzati in un pilastro devono essere univoci.

  Quando si mappano le domande ai pilastri del Framework, si devono usare i seguenti ID:

  - `operationalExcellence`
  - `security`
  - `reliability`
  - `performance`
  - `costOptimization`
  - `sustainability`
- `name`: nome del pilastro. Il nome può contenere fino a 128 caratteri.

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
           .
           .
           .
       },
       {
           "id": "company_Security",
           "name": "Security",
           .
           .
           .
       }
    ]
```

Sezione Domande

Questa sezione definisce le domande associate a un pilastro.

Si possono definire fino a 20 domande in un pilastro di un obiettivo personalizzato.

- `id`: ID della domanda. L'ID può contenere da 3 a 128 caratteri alfanumerici o di sottolineatura ("_"). Gli ID utilizzati in una domanda devono essere univoci.
- `title`: titolo della domanda. Il titolo può contenere fino a 128 caratteri.
- `description`: descrive la domanda in modo più dettagliato. La descrizione può contenere fino a 2048 caratteri.
- `helpfulResource displayText`: facoltativo. Testo che fornisce informazioni utili sulla domanda. Il testo può contenere fino a 2048 caratteri. Deve essere immesso se viene specificato `helpfulResource url`.
- `helpfulResource url`: facoltativo. Risorsa URL che spiega la domanda in modo più dettagliato. L'URL deve iniziare con `http://` o `https://`.

> **Note**
>
> Quando si sincronizza un carico di lavoro personalizzato con Jira, le domande mostrano l'ID e il titolo.
> Il formato utilizzato nei ticket Jira è `[ QuestionID ] QuestionTitle`.

```
"questions": [
    {
        "id": "privacy01",
        "title": "How do you ensure HR conversations are private?",
        "description": "Career and benefits discussions should occur on secure channels
 only and be audited regularly for compliance.",
        "helpfulResource": {
            "displayText": "This is helpful text for the first question",
            "url": "https://example.com/poptquest01_help.html"
        },
        .
        .
```

```
        .
    },
    {
        "id": "privacy02",
        "title": "Is your team following the company privacy policy?",
        "description": "Our company requires customers to opt-in to data use and does
 not disclose customer data to third parties either individually or in aggregate.",
        "helpfulResource": {
            "displayText": "This is helpful text for the second question",
            "url": "https://example.com/poptquest02_help.html"
        },
        .
        .
        .
    }
]
```

Sezione Scelte

Questa sezione definisce le scelte associate a una domanda.

Si possono definire fino a 15 scelte per una domanda di un obiettivo personalizzato.

- `id`: ID della scelta. L'ID può contenere da 3 a 128 caratteri alfanumerici o di sottolineatura ("_"). È necessario specificare un ID univoco per ogni scelta di una domanda. L'aggiunta di una scelta con il suffisso _no equivale alla scelta `None of these` per la domanda.
- `title`: titolo della scelta. Il titolo può contenere fino a 128 caratteri.
- `helpfulResource displayText`: facoltativo. Testo che fornisce informazioni utili su una scelta. Il testo può contenere fino a 2048 caratteri. Deve essere incluso se viene specificato `helpfulResource url`.
- `helpfulResource url`: facoltativo. Risorsa URL che spiega la scelta in modo più dettagliato. L'URL deve iniziare con `http://` o `https://`.
- `improvementPlan displayText`: testo che descrive come migliorare una scelta. Il testo può contenere fino a 2048 caratteri. `improvementPlan` è obbligatorio per ogni scelta, ad eccezione della scelta `None of these`.
- `improvementPlan url`: facoltativo. Risorsa URL che può contribuire al miglioramento. L'URL deve iniziare con `http://` o `https://`.
- `additionalResources type`: facoltativo. Il tipo di risorse aggiuntive. Il valore può essere `HELPFUL_RESOURCE` o `IMPROVEMENT_PLAN`.

- `additionalResources content`: facoltativo. Specifica i valori `displayText` e `url` per la risorsa aggiuntiva. È possibile specificare fino a cinque risorse aggiuntive utili e fino a cinque elementi aggiuntivi del piano di miglioramento per una scelta.
  - `displayText`: facoltativo. Testo che descrive la risorsa utile o il piano di miglioramento. Il testo può contenere fino a 2048 caratteri. Deve essere incluso se viene specificato `url`.
  - `url`: facoltativo. Risorsa URL per la risorsa utile o il piano di miglioramento. L'URL deve iniziare con `http://` o `https://`.

> **Note**
>
> Quando si sincronizza un carico di lavoro di un obiettivo personalizzato con Jira, le scelte mostrano l'ID della domanda e della scelta, nonché il titolo della scelta.
> Il formato utilizzato è `[ QuestionID | ChoiceID ] ChoiceTitle`.

```
    "choices": [
         {
             "id": "choice_1",
             "title": "Option 1",
             "helpfulResource": {
                 "displayText": "This is helpful text for the first choice",
                 "url": "https://example.com/popt01_help.html"
             },
             "improvementPlan": {
                 "displayText": "This is text that will be shown for improvement of
this choice.",
                 "url": "https://example.com/popt01_iplan.html"
             }
         },
         {
             "id": "choice_2",
             "title": "Option 2",
             "helpfulResource": {
                 "displayText": "This is helpful text for the second choice",
                 "url": "https://example.com/hr_manual_CORP_1.pdf"
             },
             "improvementPlan": {
                 "displayText": "This is text that will be shown for improvement of
this choice.",
                 "url": "https://example.com/popt02_iplan_01.html"
```

```
            },
            "additionalResources":[
               {
                 "type": "HELPFUL_RESOURCE",
                 "content": [
                   {
                     "displayText": "This is the second set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_country.html"
                   },
                   {
                     "displayText": "This is the third set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_city.html"
                   }
                 ]
               },
               {
                 "type": "IMPROVEMENT_PLAN",
                 "content": [
                   {
                     "displayText": "This is additional text that will be shown for
improvement of this choice.",
                     "url": "https://example.com/popt02_iplan_02.html"
                   },
                   {
                     "displayText": "This is the third piece of improvement plan
text.",
                     "url": "https://example.com/popt02_iplan_03.html"
                   }
                   {
                     "displayText": "This is the fourth piece of improvement plan
text.",
                     "url": "https://example.com/popt02_iplan_04.html"
                   }
                 ]
               }
             ]
        },
        {
             "id": "option_no",
             "title": "None of these",
             "helpfulResource": {
```

```
                "displayText": "Choose this if your workload does not follow these best
practices.",
                "url": "https://example.com/popt02_iplan_none.html"
              }

            }
```

Sezione Regole di rischio

Questa sezione definisce in che modo le scelte selezionate determinano il livello di rischio.

È possibile definire un massimo di tre regole di rischio per ogni domanda, una per ciascun livello di rischio.

- `condition`: espressione booleana delle scelte che corrisponde a un livello di rischio per la domanda oppure `default`.

  Deve essere presente una regola di rischio `default` per ogni domanda.
- `risk`: indica il rischio associato alla condizione. I valori validi sono `HIGH_RISK`, `MEDIUM_RISK` e `NO_RISK`.

L'ordine delle regole di rischio è significativo. La prima `condition` che restituisce `true` stabilisce il rischio della domanda. Uno schema comune per l'implementazione delle regole di rischio consiste nell'iniziare con le regole meno rischiose (e in genere più granulari) per poi arrivare alle regole più rischiose (e meno specifiche).

Per esempio:

```
"riskRules": [
      {
        "condition": "choice_1 && choice_2 && choice_3",
        "risk": "NO_RISK"
      },
      {
        "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 &&
choice_3)",
        "risk": "MEDIUM_RISK"
      },
      {
```

```
        "condition": "default",
        "risk": "HIGH_RISK"
      }
]
```

Se la domanda include tre scelte (`choice_1`, `choice_2` e `choice_3`), queste regole di rischio determinano il comportamento seguente:

- Se sono selezionate tutte e tre le scelte, non vi è alcun rischio.
- Se `choice_1` o `choice_2` è selezionata e `choice_3` è selezionata, il rischio è medio.
- Se `choice_1` non è selezionata ma `choice_3` è selezionata, il rischio è sempre medio.
- Se nessuna di queste condizioni precedenti è vera, il rischio è elevato.

Aggiornamenti dell'obiettivo in AWS WA Tool

L'obiettivo Framework AWS Well-Architected e gli altri obiettivi forniti da AWS vengono aggiornati man mano che vengono introdotti nuovi servizi, vengono perfezionate le best practice esistenti per i sistemi basati su cloud e vengono aggiunte nuove best practice. Quando una nuova versione dell'approfondimento diventa disponibile, AWS WA Tool viene aggiornato in modo da riflettere le ultime best practice. Tutti i nuovi carichi di lavoro definiti utilizzano la nuova versione dell'obiettivo.

L'aggiornamento di un obiettivo avviene anche quando un obiettivo personalizzato applicato a un carico di lavoro o a un modello di revisione dispone di una nuova versione principale pubblicata.

L'aggiornamento di un obiettivo può essere costituito da qualsiasi combinazione di:

- Aggiunta di nuove domande o best practice
- Rimozione di vecchie domande o practice che non sono più consigliate
- Aggiornamento di domande o best practice esistenti
- Aggiunta e rimozione di pilastri

Le risposte alle domande esistenti vengono mantenute.

> **Note**
>
> Non è possibile annullare un aggiornamento dell'obiettivo. Dopo aver aggiornato un carico di lavoro all'ultima versione dell'obiettivo, non è possibile tornare alla versione precedente dell'obiettivo.

Determinazione dell'obiettivo da aggiornare in AWS WA Tool

È possibile individuare quali carichi di lavoro non utilizzano la versione più recente dell'obiettivo consultando la pagina Notifiche.

Nella pagina Notifiche per ogni carico di lavoro vengono visualizzate le seguenti informazioni:

Risorsa

Nome del carico di lavoro o del modello di revisione.

Tipo di risorsa

Il tipo di risorsa. Può essere Carico di lavoro o Modello di revisione.

Risorsa associata

Nome dell'obiettivo.

Tipo di notifica

Il tipo di notifica dell'upgrade.

- Not current (Non corrente): il carico di lavoro utilizza una versione dell'approfondimento che non è più corrente. Effettua l'aggiornamento alla versione corrente dell'approfondimento per migliori linee guida.
- Disattivato: il carico di lavoro utilizza una versione dell'obiettivo che non riflette più le best practice. Effettuare l'aggiornamento alla versione corrente dell'approfondimento.
- Eliminato: il carico di lavoro utilizza un obiettivo che è stato eliminato dal proprietario.

Versione in uso

La versione dell'approfondimento attualmente utilizzata per il carico di lavoro.

Current available version (Versione corrente disponibile)

La versione dell'obiettivo disponibile per l'aggiornamento o Nessuno se l'obiettivo è stato eliminato.

Per aggiornare l'approfondimento associato a un carico di lavoro, selezionare il carico di lavoro e scegliere Upgrade lens version (Aggiorna versione approfondimento).

Aggiornamento di un obiettivo in AWS WA Tool

Gli obiettivi possono essere aggiornati per carichi di lavoro e modelli di revisione.

> **Note**
>
> Non è possibile annullare un aggiornamento dell'obiettivo. Dopo aver aggiornato un carico di lavoro o un modello di revisione all'ultima versione dell'obiettivo, non è possibile tornare alla versione precedente dell'obiettivo.

Aggiornamento di un obiettivo per un carico di lavoro

1. Nella pagina Notifiche, selezionare un carico di lavoro da aggiornare e scegliere Aggiorna la versione dell'obiettivo. Vengono visualizzate le informazioni su ciò che è cambiato in ogni pilastro.

   > **Note**
   >
   > È anche possibile scegliere Visualizza gli aggiornamenti disponibili nella scheda Panoramica del carico di lavoro.

2. Prima di aggiornare un obiettivo per un carico di lavoro, viene creata una tappa fondamentale per salvare lo stato del carico di lavoro esistente per riferimento futuro. Immettere un nome univoco per la tappa fondamentale nel campo Nome della tappa fondamentale.
3. Selezionare la casella Conferma accanto a Riconosco e accetto queste modifiche e scegliere Salva.

Una volta aggiornato l'obiettivo, è possibile visualizzare la versione precedente dell'obiettivo nella scheda Tappe fondamentali.

Aggiornamento di un obiettivo per un modello di revisione

1. Per aggiornare l'obiettivo per un modello di revisione, attenersi alla seguente procedura.

2. Nella pagina Notifiche, selezionare un modello di revisione da aggiornare e scegliere Aggiorna la versione dell'obiettivo. Vengono visualizzate le informazioni su ciò che è cambiato in ogni pilastro.

> **Note**
>
> È anche possibile scegliere Visualizza gli aggiornamenti disponibili nella scheda Panoramica del modello di revisione.

3. Selezionare la casella Conferma accanto a Riconosco e accetto queste modifiche e scegliere Aggiorna e modifica le risposte del modello per modificare le risposte alle domande delle best practice per il modello di revisione oppure Aggiorna per aggiornare l'obiettivo senza modificare le risposte del modello.

Catalogo Lens per AWS WA Tool

Catalogo Lens è una raccolta di obiettivi AWS ufficiali creati per AWS Well-Architected Tool al fine di offrire una tecnologia aggiornata e le best practice incentrate sul settore. Questi obiettivi sono disponibili per tutti gli utenti e non richiedono alcuna installazione aggiuntiva per essere utilizzati.

La tabella seguente descrive tutti gli obiettivi AWS ufficiali attualmente disponibili in Catalogo Lens.

Nome obiettivo	Descrizione
Framework AWS Well-Architected	Applicato per impostazione predefinita a tutti i carichi di lavoro. Raccolta di best practice architetturali per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili nel cloud.
Mobilità connessa	Best practice per integrare la tecnologia nei sistemi di trasporto e migliorare l'esperienza di mobilità complessiva.
Creazione di container	Fornisce le best practice per il processo di progettazione e creazione dei container.

Nome obiettivo	Descrizione
Analisi dei dati	Include gli approfondimenti raccolti da AWS dai casi di studio reali e consente di apprendere gli elementi di progettazione chiave dei carichi di lavoro di analisi Well-Architected, insieme a suggerimenti per il miglioramento.
DevOps	Descrive un approccio strutturato che le organizzazioni di tutte le dimensioni possono seguire per coltivare una cultura incentrata sulla sicurezza a velocità elevata, in grado di fornire un valore aziendale sostanziale utilizzan do tecnologie moderne e best practice DevOps.
Settore dei servizi finanziari	Best practice per l'architettura dei carichi di lavoro del settore dei servizi finanziari su AWS.
IA generativa	Best practice per l'architettura dei carichi di lavoro di IA generativa su AWS.
Governance	Best practice per la progettazione e l'erogazi one di servizi di governance su AWS.
Settore sanitario	Best practice e linee guida su come progettar e, implementare e gestire i carichi di lavoro del settore sanitario su Cloud AWS.
IoT	Best practice per la gestione di carichi di lavoro Internet delle cose (IoT) su AWS.
Fusioni e acquisizioni	Best practice per l'integrazione e la migrazion e al cloud di carichi di lavoro durante fusioni e acquisizioni.
Machine Learning	Best practice per la gestione delle risorse e dei carichi di lavoro di machine learning su AWS.
Migrazione	Best practice per la migrazione al Cloud AWS.

Nome obiettivo	Descrizione
SaaS	Incentrato sulla progettazione, sull'implementazione e sull'architettura dei carichi di lavoro software as a service (SaaS) su Cloud AWS.
SAP	Principi di progettazione e best practice per i carichi di lavoro SAP su Cloud AWS.
Applicazioni serverless	Best practice per la creazione di carichi di lavoro serverless su AWS. Vengono affrontati i diversi scenari, tra cui microservizi RESTful, backend per app mobili, elaborazione di flussi e applicazioni Web.

Rivedi i modelli in AWS WA Tool

Puoi creare modelli di recensione AWS WA Tool che contengano risposte precompilate per Well-Architected Framework e domande sulle best practice sulle lenti personalizzate. I modelli di revisione Well-Architected riducono la necessità di inserire manualmente le stesse risposte per le best practice comuni a più carichi di lavoro durante l'esecuzione di una revisione Well-Architected e aiutano a promuovere la coerenza e la standardizzazione delle best practice tra team e carichi di lavoro.

Puoi creare un modello di revisione per rispondere a domande comuni sulle best practice o creare note, che possono essere condivise con un altro IAM utente o account oppure con un'organizzazione o un'unità organizzativa dello stesso. Regione AWS Puoi definire un carico di lavoro partendo da un modello di revisione, che consente di scalare le best practice comuni e ridurre la ridondanza tra i carichi di lavoro.

Creazione di un modello di recensione in AWS WA Tool

Per creare un modello di recensione

1. Seleziona Modelli di revisione nel riquadro di navigazione a sinistra.
2. Scegli Crea modello.
3. Nella pagina Specificare i dettagli del modello, fornisci un nome e una descrizione per il modello di recensione.
4. (Facoltativo) Nelle sezioni Note sul modello e Tag, aggiungi le note o i tag del modello che desideri associare al modello di recensione. Le note aggiunte vengono applicate a tutti i carichi di lavoro che utilizzano il modello di recensione, mentre i tag sono specifici del modello di recensione.

   Per ulteriori informazioni sui tag, consultaTagging delle risorse AWS WA Tool.
5. Scegli Next (Successivo).
6. Nella pagina Applica lenti, seleziona le lenti che desideri applicare al modello di recensione. Il numero massimo di obiettivi che è possibile applicare è 20.

   Gli obiettivi possono essere selezionati da Custom lens, Lens Catalog o entrambi.

> **Note**
>
> Le lenti condivise con te non possono essere applicate al modello di recensione.

7. Scegli Crea modello.

Per iniziare a rispondere alle domande sul modello di recensione che hai appena creato

1. Nella scheda Panoramica del modello, nell'avviso informativo Inizia a rispondere alle domande, seleziona l'obiettivo nel menu a discesa Rispondi alle domande.

> **Note**
>
> Puoi anche andare alla sezione Obiettivi, selezionare l'obiettivo e scegliere Rispondi alle domande.

2. Per ogni obiettivo che hai applicato al tuo modello di recensione, rispondi alle domande pertinenti e scegli Salva ed esci quando hai finito.

Una volta creato il modello di recensione, puoi definire un nuovo carico di lavoro a partire da esso.

La scheda Panoramica del modello di recensione dovrebbe riflettere il numero totale di domande a cui è stata data risposta nella sezione Dettagli del modello e le domande a cui è stata data risposta per ogni obiettivo nella sezione Obiettivi.

Modificare un modello di recensione in AWS WA Tool

Per modificare un modello di recensione

1. Seleziona Modelli di revisione nel riquadro di navigazione a sinistra.
2. Seleziona il nome del modello di recensione che desideri modificare.
3. Per aggiornare le note relative al nome, alla descrizione o al modello di recensione, scegli Modifica nella sezione Dettagli del modello della scheda Panoramica.
   a. Apporta le modifiche alle note relative al nome, alla descrizione o al modello.
   b. Scegli Salva modello per aggiornare il modello di recensione con le modifiche.

4. Per aggiornare gli obiettivi applicati al modello di recensione, nella sezione Lenti della scheda Panoramica, scegli Modifica obiettivi applicati.
   a. Seleziona o deseleziona le caselle di controllo delle lenti che desideri aggiungere o rimuovere.

      Le lenti possono essere selezionate o deselezionate da Custom lens, Lens Catalog o entrambi.
   b. Scegli Salva modello per salvare le modifiche.
5. Per aggiornare le risposte alle domande sulle migliori pratiche sull'obiettivo, nella sezione Obiettivi della scheda Panoramica, seleziona il nome dell'obiettivo.
   a. Nella sezione Panoramica dell'obiettivo, scegli Rispondi alle domande.

      > **Note**
      >
      > Facoltativamente, puoi selezionare il nome dell'obiettivo nel menu a discesa Review templates nel riquadro di navigazione a sinistra per accedere alla sezione Panoramica dell'obiettivo.
   b. Seleziona o deseleziona le caselle di controllo accanto alle risposte sulle best practice che desideri modificare.
   c. Scegli Salva ed esci per salvare le modifiche.

Condivisione di un modello di recensione in AWS WA Tool

I modelli di revisione possono essere condivisi con utenti o account oppure possono essere condivisi con un'intera organizzazione o unità organizzativa.

Per condividere un modello di recensione

1. Seleziona Modelli di revisione nel riquadro di navigazione a sinistra.
2. Seleziona il nome del modello di recensione che desideri condividere.
3. Scegli la scheda Condivisioni.
4. Per condividere con un utente o un account, scegli Crea e seleziona Condividi con IAM utenti o account. Nella casella Invia inviti, specifica l'utente o l'account IDs e scegli Crea.
5. Per condividere con un'organizzazione o un'unità organizzativa, scegli Crea e seleziona Condividi con Organizzazioni. Per condividere con un'intera organizzazione, seleziona Concedi autorizzazioni all'intera organizzazione. Per condividere con un'unità organizzativa, seleziona

Concedi autorizzazioni a singole unità organizzative, specifica l'unità organizzativa nella casella e scegli Crea.

> **Important**
>
> Prima di condividere un profilo con un'organizzazione o un'unità organizzativa (OU), devi abilitare AWS Organizations l'accesso.

Definizione di un carico di lavoro da un modello in AWS WA Tool

Puoi definire un carico di lavoro a partire da un modello di recensione che hai creato o da un modello di recensione che è stato condiviso con te. Non puoi definire un nuovo carico di lavoro da un modello di recensione che è stato eliminato e, se il modello di recensione contiene una versione obsoleta di un obiettivo, devi aggiornare il modello di recensione prima di poter definire un nuovo carico di lavoro da esso. Per informazioni su come aggiornare un modello di recensione, consulta. the section called "Aggiornamento di un obiettivo"

> **Note**
>
> Per definire un carico di lavoro da un modello di revisione, devi disporre IAM delle autorizzazioni per creare un carico di lavoro abilitate:`wellarchitected:CreateWorkload`,, e delle seguenti autorizzazioni per il modello di revisione:`wellarchitected:GetReviewTemplate`,, `wellarchitected:GetReviewTemplateAnswer` e. `wellarchitected:ListReviewTemplateAnswers` `wellarchitected:GetReviewTemplateLensReview` Per ulteriori informazioni sulle IAM autorizzazioni, consulta la Guida per l'utente.AWS Identity and Access Management

Per definire un carico di lavoro a partire da un modello di revisione

1. Seleziona Rivedi i modelli nel riquadro di navigazione a sinistra.
2. Seleziona il nome del modello di recensione da cui desideri definire un carico di lavoro.
3. Scegli Definisci carico di lavoro da modello.

> **Note**
>
> Puoi anche scegliere Definisci dal modello di revisione dal menu a discesa Definisci carico di lavoro nella pagina Carichi di lavoro.

4. Nel passaggio Seleziona il modello di revisione, seleziona la scheda del modello di revisione e scegli Avanti.
5. Nel passaggio Specificare le proprietà, compila i campi obbligatori per le proprietà del carico di lavoro e scegli Avanti. Per ulteriori dettagli, consulta the section called “Definizione di un carico di lavoro”.
6. (Facoltativo) Nel passo Applica profilo, associa un profilo al carico di lavoro selezionando un profilo esistente, cercando il nome del profilo o scegliendo Crea profilo per creare un profilo. Scegli Next (Successivo).

   I profili Well-Architected e i modelli di revisione possono essere utilizzati in tandem. Le domande precompilate nel modello di recensione mantengono le risposte durante il carico di lavoro e alle domande viene assegnata una priorità in base al profilo dell'utente.
7. (Facoltativo) Nella fase Applica lenti, puoi scegliere di applicare obiettivi aggiuntivi da Lenti personalizzati o dal catalogo Lens che non erano già stati applicati al modello di recensione.
8. Scegliere Define workload (Definisci carico di lavoro).

Eliminazione di un modello di recensione in AWS WA Tool

Per eliminare un modello di recensione

1. Seleziona Modelli di revisione nel riquadro di navigazione a sinistra.
2. Nella sezione Modelli di revisione, scegli il modello di recensione che desideri eliminare e nel menu a discesa Azioni, seleziona Elimina.

> **Note**
>
> Puoi anche selezionare il nome del modello e scegliere Elimina dalla scheda Panoramica del modello di recensione.

3. Nella finestra di dialogo Elimina modello di recensione, inserisci il nome del modello di recensione nel campo per confermare l'eliminazione.

4. Scegli Elimina.

Non puoi creare un nuovo carico di lavoro da un modello di recensione che è stato eliminato. Se hai condiviso un modello di recensione che hai eliminato con altri IAM utenti, account o organizzazioni, questi non saranno in grado di creare carichi di lavoro a partire da esso.

Utilizzo dei profili in AWS WA Tool

Puoi creare profili per fornire il contesto aziendale e identificare gli obiettivi che vorresti raggiungere quando esegui una revisione Well-Architected. AWS Well-Architected Tool utilizza le informazioni raccolte dal tuo profilo per aiutarti a concentrarti su un elenco prioritario di domande pertinenti alla tua attività durante la revisione del carico di lavoro. L'associazione di un profilo al carico di lavoro consente inoltre di individuare i rischi prioritari da affrontare con il piano di miglioramento.

Puoi creare un profilo dalla pagina Profili e associarlo a un nuovo carico di lavoro oppure puoi aggiungere un profilo a un carico di lavoro esistente.

Creazione di un profilo

Per creare un profilo

1. Seleziona Profili nel riquadro di navigazione a sinistra.
2. Scegli Create profile (Crea profilo).
3. Nella sezione Proprietà del profilo, fornisci un nome e una descrizione per il tuo profilo.
4. Per rifinire le informazioni prioritarie per la tua attività nel piano di revisione e miglioramento del carico di lavoro, seleziona le risposte più pertinenti per la tua attività nella sezione Domande sul profilo.
5. (Facoltativo) Nella sezione Tag, aggiungi i tag che desideri associare al profilo.

   Per ulteriori informazioni sui tag, consultaTagging delle risorse AWS WA Tool.
6. Seleziona Salva. Quando il profilo viene creato correttamente, viene visualizzato un messaggio di successo.

Quando viene creato un profilo, viene visualizzata la panoramica del profilo. La panoramica mostra i dati associati al profilo, inclusi il nome, la descrizioneARN, le date di creazione e aggiornamento e le risposte alle domande del profilo. Dalla pagina di panoramica del profilo puoi modificare, eliminare o condividere il tuo profilo.

Modifica di un profilo in AWS WA Tool

Per modificare un profilo

1. Seleziona Profili nel riquadro di navigazione a sinistra o scegli Visualizza profilo nella sezione Profili del carico di lavoro.
2. Seleziona il nome del profilo che desideri aggiornare.
3. Scegli Modifica nella pagina di panoramica del profilo.
4. Apporta le modifiche necessarie alle domande del profilo.
5. Seleziona Salva.

Condivisione di un profilo in AWS WA Tool

I profili possono essere condivisi con utenti o account oppure possono essere condivisi con un'intera organizzazione o unità organizzativa.

Per condividere un profilo

1. Seleziona Profili nel riquadro di navigazione a sinistra.
2. Seleziona il nome del profilo che desideri condividere.
3. Scegli la scheda Condivisioni.
4. Per condividere con un utente o un account, scegli Crea e seleziona Crea condivisioni per IAM utenti o account. Nella casella Invia inviti, specifica l'utente o l'account IDs e scegli Crea.
5. Per condividere con un'organizzazione o un'unità organizzativa, scegli Crea e seleziona Crea condivisioni per Organizzazioni. Per condividere con un'intera organizzazione, seleziona Concedi autorizzazioni all'intera organizzazione. Per condividere con un'unità organizzativa, seleziona Concedi autorizzazioni a singole unità organizzative, specifica l'unità organizzativa nella casella e scegli Crea.

> **Important**
>
> Prima di condividere un profilo con un'organizzazione o un'unità organizzativa (OU), devi abilitare AWS Organizations l'accesso.

Aggiungere un profilo a un carico di lavoro in AWS WA Tool

Puoi aggiungere un profilo a un carico di lavoro esistente o, durante la definizione di un carico di lavoro, per velocizzare il processo di revisione del carico di lavoro. AWS WA Tool utilizza le informazioni raccolte dal tuo profilo per dare priorità alle domande relative alla tua attività nella revisione del carico di lavoro.

Per ulteriori informazioni sull'aggiunta di un profilo durante la definizione di un carico di lavoro, consulta. the section called “Definizione di un carico di lavoro”

Per aggiungere un profilo a un carico di lavoro esistente

1. Seleziona Carichi di lavoro nel riquadro di navigazione a sinistra e seleziona il nome del carico di lavoro che desideri associare a un profilo.

   > **Note**
   >
   > È possibile associare un solo profilo a un carico di lavoro.

2. Nella sezione Profilo, scegli Aggiungi profilo.
3. Seleziona il profilo che desideri applicare al carico di lavoro dall'elenco dei profili disponibili oppure scegli Crea profilo. Per ulteriori informazioni, consulta the section called “Creazione di un profilo ”.
4. Seleziona Save (Salva.

La panoramica del carico di lavoro mostra un numero di domande con priorità a cui è stata data risposta e di rischi a cui è stata assegnata la priorità in base alle informazioni nel profilo associato. Scegli Continua la revisione per rispondere alle domande prioritarie nella revisione del carico di lavoro. Per ulteriori informazioni, consulta the section called “Documentazione di un carico di lavoro”.

La sezione Profilo mostra il nome, la descrizioneARN, la versione e la data dell'ultimo aggiornamento del profilo associato al carico di lavoro.

Rimuovere un profilo da un carico di lavoro in AWS WA Tool

La rimozione di un profilo dal carico di lavoro riporta il carico di lavoro alla versione precedente a cui il profilo era associato e le domande e i rischi relativi alla revisione del carico di lavoro non hanno più la priorità.

Per rimuovere un profilo da un carico di lavoro

1. Nella sezione Profili del carico di lavoro, scegli Rimuovi.
2. Per confermare la rimozione, inserisci il nome del profilo nel campo di immissione del testo.
3. Scegli Rimuovi.

Viene visualizzata una notifica che indica che il profilo è stato rimosso correttamente dal carico di lavoro. La rimozione di un profilo riporta il carico di lavoro alla versione precedente a quando il profilo gli era associato e le domande e i rischi relativi alla revisione del carico di lavoro non hanno più la priorità.

Eliminazione di un profilo da AWS WA Tool

Se hai creato un profilo, puoi eliminarlo dall'elenco di profili disponibile in AWS WA Tool.

L'eliminazione di un profilo dalla pagina Profili non rimuove il profilo dai carichi di lavoro associati. È possibile continuare a utilizzare i profili condivisi e associati a un carico di lavoro prima dell'eliminazione, tuttavia non è possibile associare nuovi carichi di lavoro a un profilo eliminato. the section called “Notifiche sul profilo”vengono inviati ai proprietari dei carichi di lavoro utilizzando profili eliminati.

> **Dichiarazione di non responsabilità**
>
> Condividendo i propri profili con altri Account AWS, l'utente riconosce che AWS metterà i propri profili a disposizione di tali altri account. Questi altri account possono continuare ad accedere e utilizzare i tuoi profili condivisi anche se elimini il profilo dal tuo account Account AWS o elimini i tuoi Account AWS.

Per eliminare un profilo dall'elenco dei profili

1. Seleziona Profili nel riquadro di navigazione a sinistra.
2. Seleziona il nome del profilo che desideri rimuovere.
3. Scegli Elimina.
4. Per confermare la rimozione, inserisci il nome del profilo nel campo di immissione del testo.
5. Scegli Elimina.

Se desideri mantenere un profilo nell'elenco dei profili, ma rimuoverlo da un carico di lavoro, consultathe section called “Rimuovere un profilo da un carico di lavoro”.

AWS Well-Architected Tool Connettore per Jira

Puoi utilizzare AWS Well-Architected Tool Connector for Jira per collegare il tuo account Jira AWS Well-Architected Tool e sincronizzare gli elementi di miglioramento dai tuoi carichi di lavoro ai progetti Jira per aiutarti a creare un meccanismo a ciclo chiuso per l'implementazione dei miglioramenti.

Il connettore fornisce la sincronizzazione automatica e manuale. Per ulteriori dettagli, vedere Configurazione del connettore.

Il connettore può essere configurato a livello di account e carico di lavoro, con la possibilità di sovrascrivere le impostazioni a livello di account per carico di lavoro. A livello di carico di lavoro, puoi anche scegliere di escludere completamente un carico di lavoro dalla sincronizzazione.

Puoi scegliere di sincronizzare gli elementi di miglioramento con il progetto WA Jira predefinito o specificare una chiave di progetto esistente con cui sincronizzarli. A livello di carico di lavoro, puoi sincronizzare ogni carico di lavoro con un progetto Jira unico, se necessario.

> **Note**
>
> Il connettore supporta solo progetti scrum e kanban in Jira.

Quando gli elementi di miglioramento vengono sincronizzati con Jira, vengono organizzati nel modo seguente:

- Progetto: WA (o progetto esistente da te specificato)
- Epic: Carico di lavoro
- Compito: Domanda
- Attività secondaria: best practice
- Etichetta: Pillar

Dopo aver configurato la sincronizzazione dell'account Jira nella pagina Impostazioni, puoi configurare il connettore Jira e sincronizzare gli elementi di miglioramento con il tuo account Jira.

Configurazione del connettore

Per installare il connettore

> **Note**
>
> Tutti i passaggi seguenti vengono eseguiti nel tuo account Jira, non nel tuo Account AWS.

1. Accedi al tuo account Jira.
2. Nella barra di navigazione in alto, scegli App, quindi seleziona Esplora altre app.
3. Nella pagina Scopri app e integrazioni per Jira, inserisci Well-Architected AWS . Quindi, scegli il connettore per Jira AWS Well-Architected Tool .
4. Nella pagina dell'app, scegli Get app.
5. Nel riquadro Aggiungi a Jira, scegli Scarica subito.
6. Dopo l'installazione dell'app, per completare la configurazione, scegli Configura.
7. Nella pagina AWS Well-Architected Tool Configurazione, scegli Connect a new Account AWS.
8. Inserisci il tuo AccessKeyID e la tua chiave segreta. Facoltativo: inserisci il tuo token di sessione. Quindi, scegli Connect.

   > **Note**
   >
   > Assicurati che il tuo account disponga dell'autorizzazione`wellarchitected:ConfigureIntegration`. Queste autorizzazioni sono necessarie per l'aggiunta Account AWS a Jira.
   > Account AWS È possibile collegarne più di uno. AWS WA Tool

   > **Note**
   >
   > Come best practice di sicurezza, si consiglia vivamente di utilizzare credenziali IAM a breve termine. Per informazioni dettagliate sulla creazione di un AccessKeyID e di una chiave segreta per te Account AWS, consulta Gestione delle chiavi di accesso (console) e per informazioni dettagliate sull'utilizzo di credenziali a breve termine, consulta Richiesta di credenziali temporanee.

9. Per le regioni, seleziona quelle Regioni AWS che desideri connettere. Quindi, scegli Connect.

Configurazione del progetto Jira

Quando usi progetti personalizzati, assicurati di avere i seguenti tipi di problemi nella configurazione del progetto:

- Scrum: Epic, Story, Subtask
- Kanban: Epic, Task, Sottotask

Per informazioni dettagliate sulla gestione dei tipi di problema, consulta Atlassian Support | Aggiungere, modificare ed eliminare un tipo di problema.

Per verificare lo stato del connettore in AWS Well-Architected Tool

1. Accedi al tuo Account AWS e vai a AWS Well-Architected Tool.
2. Seleziona Impostazioni nel riquadro di navigazione a sinistra.
3. Nella sezione Sincronizzazione dell'account Jira, sotto Stato della connessione all'app Jira, controlla lo stato Configurato.

Il connettore è ora configurato e pronto per essere configurato. Per configurare le impostazioni di sincronizzazione di Jira a livello di account e carico di lavoro, consulta Configurazione del connettore.

Configurazione del connettore

Con il AWS Well-Architected Tool Connector for Jira, puoi configurare la sincronizzazione di Jira a livello di account, a livello di carico di lavoro o entrambi. Puoi configurare le impostazioni Jira a livello di carico di lavoro indipendentemente dalle impostazioni a livello di account o sovrascrivere le impostazioni a livello di account su un carico di lavoro specifico per specificare il comportamento di sincronizzazione del carico di lavoro. Puoi anche configurare le impostazioni di Jira durante la definizione di un carico di lavoro.

Il connettore offre due metodi di sincronizzazione: sincronizzazione automatica e manuale. In entrambi i metodi di sincronizzazione, le modifiche apportate AWS WA Tool si riflettono nel progetto Jira e le modifiche apportate in Jira vengono sincronizzate con. AWS WA Tool

> **Important**
>
> Utilizzando la sincronizzazione automatica, acconsenti a AWS WA Tool modificare il carico di lavoro in risposta alle modifiche in Jira.
> Se hai informazioni sensibili che non desideri sincronizzare con Jira, non inserire queste informazioni nel campo Notes dei tuoi carichi di lavoro.

- Sincronizzazione automatica: il connettore aggiorna automaticamente il progetto Jira e il carico di lavoro ogni volta che viene aggiornata una domanda, inclusa la selezione o la deselezione di una best practice e il completamento di una domanda.
- Sincronizzazione manuale: devi scegliere Sincronizza con Jira nella dashboard del carico di lavoro quando desideri sincronizzare gli elementi di miglioramento tra Jira e il. AWS WA Tool Puoi anche scegliere quali pilastri e domande specifici vuoi sincronizzare. Per maggiori dettagli, consulta Sincronizzazione di un carico di lavoro.

Per configurare il connettore a livello di account

1. Seleziona Impostazioni nel riquadro di navigazione a sinistra.
2. Nel riquadro di sincronizzazione dell'account Jira, scegli Modifica.
3. Per Tipo di sincronizzazione, seleziona una delle seguenti opzioni:
   a. Per sincronizzare automaticamente i carichi di lavoro quando vengono apportate modifiche, seleziona Automatico.
   b. Per scegliere manualmente quando sincronizzare i carichi di lavoro, seleziona Manuale.
4. Per impostazione predefinita, il connettore crea un progetto WA Jira. Per specificare la tua chiave di progetto Jira, procedi come segue:
   a. Seleziona Sostituisci la chiave di progetto Jira predefinita.
   b. Inserisci la chiave del tuo progetto Jira.

   > **Note**
   >
   > La chiave di progetto Jira specificata viene utilizzata per tutti i carichi di lavoro a meno che non si modifichi il progetto a livello di carico di lavoro.
5. Scegliere Save settings (Salva impostazioni).

Per configurare il connettore a livello di carico di lavoro

1. Seleziona Carichi di lavoro nel riquadro di navigazione a sinistra e seleziona il nome del carico di lavoro che desideri configurare.
2. Scegli Properties (Proprietà).
3. Nel riquadro Jira, scegli Modifica.
4. Per configurare le impostazioni Jira del carico di lavoro, seleziona Ignora le impostazioni a livello di account.

   > **Note**
   >
   > Le impostazioni a livello di account Override devono essere selezionate per applicare le impostazioni specifiche del carico di lavoro.

5. Per Sync override, seleziona una delle seguenti opzioni:

   a. Per escludere il carico di lavoro da Jira sync, seleziona Non sincronizzare il carico di lavoro.

   b. Per scegliere manualmente quando sincronizzare il carico di lavoro, seleziona Sincronizza carico di lavoro - Manuale.

   c. Per sincronizzare automaticamente le modifiche del carico di lavoro, seleziona Sincronizza carico di lavoro - Automatico.

6. (Facoltativo) Per la chiave del progetto Jira, inserisci la chiave del progetto con cui sincronizzare il carico di lavoro. Questa chiave di progetto può essere diversa dalla chiave di progetto a livello di account.

   Se non specifichi una chiave di progetto, il connettore crea un progetto WA Jira.

7. Selezionare Salva.

Per informazioni dettagliate sull'esecuzione di una sincronizzazione manuale, consulta Sincronizzazione di un carico di lavoro.

Sincronizzazione di un carico di lavoro

Per la sincronizzazione automatica, il connettore sincronizza automaticamente gli elementi di miglioramento quando si aggiorna un carico di lavoro (ad esempio, quando si completa una domanda o si seleziona una nuova procedura consigliata).

Sia nella sincronizzazione manuale che in quella automatica, tutte le modifiche apportate in Jira (come il completamento di una domanda o le migliori pratiche) vengono sincronizzate con. AWS Well-Architected Tool

Per sincronizzare manualmente un carico di lavoro

1. Quando sei pronto per sincronizzare il tuo carico di lavoro con Jira, seleziona Carichi di lavoro nel riquadro di navigazione a sinistra. Quindi, seleziona il carico di lavoro che desideri sincronizzare.
2. Nella panoramica del carico di lavoro, scegli Sincronizza con Jira.
3. Seleziona l'obiettivo che desideri sincronizzare.
4. Per le domande da sincronizzare con Jira, seleziona le domande o gli interi pilastri che desideri sincronizzare con il progetto Jira.
    - Per tutte le domande che desideri rimuovere, seleziona l'icona X accanto al titolo della domanda.
5. Scegli Sincronizza.

Disinstallazione del connettore

Per disinstallare completamente AWS Well-Architected Tool Connector for Jira, esegui le seguenti operazioni:

- Disattiva la sincronizzazione con Jira in tutti i carichi di lavoro che sostituiscono le impostazioni di sincronizzazione a livello di account
- Disattiva la sincronizzazione con Jira a livello di account
- Scollega il tuo Account AWS account in Jira
- Disinstalla il connettore dal tuo account Jira

Per disattivare il connettore a livello di account

> **Note**
>
> I seguenti passaggi vengono eseguiti nel tuo Account AWS.

1. Seleziona Impostazioni nel riquadro di navigazione a sinistra.
2. Nella sezione Sincronizzazione dell'account Jira, scegli Modifica.
3. Deseleziona l'opzione Attiva la sincronizzazione dell'account Jira.
4. Scegliere Save settings (Salva impostazioni).

Per scollegare un Account AWS

> **Note**
>
> Tutti i passaggi seguenti vengono eseguiti nel tuo account Jira, non nel tuo. Account AWS

1. Accedi al tuo account Jira.
2. Nella barra di navigazione in alto, scegli App, quindi seleziona Gestisci le tue app.
3. Scegli la freccia a discesa accanto a AWS Well-Architected Tool Connector for Jira, quindi scegli Configura.
4. Nel riquadro AWS Well-Architected Tool Configurazione, per scollegare un Account AWS, scegli X in Azioni.

Per disinstallare il connettore

> **Note**
>
> Tutti i passaggi seguenti vengono eseguiti nel tuo account Jira, non nel tuo Account AWS. Ti consigliamo di verificare che tutte le connessioni Account AWS siano scollegate nella configurazione del connettore prima di disinstallare il connettore.

1. Accedi al tuo account Jira.
2. Nella barra di navigazione in alto, scegli App, quindi seleziona Gestisci le tue app.
3. Scegli la freccia a discesa accanto a AWS Well-Architected Tool Connector for Jira.
4. Scegli Disinstalla, quindi scegli Disinstalla app.

Milestone

Un milestone registra lo stato di un carico di lavoro in un determinato momento.

Salvare un milestone al temine del completamento iniziale di tutte le domande associate a un carico di lavoro. A seguito della modifica del carico di lavoro in base a elementi nel piano di miglioramento, puoi risparmiare ulteriori milestone per misurare lo stato di avanzamento.

Una best practice consiste nel salvare un milestone ogni volta che si apportano miglioramenti a un carico di lavoro.

Salvataggio di un milestone

Un milestone registra lo stato corrente di un carico di lavoro. Il proprietario di un carico di lavoro può salvare un milestone in qualsiasi momento.

Per salvare un milestone

1. Nella pagina dei dettagli del carico di lavoro, scegliere Save milestone (Salva milestone).
2. Nella casella Milestone name (Nome del milestone), immettere un nome per il milestone.

   > **Note**
   >
   > Il nome deve contenere da 3 a 100 caratteri. Almeno tre caratteri non devono essere costituiti da spazi. I nomi milestone associati a un carico di lavoro devono essere univoci. Spazi e maiuscole vengono ignorati durante la verifica dell'unicità.

3. Selezionare Save (Salva) per salvare il milestone.

Dopo il salvataggio di un milestone, non è possibile modificare i dati del carico di lavoro che sono stati registrati. Quando elimini un carico di lavoro, vengono eliminati anche i milestone associati.

Visualizzazione di milestone

Puoi visualizzare milestone per un carico di lavoro nei modi seguenti:

- Nella pagina dei dettagli del carico di lavoro, scegli Milestones (Milestone) e seleziona il milestone da visualizzare.

- Dalla pagina Dashboard (Pannello di controllo), scegli il carico di lavoro e nella sezione Milestones (Milestone) e seleziona il milestone da visualizzare.

Generazione di un report milestone

Puoi generare un report milestone. Il report contiene le risposte alle domande sul carico di lavoro, le note ed eventuali rischi elevati e medi che erano presenti al momento del salvataggio del milestone.

Un report consente di condividere i dettagli sul milestone con altri utenti che non hanno accesso a AWS Well-Architected Tool.

Per generare report milestone

1. Selezionare il milestone in uno dei seguenti modi.
   - Nella pagina dei dettagli del carico di lavoro, scegliere Milestones (Milestone) e selezionare il milestone.
   - Nella pagina Dashboard (Pannello di controllo), scegliere il carico di lavoro con il milestone di cui si desidera creare il report. Nella sezione Milestones (Milestone), scegliere il milestone.
2. Scegliere Generate report (Genera report) per generare un report.

   Viene generato un file PDF che può essere scaricato o visualizzato.

Condividi gli inviti

Un invito alla condivisione è una richiesta di condivisione di un carico di lavoro, un obiettivo personalizzato o un modello di recensione di proprietà di un altro account. AWS Un carico di lavoro o un obiettivo possono essere condivisi con tutti gli utenti di uno stessoAccount AWS, con singoli utenti o con entrambi.

- Se accetti un invito al carico di lavoro, il carico di lavoro viene aggiunto alle pagine Carichi di lavoro e Dashboard.
- Se accetti un invito a un obiettivo personalizzato, l'obiettivo viene aggiunto alla tua pagina Lenti personalizzate.
- Se accetti un invito al profilo, il profilo viene aggiunto alla pagina Profili.
- Se accetti un invito al modello di recensione, il modello viene aggiunto alla pagina dei modelli di recensione.

Se rifiuti, l'invito viene rimosso dall'elenco.

> **Note**
>
> I carichi di lavoro, gli obiettivi personalizzati, i profili e i modelli di recensione possono essere condivisi solo all'interno della stessaRegione AWS.

Il proprietario del carico di lavoro o dei controlli personalizzati dell'obiettivo con accesso condiviso.

La pagina Condividi gli inviti, disponibile nella barra di navigazione a sinistra, fornisce informazioni sul carico di lavoro in sospeso e sugli inviti personalizzati per obiettivi.

Le seguenti informazioni vengono visualizzate per ogni invito al carico di lavoro:

Nome

Il nome del carico di lavoro, dell'obiettivo personalizzato o del modello di recensione da condividere.

Tipo di risorsa

Il tipo di invito, Workload, Custom lens, Profiles o Review template.

Owner

L'Account AWSID che possiede il carico di lavoro.

Autorizzazione

L'autorizzazione concessa al carico di lavoro.

- Sola-lettura

  Fornisce accesso in sola lettura al carico di lavoro, all'obiettivo personalizzato, ai profili o al modello di recensione.

- Collaboratore

  Fornisce l'accesso di aggiornamento alle risposte e alle relative note e l'accesso di sola lettura al resto del carico di lavoro. Questa autorizzazione è disponibile solo per i carichi di lavoro.

Dettagli dell'autorizzazione

Descrizione dettagliata dell’autorizzazione.

Accettazione di un invito alla condivisione

Accettare un invito a condividere

1. Seleziona l'invito di condivisione da accettare.
2. Scegliere Accept (Accetta).

Per gli inviti ai carichi di lavoro, il carico di lavoro viene aggiunto alle pagine Carichi di lavoro e Dashboard. Per gli inviti con obiettivi personalizzati, l'obiettivo personalizzato viene aggiunto alla pagina Lenti personalizzate. Per gli inviti al profilo, il profilo viene aggiunto alla pagina Profili. Per gli inviti ai modelli di recensione, il modello viene aggiunto alla pagina Rivedi i modelli.

Hai sette giorni per accettare un invito. Se non lo accetti entro sette giorni, l'invito scade automaticamente.

Se un utente e Account AWS entrambi hanno accettato gli inviti al carico di lavoro, l'invito al carico di lavoro per l'utente determina l'autorizzazione dell'utente.

Rifiutare un invito alla condivisione

Rifiutare un invito alla condivisione

1. Seleziona il carico di lavoro o l'invito personalizzato all'obiettivo da rifiutare.
2. Scegli Rifiuta.

L'invito viene rimosso dall'elenco.

Notifiche

La pagina Notifiche mostra le differenze di versione per i carichi di lavoro e i modelli di recensione a cui sono associati obiettivi e profili. Puoi eseguire l'aggiornamento alla versione più recente di un obiettivo o di un profilo per un carico di lavoro dalla pagina Notifiche.

Notifiche sull'obiettivo

Quando è disponibile una nuova versione di un obiettivo, nella parte superiore della pagina Carichi di lavoro o Modelli di revisione viene visualizzato un banner per avvisarti. Se visualizzi un carico di lavoro o un modello di recensione specifico utilizzando un obiettivo obsoleto, vedrai anche un banner che indica che è disponibile una nuova versione di obiettivo.

Scegli Visualizza gli aggiornamenti disponibili per un elenco di carichi di lavoro o modelli di revisione che possono essere aggiornati.

Consulta le istruzioni su come aggiornare un obiettivo the section called “Aggiornamento di un obiettivo” per un carico di lavoro o un modello di revisione.

Quando il proprietario di un obiettivo condiviso lo elimina, se hai un carico di lavoro associato all'obiettivo eliminato, riceverai una notifica indicante che puoi ancora utilizzare l'obiettivo nel tuo carico di lavoro esistente, ma non potrai aggiungerlo a nuovi carichi di lavoro.

Notifiche sul profilo

Esistono due tipi di notifiche del profilo:

- Aggiornamento del profilo
- Eliminazione del profilo

Quando un profilo associato a un carico di lavoro è stato modificato (per ulteriori informazioni, consultathe section called “Modifica di un profilo”), nelle Notifiche del profilo viene visualizzata una notifica relativa alla disponibilità di una nuova versione del profilo.

Quando il proprietario di un profilo condiviso lo elimina, se hai un carico di lavoro associato al profilo eliminato, riceverai una notifica indicante che puoi ancora utilizzare il profilo nel carico di lavoro esistente, ma non potrai aggiungerlo a nuovi carichi di lavoro.

Per aggiornare una versione del profilo

1. Nel riquadro di navigazione a sinistra, seleziona Notifiche.
2. Seleziona il nome del carico di lavoro dall'elenco nella scheda Notifiche del profilo oppure utilizza la barra di ricerca per cercare in base al nome del carico di lavoro.
3. Scegli la versione di aggiornamento del profilo.
4. Nella sezione Riconoscimento, seleziona la casella di conferma relativa a Comprendo e accetto queste modifiche.
5. (Facoltativo) Se scegli di salvare un traguardo, seleziona la casella Salva un traguardo e fornisci un nome per un traguardo.
6. Seleziona Save (Salva).

Una volta aggiornato il profilo, il numero di versione e la data di aggiornamento più recenti vengono visualizzati nella sezione Profilo del carico di lavoro.

Per ulteriori informazioni, consulta Profili.

Dashboard (Pannello di controllo)

La dashboard, disponibile dalla barra di navigazione a sinistra, consente di accedere ai carichi di lavoro e ai relativi problemi a rischio medio e alto. Puoi anche includere i carichi di lavoro che sono stati condivisi con te. La dashboard è composta da quattro sezioni.

- Riepilogo: mostra il numero totale di carichi di lavoro, quanti presentano rischi alti e medi e il numero totale di problemi ad alto e medio rischio in tutti i carichi di lavoro.
- Problemi del Well-Architected Framework per pilastro: mostra una rappresentazione grafica dei problemi ad alto e medio rischio per pilastro per tutti i carichi di lavoro.
- Problemi di Well-Architected Framework per carico di lavoro: mostra i problemi ad alto e medio rischio per pilastro per ciascuno dei tuoi carichi di lavoro.
- Problemi di Well-Architected Framework per elemento del piano di miglioramento: mostra gli elementi del piano di miglioramento per tutti i carichi di lavoro.

Riepilogo

Questa sezione mostra il numero totale di carichi di lavoro e il numero di carichi di lavoro con problemi ad alto e medio rischio nell'ottica Well-Architected Framework e in tutti gli altri obiettivi. Viene visualizzato il numero totale di problemi ad alto e medio rischio in tutti i carichi di lavoro, di proprietà o condivisi con l'utenteAccount AWS.

Scegli Includi i carichi di lavoro condivisi con me per fare in modo che le statistiche di riepilogo, il report consolidato e le altre sezioni del dashboard riflettano sia i carichi di lavoro che i carichi di lavoro che sono stati condivisi con te.

Scegli Genera rapporto per avere un rapporto consolidato creato per te come file PDF.

Il nome del rapporto è sotto forma di:`wellarchitected_consolidatedreport_`*`account-ID`*`.pdf`.

Wellate Framework, problemi del Wellato Framework Framework,

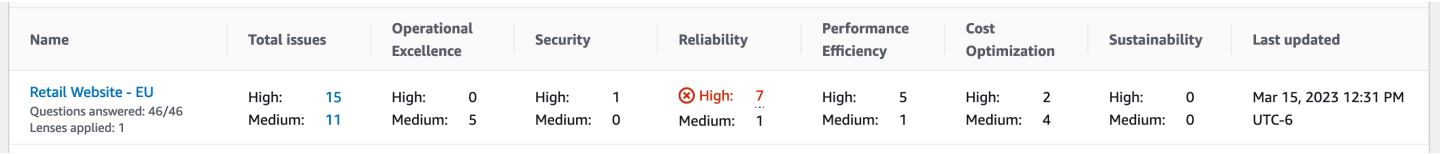
La sezione Problemi per pilastro del Well-Architected Framework mostra una rappresentazione grafica del numero di problemi ad alto e medio rischio per pilastro per tutti i carichi di lavoro.

Usa le sezioni rimanenti della dashboard per passare da un livello di dettaglio al successivo.

> **Note**
>
> In questa sezione sono inclusi solo i problemi dell'obiettivo Well-Architected Framework.

Problemi del Well-Well-Framework Framework di Well-Well-

La sezione Problemi di Well-Architected Framework per carico di lavoro mostra informazioni per ogni carico di lavoro.



Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Retail Website - EU Questions answered: 46/46 Lenses applied: 1	High: 15 Medium: 11	High: 0 Medium: 5	High: 1 Medium: 0	High: 7 Medium: 1	High: 5 Medium: 1	High: 2 Medium: 4	High: 0 Medium: 0	Mar 15, 2023 12:31 PM UTC-6

Le seguenti informazioni vengono visualizzate per ogni carico di lavoro:

Nome

Il nome del carico di lavoro. Vengono inoltre visualizzati il numero di domande a cui è stato risposto e il numero di obiettivi applicati al carico di lavoro.

Scegli il nome del carico di lavoro per visitare la pagina dei dettagli del carico di lavoro e visualizzare traguardi, piani di miglioramento e condivisioni.

Problemi totale dei problemi totale

Il numero totale di problemi identificati dall'obiettivo Well-Architected Framework per il carico di lavoro.

Scegli il numero di problemi ad alto o medio rischio per visualizzare i piani di miglioramento consigliati per tali problemi.

Eccellenza operativa

Il numero di problemi ad alto rischio (HRI) e a rischio medio (RM) identificati nel carico di lavoro per il pilastro dell'eccellenza operativa.

Sicurezza

Il numero di HRI e risonanza magnetica identificati per il pilastro Sicurezza.

Affidabilità

Il numero di HRI e RM identificati per il pilastro Affidabilità.

Efficacia delle prestazioni

Il numero di HRI e RM identificati per il pilastro dell'efficienza delle prestazioni.

Ottimizzazione dei costi

Il numero di HRI e risonanza magnetica identificati per il pilastro dell'ottimizzazione dei costi.

Sostenibilità

Il numero di HRI e risonanza magnetica identificati per il pilastro Sostenibilità.

Ultimo aggiornamento

Data e ora dell'ultimo aggiornamento del carico di lavoro.

Per ogni carico di lavoro, viene evidenziato il pilastro con il maggior numero di problemi ad alto rischio (HRI).

> **Note**
>
> In questa sezione sono inclusi solo i problemi dell'obiettivo Well-Architected Framework.

I problemi del Well-Framework Framework di Well-Well-Framework

La sezione Problemi relativi al piano di miglioramento di Well-Architected Framework mostra gli elementi del piano di miglioramento per tutti i carichi di lavoro. Puoi filtrare gli articoli in base al pilastro e alla gravità.

Vengono visualizzate le seguenti informazioni per ogni elemento del piano di miglioramento le seguenti informazioni per ogni elemento del piano di miglioramento

elemento di miglioramento dell'elemento

Il nome dell'elemento del piano di miglioramento.

Scegli il nome per mostrare la best practice associata all'elemento del piano di miglioramento.

Pilastro

Il pilastro associato all'elemento di miglioramento.

Rischio

Indica se il problema associato è a rischio elevato o medio.

Carichi di lavoro applicabili

Il numero di carichi di lavoro a cui si applica questo piano di miglioramento.

Seleziona un elemento del piano di miglioramento per visualizzare i carichi di lavoro applicabili.

> **Note**
>
> In questa sezione sono inclusi solo gli elementi del piano di miglioramento dell'obiettivo Well-Architected Framework.

Sicurezza dell'AWS Well-Architected Tool

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWSe l'utente. Il modello di responsabilità condivisa fa riferimento ad una sicurezza del cloud e nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS in Cloud AWS. AWS fornisce inoltre i servizi che è possibile utilizzare in modo sicuro. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili a AWS Well-Architected Tool, consulta Servizi AWScoperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWSche utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione serve a facilitare la comprensione dell'applicazione del modello di responsabilità condivisa quando si utilizza l'AWS WA Tool. I seguenti argomenti illustrano come configurare l'AWS WA Tool per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri servizi di AWS per monitorare e proteggere le risorse AWS WA Tool.

Argomenti

- Protezione dei dati dell'AWS Well-Architected Tool
- Gestione delle identità e degli accessi per l'AWS Well-Architected Tool
- Risposta agli incidenti in AWS Well-Architected Tool
- Convalida della conformità per AWS Well-Architected Tool
- Resilienza nell'AWS Well-Architected Tool
- Sicurezza dell'infrastruttura nell'AWS Well-Architected Tool
- Analisi della configurazione e delle vulnerabilità in AWS Well-Architected Tool
- Prevenzione del confused deputy tra servizi

Protezione dei dati dell'AWS Well-Architected Tool

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

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWSe di configurare i singoli utenti con AWS IAM Identity Centero AWS Identity and Access Management(IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei percorsi CloudTrail per acquisire le attività AWS, consulta Utilizzo dei percorsi CloudTrail nella Guida per l'utente di AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei 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 necessiti di moduli crittografici convalidati FIPS 140-3 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

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

Crittografia dei dati a riposo

Tutti i dati inattivi memorizzati da AWS WA Tool sono crittografati.

Crittografia in transito

Tutti i dati in transito da e verso AWS WA Tool sono crittografati.

Come AWS utilizza i tuoi dati

Il team AWS Well-Architected raccoglie dati aggregati dallo AWS Well-Architected Tool per fornire e migliorare il servizio AWS WA Tool per i clienti. I dati dei singoli clienti possono essere condivisi con i team dell'Account AWS per supportare gli sforzi dei nostri clienti per migliorare i carichi di lavoro e l'architettura. Il team AWS Well-Architected può accedere solo alle proprietà del carico di lavoro e alle scelte selezionate per ogni domanda. AWS non condivide alcun dato proveniente dallo AWS WA Tool al di fuori di AWS.

Le proprietà del carico di lavoro a cui il team AWS Well-Architected ha accesso includono:

- Nome del carico di lavoro
- Proprietario del riesame
- Ambiente
- Regioni
- ID account
- Tipo di settore

Il team AWS Well-Architected non ha accesso a:

- Descrizione del carico di lavoro
- Progettazione dell’architettura
- Tutte le note inserite

Gestione delle identità e degli accessi per l'AWS Well-Architected Tool

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse AWS WA Tool. IAM è un Servizio AWS che è possibile utilizzare senza alcun costo aggiuntivo.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Funzionamento di AWS Well-Architected Tool con IAM
- Esempi di policy AWS Well-Architected Tool di basate su identità
- Policy gestite da AWS per AWS Well-Architected Tool
- Risoluzione dei problemi di identità e accesso in AWS Well-Architected Tool

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in AWS WA Tool.

Utente del servizio: se utilizzi il servizio AWS WA Tool per eseguire il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità AWS WA Tool utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS WA Tool, consulta Risoluzione dei problemi di identità e accesso in AWS Well-Architected Tool.

Amministratore del servizio: se sei il responsabile delle risorse AWS WA Tool presso la tua azienda, probabilmente disponi dell'accesso completo a AWS WA Tool. Il tuo compito è determinare le caratteristiche e le risorse AWS WA Tool a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS WA Tool, consulta Funzionamento di AWS Well-Architected Tool con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS WA Tool. Per visualizzare policy basate su identità di AWS WA Tool di esempio che è possibile utilizzare in IAM, consulta Esempi di policy AWS Well-Architected Tool di basate su identità.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWScon le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

È possibile accedere ad AWScome identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, è possibile accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWSnella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia della linea di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente

root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ad Servizi AWSutilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono a Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWSche dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali

temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM nella AWS Management Console, è possibile passare da un ruolo utente a un ruolo IAM (console). È possibile assumere un ruolo chiamando un'operazione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso multi-servizio: alcuni Servizi AWSutilizzano funzionalità che in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Forward access sessions (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è

possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. La tecnologia FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con la richiesta di un Servizio AWS per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che comporta interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, è possibile creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Use an IAM role to grant permissions to applications running on Amazon EC2 instances nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWSè possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

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

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

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

Liste di controllo degli accessi (ACL)

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

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

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, è possibile applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni sulle SCP, consulta Policy di controllo dei servizi nella AWS OrganizationsGuida per l'utente di Organizations.
- Policy di controllo delle risorse (RCP): le RCP sono policy JSON che consentono di impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le policy IAM collegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account membri e può influire sulle autorizzazioni valide per le identità, tra cui Utente root

dell'account AWS, indipendentemente dal fatto che appartengano o meno alla tua organizzazione. Per ulteriori informazioni su organizzazioni e RCP, incluso un elenco di Servizi AWS che supportano le RCP, consulta Resource control policies (RCPs) nella Guida per l'utente di AWS Organizations.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWSdetermina se consentire una richiesta quando sono coinvolti più tipi di policy, consultare Logica di valutazione delle policy nella Guida per l'utente di IAM.

Funzionamento di AWS Well-Architected Tool con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS WA Tool, scopri quali funzionalità di IAM sono disponibili per l'uso con AWS WA Tool.

Funzionalità IAM che è possibile utilizzare con AWS Well-Architected Tool

Funzionalità IAM	Supporto di AWS WA Tool
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No

Funzionalità IAM	Supporto di AWS WA Tool
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per ottenere un quadro generale del funzionamento di AWS WA Tool e altri servizi AWS con la maggior parte delle caratteristiche di IAM, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Policy AWS WA Tool basate su identità

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

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

Policy basate su risorse all'interno di AWS WA Tool

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa,

una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Operazioni di policy per AWS WA Tool

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le operazioni delle policy in AWS WA Tool utilizzano il seguente prefisso prima dell'operazione: `wellarchitected:`. Ad esempio, per consentire a un'entità di definire un carico di lavoro, un amministratore deve collegare una policy che consenta operazioni `wellarchitected:CreateWorkload`. Analogamente, per evitare che un'entità elimini i carichi di lavoro, l'amministratore può collegare una policy che non consenta le operazioni `wellarchitected:DeleteWorkload`. Le istruzioni delle policy devono includere un elemento `Action` o `NotAction`. AWS WA Tooldefinisce un proprio set di operazioni che descrivono le attività che è possibile eseguire con questo servizio.

Per visualizzare un elenco di operazioni AWS WA Tool, consulta Operazioni definite da AWS Well-Architected Tool in Riferimento per l'autorizzazione del servizio.

Risorse relative alle policy

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco di tipi di risorse AWS WA Tool e dei relativi ARN, consulta Risorse definite da AWS Well-Architected Tool nella Guida di riferimento sull'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Well-Architected Tool.

La risorsa del carico di lavoro AWS WA Tool ha il seguente ARN:

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

Per ulteriori informazioni sul formato degli ARN, consulta Nome della risorsa Amazon (ARN) e spazi dei nomi del servizio AWS.

L'ARN può essere trovato nella pagina delle proprietà del carico di lavoro dei un carico di lavoro. Ad esempio, per specificare un carico di lavoro specifico:

```
"Resource": "arn:aws:wellarchitected:us-
west-2:123456789012:workload/11112222333344445555666677778888"
```

Per specificare tutti i carichi di lavoro che appartengono a un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

Alcune operazioni AWS WA Tool, ad esempio quelle per la creazione e l'elencazione di carichi di lavoro, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Per visualizzare un elenco di tipi di risorse AWS WA Tool e dei relativi ARN, consulta Risorse definite da AWS Well-Architected Tool nella Guida di riferimento sull'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS Well-Architected Tool.

Chiavi di condizione delle policy per AWS WA Tool

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWSutilizzando un'operazione `AND`logica. Se specifichi più valori per una singola chiave di condizione, AWSvaluta la condizione utilizzando un'operazione 0Rlogica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

AWS WA Tool fornisce una chiave di condizione specifica del servizio (`wellarchitected:JiraProjectKey`) e supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta AWS Global Condition Context Keys nella Guida di riferimento per l'autorizzazione del servizio.

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

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

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Liste di controllo degli accessi in AWS WA Tool

Supporta le ACL: no

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

Autorizzazione basata su tag AWS WA Tool

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS WA Tool

Supporta le credenziali temporanee: sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWSche funzionano con le credenziali temporanee, consulta Servizi AWSsupportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Consoleutilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi alla AWSutilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo

scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLI o l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni del principale tra servizi per AWS WA Tool

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. La tecnologia FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con la richiesta di un Servizio AWS per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che comporta interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS WA Tool

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi per l'AWS WA Tool

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked

role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy AWS Well-Architected Tool di basate su identità

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS WA Tool. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, AWS CLI o un'API 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 devi quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

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

Argomenti

- Best practice delle policy
- Utilizzo della console di AWS WA Tool
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Concessione dell'accesso completo ai carichi di lavoro
- Concessione dell'accesso in sola lettura ai carichi di lavoro
- Accesso a un carico di lavoro
- Utilizzo di una chiave di condizione specifica del servizio per AWS Well-Architected Tool Connector for Jira

Best practice delle policy

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

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo

policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWSper le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È possibile inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

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

Utilizzo della console di AWS WA Tool

Per accedere alla console AWS Well-Architected Tool è necessario disporre di un insieme di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse AWS WA Tool nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la console AWS WA Tool, collega anche la seguente policy gestita AWS alle entità:

```
WellArchitectedConsoleReadOnlyAccess
```

Per consentire la possibilità di creare, modificare ed eliminare carichi di lavoro, collegare la seguente policy gestita AWS alle entità:

```
WellArchitectedConsoleFullAccess
```

Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Non sono necessarie le autorizzazioni minime della console per gli utenti che effettuano chiamate solo all'API di AWS CLI o di AWS. 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 cpllegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API 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": "*"
        }
    ]
}
```

Concessione dell'accesso completo ai carichi di lavoro

In questo esempio, si desidera concedere a un utente nel tuo Account AWS l'accesso completo ai carichi di lavoro. L'accesso completo consente all'utente di eseguire tutte le operazioni in AWS WA Tool. Questo accesso è necessario per definire, eliminare, visualizzare e aggiornare i carichi di lavoro.

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

Concessione dell'accesso in sola lettura ai carichi di lavoro

In questo esempio, desideri concedere a un utente nell'Account AWS l'accesso in sola lettura ai carichi di lavoro. L'accesso in sola lettura consente all'utente di visualizzare i carichi di lavoro in AWS WA Tool.

```
{
```

```
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "*"
     }
   ]
}
```

Accesso a un carico di lavoro

In questo esempio, desideri concedere a un utente nell'Account AWS l'accesso in sola lettura a uno dei carichi di lavoro, 99999999999955555555555566666666, nella Regione `us-west-2`. L'ID dell'account è 777788889999.

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
     }
   ]
}
```

Utilizzo di una chiave di condizione specifica del servizio per AWS Well-Architected Tool Connector for Jira

In questo esempio viene illustrato come utilizzare la chiave di condizione specifica del servizio `wellarchitected:JiraProjectKey` per controllare quali progetti Jira possono essere collegati ai carichi di lavoro nel tuo account.

Di seguito vengono descritti gli usi pertinenti della chiave di condizione:

- **`CreateWorkload`:** quando applichi `wellarchitected:JiraProjectKey` a `CreateWorkload`, puoi definire i progetti Jira personalizzati che possono essere collegati a qualsiasi carico di lavoro creato dall'utente. Ad esempio, se un utente tenta di creare un nuovo carico di lavoro con il progetto ABC, ma la policy specifica solo il progetto PQR, l'azione viene negata.
- **`UpdateWorkload`:** quando applichi `wellarchitected:JiraProjectKey` a `UpdateWorkload`, puoi definire i progetti Jira personalizzati che possono essere collegati a un determinato carico di lavoro oppure a qualsiasi carico di lavoro. Ad esempio, se un utente tenta di aggiornare un carico di lavoro esistente con il progetto ABC, ma la policy specifica il progetto PQR, l'azione viene negata. Inoltre, se l'utente ha un carico di lavoro collegato al progetto PQR e tenta di aggiornare il carico di lavoro per collegarlo al progetto ABC, l'azione viene negata.
- **`UpdateGlobalSettings`:** quando applichi `wellarchitected:JiraProjectKey` a `UpdateGlobalSettings`, puoi definire i progetti Jira personalizzati che possono essere collegati all'Account AWS. L'impostazione a livello di account protegge i carichi di lavoro del tuo account che non sostituiscono le impostazioni di Jira a livello di account. Ad esempio, se un utente ha accesso a `UpdateGlobalSettings`, non può collegare i carichi di lavoro del tuo account ai progetti che non sono specificati nella policy.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateGlobalSettings",
    "wellarchitected:CreateWorkload"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  },
  {
   "Sid": "VisualEditor1",
   "Effect": "Allow",
   "Action": [
```

```
    "wellarchitected:UpdateWorkload"
   ],
   "Resource": "WORKLOAD_ARN",
   "Condition": {
    "StringEqualsIfExists": {
     "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  }
 ]
}
```

Policy gestite da AWS per AWS Well-Architected Tool

Una policy gestita da AWSè una policy autonoma creata e amministrata da AWS. Le policy gestite da AWSsono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWSpotrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWSaggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

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

Policy gestita da AWS: WellArchitectedConsoleFullAccess

È possibile allegare la policy `WellArchitectedConsoleFullAccess` alle identità IAM.

Questa policy concede l'accesso completo ad AWS Well-Architected Tool.

Dettagli dell'autorizzazione

```
{
```

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

Policy gestita da AWS: WellArchitectedConsoleReadOnlyAccess

È possibile allegare la policy `WellArchitectedConsoleReadOnlyAccess` alle identità IAM.

Questa policy concede l'accesso in sola lettura a AWS Well-Architected Tool.

Dettagli dell'autorizzazione

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
          "wellarchitected:ExportLens"
     ],
     "Resource": "*"
     }
   ]
}
```

Policy gestita da AWS: AWSWellArchitectedOrganizationsServiceRolePolicy

È possibile allegare la policy `AWSWellArchitectedOrganizationsServiceRolePolicy` alle identità IAM.

Questa policy concede le autorizzazioni amministrative in AWS Well-Architected Tool che sono necessarie per supportare l'integrazione di AWS Organizations con Organizations. Queste

autorizzazioni consentono all'account di gestione dell'organizzazione di abilitare la condivisione delle risorse con AWS WA Tool.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations:ListAWSServiceAccessForOrganization`: consente ai principali di verificare se l'accesso al servizio AWS è abilitato per AWS WA Tool.
- `organizations:DescribeAccount`: consente ai principali di recuperare informazioni su un account nell'organizzazione.
- `organizations:DescribeOrganization`: consente ai principali di recuperare informazioni sulla configurazione dell'organizzazione.
- `organizations:ListAccounts`: consente ai principali di recuperare l'elenco degli account che appartengono a un'organizzazione.
- `organizations:ListAccountsForParent`: consente ai principali di recuperare l'elenco degli account che appartengono a un'organizzazione da un determinato nodo root dell'organizzazione.
- `organizations:ListChildren`: consente ai principali di recuperare l'elenco degli account e delle unità organizzative che appartengono a un'organizzazione da un determinato nodo root dell'organizzazione.
- `organizations:ListParents`: consente ai principali di recuperare l'elenco degli elementi padre diretti specificati dall'unità organizzativa o dall'account all'interno di un'organizzazione.
- `organizations:ListRoots`: consente ai principali di recuperare l'elenco di tutti i nodi root all'interno di un'organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
```

```
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        }
    ]
}
```

Policy gestita da AWS: AWSWellArchitectedDiscoveryServiceRolePolicy

È possibile allegare la policy `AWSWellArchitectedDiscoveryServiceRolePolicy` alle identità IAM.

Questa policy consente allo AWS Well-Architected Tool di accedere alle risorse e ai servizi AWS correlati alle risorse di AWS WA Tool.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `trustedadvisor:DescribeChecks`: elenca i controlli Trusted Advisor disponibili.
- `trustedadvisor:DescribeCheckItems`: recupera i dati di controllo di Trusted Advisor, inclusi lo stato e le risorse contrassegnati da Trusted Advisor.
- `servicecatalog:GetApplication`: recupera i dettagli di un'applicazione AppRegistry.
- `servicecatalog:ListAssociatedResources`: elenca le risorse associate a un'applicazione AppRegistry.
- `cloudformation:DescribeStacks`: ottiene i dettagli degli stack AWS CloudFormation.
- `cloudformation:ListStackResources`: elenca le risorse associate agli stack AWS CloudFormation.
- `resource-groups:ListGroupResources`: elenca le risorse di un ResourceGroup.
- `tag:GetResources`: richiesta per ListGroupResources.
- `servicecatalog:CreateAttributeGroup`: crea un gruppo di attributi gestito dal servizio quando richiesto.
- `servicecatalog:AssociateAttributeGroup`: associa un gruppo di attributi gestito dal servizio a un'applicazione AppRegistry.
- `servicecatalog:UpdateAttributeGroup`: aggiorna un gruppo di attributi gestito dal servizio.

- `servicecatalog:DisassociateAttributeGroup`: dissocia un gruppo di attributi gestito dal servizio da un'applicazione AppRegistry.
- `servicecatalog:DeleteAttributeGroup`: elimina un gruppo di attributi gestito dal servizio quando richiesto.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeChecks",
    "trustedadvisor:DescribeCheckItems"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:GetApplication",
    "servicecatalog:CreateAttributeGroup"
   ],
   "Resource": [
    "*"
   ]
  },
  {
```

```
    "Effect": "Allow",
    "Action": [
     "servicecatalog:AssociateAttributeGroup",
     "servicecatalog:DisassociateAttributeGroup"
    ],
    "Resource": [
     "arn:*:servicecatalog:*:*:/applications/*",
     "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:UpdateAttributeGroup",
     "servicecatalog:DeleteAttributeGroup"
    ],
    "Resource": [
     "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
   }
  ]
}
```

Aggiornamenti di AWS WA Tool alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per AWS WA Tool da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di AWS WA Tool.

Modifica	Descrizione	Data
AWS WA Tool: modifica della policy gestita	È stato aggiunto `"wellarchitected:Export*"` a `WellArchitectedConsoleReadOnlyAccess`.	22 giugno 2023
AWS WA Tool: aggiunta della policy del ruolo di servizio	È stato aggiunto `AWSWellArchitectedDiscoveryServiceRolePolicy` per consentire allo AWS Well-	3 maggio 2023

Modifica	Descrizione	Data
	Architected Tool di accedere alle risorse e ai servizi AWS correlati alle risorse di AWS WA Tool.	
AWS WA Tool: aggiunta di autorizzazioni	È stata aggiunta una nuova azione per concedere le autorizzazioni a `ListAWSServiceAccessForOrganization` per consentire allo AWS WA Tool di verificare se l'accesso al servizio AWS è abilitato per AWS WA Tool.	22 luglio 2022
AWS WA Tool ha iniziato il rilevamento delle modifiche	AWS WA Tool ha iniziato il rilevamento delle modifiche per le relative policy gestite da AWS.	22 luglio 2022

Risoluzione dei problemi di identità e accesso in AWS Well-Architected Tool

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di AWS WA Tool e di IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione in AWS WA Tool

Non sono autorizzato a eseguire un'operazione in AWS WA Tool

Se la AWS Management Console indica che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'esempio di errore seguente viene visualizzato quando l'utente *`mateojackson`* cerca di utilizzare la console per eseguire lazione `DeleteWorkload`, ma non dispone delle autorizzazioni necessarie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: wellarchitected:DeleteWorkload on resource: 11112222333344445555666677778888
```

Per questo esempio, devi contattare l'amministratore per l'aggiornamento delle policy in modo che venga autorizzato l'accesso alla risorsa `11112222333344445555666677778888` utilizzando l'operazione `wellarchitected:DeleteWorkload`.

Risposta agli incidenti in AWS Well-Architected Tool

La risposta agli eventi imprevisti per AWS Well-Architected Tool è una responsabilità AWS. AWS dispone di una policy e un programma formali e documentati che regolano la risposta agli eventi imprevisti.

I problemi operativi AWS con ampio impatto sono pubblicati sul AWS Service Health Dashboard.

Le questioni operative sono anche registrate nei singoli account tramite AWS Health Dashboard. Per ulteriori informazioni su come utilizzare AWS Health Dashboard, consulta la Guida per l'utente di AWS Health.

Convalida della conformità per AWS Well-Architected Tool

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti i Servizi AWSsono conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- AWSGuide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWSe verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: questo Servizio AWS rileva potenziali minacce ad Account AWS, carichi di lavoro, container e dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty soddisfa i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità e garantisce il rispetto di vari standard come il PCI DSS.
- AWS Audit Manager: grazie a questo Servizio AWS esegui l'audit continuo dell'utilizzo di AWS, semplificando la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza nell'AWS Well-Architected Tool

L'infrastruttura globale di AWS è progettata attorno a Regioni AWS e zone di disponibilità. Regioni AWS fornisce più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

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

Sicurezza dell'infrastruttura nell'AWS Well-Architected Tool

Come servizio gestito, AWS Well-Architected Tool è protetto dalla sicurezza di rete globale AWS. Per informazioni sui servizi di sicurezza AWSe su come AWSprotegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWSutilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWSWell-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere all'AWS WA Tool tramite la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

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

Analisi della configurazione e delle vulnerabilità in AWS Well-Architected Tool

Configurazione e controllo IT sono una responsabilità condivisa tra AWSe te, il nostro cliente. Per ulteriori informazioni, consulta il modello di responsabilità condivisa di AWS.

Prevenzione del confused deputy tra servizi

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. In AWS, la rappresentazione cross-service può comportare il problema confused deputy. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy delle risorse per limitare le autorizzazioni con cui AWS Well-Architected Tool fornisce un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:wellarchitected:*:`*`123456789012`*`:*`.

Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.

Il valore di `aws:SourceArn` deve essere un carico di lavoro o un obiettivo.

L'esempio seguente mostra il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` in AWS WA Tool per prevenire il problema confused deputy.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:ActionName",
    "Resource": [
      "arn:aws:wellarchitected:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
```

```
      }
    }
}
```

Condivisione delle AWS WA Tool risorse

Per condividere una risorsa di tua proprietà, procedi come segue:

- Attiva la condivisione delle risorse all'interno AWS Organizations (facoltativo)
- Condividi un carico di lavoro
- Condividi un obiettivo personalizzato
- Condividi un profilo
- Condividi un modello di recensione

> **Note**
>
> - La condivisione di una risorsa la rende disponibile per l'uso da parte di responsabili esterni a chi Account AWS ha creato la risorsa. La condivisione non modifica le autorizzazioni che si applicano alla risorsa nell'account che l'ha creata.
> - AWS WA Toolè un servizio regionale. I principali con cui condividi possono accedere alle condivisioni di risorse solo nelle aree Regioni AWS in cui sono state create.
> - Per condividere risorse in una Regione introdotta dopo il 20 marzo 2019, sia tu che la persona condivisa Account AWS dovete abilitare la Regione in. AWS Management Console Per ulteriori informazioni, consulta AWSGlobal Infrastructure.

Attiva la condivisione delle risorse all'interno AWS Organizations

Quando il tuo account è gestito daAWS Organizations, puoi trarne vantaggio per condividere le risorse più facilmente. Con o senza Organizations, un utente può condividere con account individuali. Tuttavia, se l'account si trova in un'organizzazione, è possibile condividerlo con singoli account o con tutti gli account dell'organizzazione o di un'unità organizzativa senza dover enumerare ogni account.

Per condividere le risorse all'interno di un'organizzazione, devi prima utilizzare la AWS WA Tool console o AWS Command Line Interface (AWS CLI) per abilitare la condivisione con. AWS Organizations Quando condividi risorse all'interno dell'organizzazione, AWS WA Tool non invia inviti ai dirigenti. I responsabili della tua organizzazione hanno accesso a risorse condivise senza scambiarsi inviti.

Quando attivi la condivisione delle risorse all'interno dell'organizzazione, AWS WA Tool crea un ruolo collegato al servizio chiamato. `AWSServiceRoleForWellArchitected` Questo ruolo può essere assunto solo dal AWS WA Tool servizio e concede l'AWS WA Toolautorizzazione a recuperare informazioni sull'organizzazione di cui è membro, utilizzando la politica gestita. AWS `AWSWellArchitectedOrganizationsServiceRolePolicy`

Se non è più necessario condividere le risorse con l'intera organizzazione o le unità organizzative, è possibile disabilitare la condivisione delle risorse.

Requisiti

- È possibile eseguire questi passaggi solo dopo aver effettuato l'accesso come responsabile nell'account di gestione dell'organizzazione.
- L'organizzazione deve avere tutte le funzionalità abilitate. Per ulteriori informazioni, vedere Abilitazione di tutte le funzionalità dell'organizzazione nella Guida per l'AWS Organizationsutente.

> **Important**
>
> È necessario attivare la condivisione con AWS Organizations utilizzando la AWS WA Tool console. Ciò garantisce la creazione del ruolo collegato ai servizi `AWSServiceRoleForWellArchitected`. Se attivi l'accesso affidabile AWS Organizations tramite la AWS Organizations console o il enable-aws-service-accessAWS CLIcomando, il ruolo `AWSServiceRoleForWellArchitected` collegato al servizio non viene creato e non puoi condividere risorse all'interno dell'organizzazione.

Per attivare la condivisione delle risorse all'interno dell'organizzazione

1. Accedi AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.

   Devi accedere come responsabile nell'account di gestione dell'organizzazione.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Scegli Attiva AWS Organizations supporto.
4. Scegliere Save settings (Salva impostazioni).

Per disabilitare la condivisione delle risorse all'interno dell'organizzazione

1. Accedi AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.

   Devi accedere come responsabile nell'account di gestione dell'organizzazione.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Deseleziona Attiva AWS Organizations supporto.
4. Scegliere Save settings (Salva impostazioni).

Tagging delle risorse AWS WA Tool

Per semplificare la gestione delle risorse AWS WA Tool, è possibile assegnare metadati personalizzati a ciascuna risorsa sotto forma di tag. Questo argomento descrive i tag e mostra come crearli.

Indice

- Nozioni di base sui tag
- Tagging delle risorse
- Limitazioni applicate ai tag
- Utilizzo di tag tramite la console
- Lavorare con i tag utilizzando l'API

Nozioni di base sui tag

Un tag è un'etichetta che assegni a una risorsa AWS. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di categorizzare le risorse AWS per scopo, proprietario o ambiente. In presenza di un numero elevato di risorse, è possibile individuare rapidamente una risorsa specifica in base ai tag assegnati. Ad esempio, puoi definire un set di tag per i servizi AWS WA Tool per monitorare il proprietario di ogni servizio e il livello di stack. Ti consigliamo di definire un set coerente di chiavi di tag per ogni tipo di risorsa.

I tag non vengono assegnati automaticamente alle risorse. Dopo aver aggiunto un tag, è possibile modificarne le chiavi e i valori o rimuovere i tag da una risorsa in qualsiasi momento. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

I tag non hanno alcun significato semantico per AWS WA Tool e vengono interpretati rigorosamente come una stringa di caratteri. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente.

Puoi lavorare con i tag utilizzando la AWS Management Console, l'AWS CLI e l'API AWS WA Tool.

Se utilizzi AWS Identity and Access Management (IAM), puoi controllare quali utenti del tuo account Account AWS sono autorizzati a creare, modificare o eliminare i tag.

Tagging delle risorse

Puoi taggare AWS WA Tool risorse nuove o esistenti.

Se utilizzi la AWS WA Tool console, puoi applicare tag alle nuove risorse al momento della creazione o alle risorse esistenti in qualsiasi momento. Per i carichi di lavoro esistenti puoi applicare i tag tramite la scheda Proprietà. Agli obiettivi personalizzati, ai profili e ai modelli di recensione esistenti, puoi applicare i tag tramite la scheda Panoramica.

Se utilizzi l'API AWS WA Tool, l'AWS CLI o un SDK AWS, puoi applicare i tag alle nuove risorse mediante il parametro `tags` nell'operazione API rilevante oppure alle risorse esistenti mediante l'operazione API `TagResource`. Per ulteriori informazioni, consulta TagResource.

Alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione. Se i tag non possono essere applicati durante la creazione della risorsa, il processo di creazione della risorsa avrà esito negativo. In questo modo, le risorse a cui desideri applicare tag al momento della creazione vengono create con tag specifici o non vengono create affatto. Se aggiungi tag alle risorse al momento della creazione, non devi eseguire script di tagging personalizzati dopo la creazione delle risorse.

Nella seguente tabella sono descritte le risorse AWS WA Tool a cui puoi associare i tag, nonché le risorse che possono essere associate a tag in fase di creazione.

Supporto del tagging per le risorse AWS WA Tool

Risorsa	support dei tag	Supporto della propagazione di tag	Supporto del tagging in fase di creazione (API AWS WA Tool, AWS CLI, SDK AWS)
AWS WA Toolcarichi di lavoro	Sì	No	Sì
AWS WA Toollenti personalizzate	Sì	No	Sì
AWS WA Toolprofili	Sì	No	Sì
AWS WA Toolmodelli di revisione	Sì	No	Sì

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- La lunghezza massima della chiave è 128 caratteri Unicode in formato UTF-8
- La lunghezza massima del valore è 256 caratteri Unicode in formato UTF-8
- Se lo schema di tagging viene utilizzato in più servizi e risorse AWS, è necessario tenere presente che in altri servizi possono essere presenti limiti sui caratteri consentiti. I caratteri generalmente consentiti sono: lettere, numeri, spazi rappresentabili in formato UTF-8 e i seguenti caratteri speciali + – = . _ : / @.
- i valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole;
- Non utilizzare `aws:`, `AWS:` o qualsiasi combinazione di maiuscole o minuscole di un tale prefisso per chiavi o valori poiché tali stringhe sono riservate per l'utilizzo esclusivo da parte di AWS. Non è possibile modificare né eliminare le chiavi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati ai fini del tags-per-resource limite.

Utilizzo di tag tramite la console

Utilizzando la AWS WA Tool console, puoi gestire i tag associati a risorse nuove o esistenti.

Aggiunta di tag a una singola risorsa alla creazione

Puoi aggiungere tag alle AWS WA Tool risorse quando le crei.

Aggiunta ed eliminazione di tag in una singola risorsa

AWS WA Toolconsente di aggiungere o eliminare i tag associati alle risorse direttamente dalla scheda Proprietà per un carico di lavoro e dalla scheda Panoramica per obiettivi, profili e modelli di recensione personalizzati.

Per aggiungere o eliminare un tag su un carico di lavoro

1. Accedi AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.

2. Dalla barra di navigazione, scegli la regione da usare.
3. Nel riquadro di navigazione, scegli Carichi di lavoro.
4. Seleziona il carico di lavoro da modificare e scegli Proprietà.
5. Nella sezione Tags scegliere Manage tags (Gestisci tag).
6. Aggiungi o elimina i tag secondo necessità.
   - Per aggiungere un tag, scegli Aggiungi nuovo tag e compila i campi Chiave e Valore.
   - Per rimuovere un tag, scegliere Remove (Rimuovi).
7. Ripeti questa procedura per ogni tag che desideri aggiungere, modificare o eliminare. Scegliere Save (Salva) per salvare le modifiche.

Per aggiungere o eliminare un tag su un obiettivo personalizzato

1. Accedi AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Dalla barra di navigazione, scegli la regione da usare.
3. Nel pannello di navigazione, scegli Obiettivi personalizzati.
4. Seleziona il nome dell'obiettivo personalizzato da modificare.
5. Nella sezione Tag della scheda Panoramica, scegli Gestisci tag.
6. Aggiungi o elimina i tag secondo necessità.
   - Per aggiungere un tag, scegli Aggiungi nuovo tag e compila i campi Chiave e Valore.
   - Per rimuovere un tag, scegliere Remove (Rimuovi).
7. Ripeti questa procedura per ogni tag che desideri aggiungere, modificare o eliminare. Scegliere Save (Salva) per salvare le modifiche.

Per aggiungere o eliminare un tag su un profilo

1. Accedi AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Dalla barra di navigazione, scegli la regione da usare.
3. Nel riquadro di navigazione, scegli Profili.
4. Seleziona il nome del profilo da modificare.
5. Nella sezione Tag della scheda Panoramica, scegli Gestisci tag.

6. Aggiungi o elimina i tag secondo necessità.
   - Per aggiungere un tag, scegli Aggiungi nuovo tag e compila i campi Chiave e Valore.
   - Per rimuovere un tag, scegliere Remove (Rimuovi).
7. Ripeti questa procedura per ogni tag che desideri aggiungere, modificare o eliminare. Scegliere Save (Salva) per salvare le modifiche.

Per aggiungere o eliminare un tag su un modello di recensione

1. Accedi AWS Management Console e apri la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Dalla barra di navigazione, scegli la regione da usare.
3. Nel riquadro di navigazione, scegli Rivedi modelli.
4. Seleziona il nome del modello di recensione da modificare.
5. Nella sezione Tag della scheda Panoramica, scegli Gestisci tag.
6. Aggiungi o elimina i tag secondo necessità.
   - Per aggiungere un tag, scegli Aggiungi nuovo tag e compila i campi Chiave e Valore.
   - Per rimuovere un tag, scegliere Remove (Rimuovi).
7. Ripeti questa procedura per ogni tag che desideri aggiungere, modificare o eliminare. Scegliere Save (Salva) per salvare le modifiche.

Lavorare con i tag utilizzando l'API

Utilizza le seguenti operazioni AWS WA Tool API per aggiungere, aggiornare, elencare ed eliminare i tag delle tue risorse.

Supporto del tagging per le risorse AWS WA Tool

Processo	Operazione API
Aggiungere sovrascrivere uno o più tag.	TagResource
Eliminare uno o più tag.	UntagResource
Elenca i tag associati a una risorsa.	ListTagsForResource

Alcune operazioni per la creazione di risorse ti consentono di specificare tag quando crei le risorse. Le seguenti operazioni supportano il tagging in fase di creazione.

Processo	Operazione API
Crea un carico di lavoro	CreateWorkload
Importa una nuova lente	ImportLens
Per creare un profilo	CreateProfile
Crea un modello di recensione	CreateReviewTemplate

Registrazione delle chiamate API AWS WA Tool con AWS CloudTrail

AWS Well-Architected Tool è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in AWS WA Tool. CloudTrail acquisisce tutte le chiamate API AWS WA Tool come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS WA Tool e le chiamate di codice alle operazioni delle API AWS WA Tool. Se si crea un trail, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per AWS WA Tool. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad AWS WA Tool, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, vedi la Guida per l'utente di AWS CloudTrail.

Informazioni su AWS WA Tool in CloudTrail

CloudTrail è abilitato sul tuo Account AWSal momento della sua creazione. Quando si verifica un'attività su AWS WA Tool, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS WA Tool, crea un trail. Un percorso consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

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

Tutte le operazioni AWS WA Tool vengono registrate da CloudTrail e sono documentate in Operazioni definite da AWS Well-Architected Tool. Ad esempio, le chiamate alle operazioni `CreateWorkload`, `DeleteWorkload` e `CreateWorkloadShare` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- 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, vedi Elemento userIdentity di CloudTrail.

Comprensione delle voci dei file di log di AWS WA Tool

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `CreateWorkload`.

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
         "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
         "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "recipientAccountId": "444455556666"
}
```

EventBridge

AWS Well-Architected Tool invia eventi ad Amazon EventBridge quando vengono intraprese operazioni su risorse Well-Architected. Puoi utilizzare EventBridge e questi eventi per scrivere regole che eseguono operazioni, ad esempio la notifica, quando si verifica una modifica di una risorsa. Per ulteriori informazioni, consulta Che cos'è Amazon EventBridge?.

> **Note**
>
> Gli eventi vengono distribuiti sulla base del miglior tentativo.

Le seguenti operazioni generano eventi EventBridge:

- Correlato al carico di lavoro
  - Creazione o eliminazione di un carico di lavoro
  - Creazione di una milestone
  - Aggiornamento delle proprietà di un carico di lavoro
  - Condivisione o annullamento della condivisione di un carico di lavoro
  - Aggiornamento dello stato di un invito alla condivisione
  - Aggiunta e rimozione di tag
  - Aggiornamento di una risposta
  - Aggiornamento delle note di revisione
  - Aggiunta o rimozione di un obiettivo da un carico di lavoro
- Correlato agli obiettivi
  - Importazione o esportazione di un obiettivo personalizzato
  - Pubblicazione di un obiettivo personalizzato
  - Eliminazione di un obiettivo personalizzato
  - Condivisione o annullamento di una condivisione di un obiettivo personalizzato
  - Aggiornamento dello stato di un invito alla condivisione
  - Aggiunta o rimozione di un obiettivo da un carico di lavoro

Eventi di AWS WA Tool di esempio

Questa sezione include eventi di AWS Well-Architected Tool di esempio.

Aggiornamento di una risposta in un carico di lavoro


```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
     "eventVersion":"1.08",
     "userIdentity":{
        "type":"AssumedRole",
        "principalId":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "arn":"arn:aws:iam::123456789012:role/Admin",
              "accountId":"123456789012",
              "userName":"Admin"
           },
           "webIdFederationData":{},
           "attributes":{
              "creationDate":"2022-02-17T07:21:54Z",
              "mfaAuthenticated":"false"
           }
        }
     },
     "eventTime":"2022-02-17T08:01:25Z",
     "eventSource":"wellarchitected.amazonaws.com",
     "eventName":"UpdateAnswer",
     "awsRegion":"us-west-2",
```

```
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "Status":"Acknowledged",
         "SelectedChoices":"***",
         "ChoiceUpdates":"***",
         "QuestionId":"priorities",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0",
         "IsApplicable":true,
         "LensAlias":"wellarchitected",
         "Reason":"NONE",
         "Notes":"***"
      },
      "responseElements":{
         "Answer":"***",
         "LensAlias":"wellarchitected",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0"
      },
      "requestID":"7bae1153-26a8-4dc0-9307-68b17b107619",
      "eventID":"8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

Pubblicazione di un obiettivo personalizzato

```
{
   "version":"0",
   "id":"4054a34b-60a9-53c1-3146-c1a384dba41b",
   "detail-type":"AWS API Call via CloudTrail",
   "source":"aws.wellarchitected",
   "account":"123456789012",
   "time":"2022-02-17T08:58:34Z",
   "region":"us-west-2",
   "resources":[],
```

```
   "detail":{
      "eventVersion":"1.08",
      "userIdentity":{
         "type":"AssumedRole",
         "principalId":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "arn":"arn:aws:iam::123456789012:role/Admin",
               "accountId":"123456789012",
               "userName":"Admin"
            },
            "webIdFederationData":{},
            "attributes":{
               "creationDate":"2022-02-17T07:21:54Z",
               "mfaAuthenticated":"false"
            }
         }
      },
      "eventTime":"2022-02-17T08:58:34Z",
      "eventSource":"wellarchitected.amazonaws.com",
      "eventName":"CreateLensVersion",
      "awsRegion":"us-west-2",
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "IsMajorVersion":true,
         "LensVersion":"***",
         "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
         "LensAlias":"***"
      },
      "responseElements":{
         "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
         "LensVersion":"***"
      },
      "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
      "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",
```

```
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

Cronologia dei documenti

La tabella seguente riporta la documentazione relativa a questa versione della AWS Well-Architected Tool.

- Versione API: ultima
- Ultimo aggiornamento della documentazione: 17 aprile 2025

Modifica	Descrizione	Data
Nuovo obiettivo	In questa versione è stato aggiunto un nuovo approfond imento al Catalogo Lens.	17 aprile 2025
Obiettivi nuovi e aggiornati	In questa versione è stato aggiunto un nuovo approfond imento al Catalogo Lens ed è stato aggiornato un altro approfondimento.	27 giugno 2024
Jira	In questa versione è stato aggiunto AWS Well-Arch itected Tool Connector for Jira.	16 aprile 2024
Nuovi obiettivi	In questa versione sono stati aggiunti nuovi approfondimenti al Catalogo Lens.	26 marzo 2024
Funzionalità aggiornate	In questa versione è stata aggiunta la funzionalità Catalogo Lens ad AWS WA Tool.	26 novembre 2023
Funzionalità aggiornate	In questa versione è stata aggiunta la funzionalità Modelli di revisione ad AWS WA Tool.	3 ottobre 2023

Policy gestita WellArchitectedConsoleReadOnlyAccess aggiornata	È stato aggiunto `"wellarchitected:ExportLens"` a `WellArchitectedConsoleReadOnlyAccess` .	22 giugno 2023
Funzionalità aggiornate	In questa versione è stata aggiunta la funzionalità Profili ad AWS WA Tool.	13 giugno 2023
Funzionalità aggiornate	In questa versione è stata migliorata l'integrazione di AWS Trusted Advisor e AWS Service Catalog AppRegistry ed è stato aggiunto `AWSWellArchitectedDiscoveryServiceRolePolicy` alle policy gestite AWS.	3 maggio 2023
Aggiornamento dei contenuti	È stata aggiornata la pagina Dashboard per includere informazioni dettagliate sui piani di rischio e miglioramento. È stata inoltre aggiunta la possibilità di creare un report sul carico di lavoro consolidato.	30 marzo 2023
Aggiornamento dei contenuti	È stato corretto il nome della policy WellArchitectedConsoleReadOnlyAccess.	19 gennaio 2023

Guida IAM per AWS WA Tool aggiornata	Guida aggiornata per l'allinea mento alle best practice IAM. Per ulteriori informazioni, consulta la sezione Best practice per la sicurezza in IAM	4 gennaio 2023
Funzionalità aggiornate	In questa versione è stato rimosso l'approfondimento FTR dallo strumento.	14 dicembre 2022
Funzionalità aggiornate	In questa versione è stata aggiunta l'integrazione di AWS Trusted Advisor e AWS Service Catalog AppRegistry.	7 novembre 2022
Aggiornamento dei contenuti	È stato corretto un problema nell'esempio JSON dell'obie ttivo personalizzato per `choices`.	29 settembre 2022
Aggiornamento dei contenuti	È stata aggiornata la sezione `choices` della specifica JSON dell'obiettivo personalizzato.	2 agosto 2022
Funzionalità aggiornate	In questa versione vengono aggiunti il tracciamento delle modifiche per le policy gestite da AWS e una nuova azione per concedere l'autorizzazione `ListAWSServiceAcce ssForOrganization` a `AWSWellArchitected OrganizationsServi ceRolePolicy` .	22 luglio 2022

Condivisione dell'organizzazione aggiunta	In questa versione è stata aggiunta la possibilità di condividere carichi di lavoro e obiettivi personalizzati con l'organizzazione e le unità organizzative (UO).	30 giugno 2022
Funzionalità aggiornate	In questa versione è stata aggiunta la possibilità di specificare ulteriori risorse per le scelte in un approfondimento personalizzato, di visualizzare in anteprima un approfondimento personalizzato prima di pubblicarlo e di aggiungere tag agli approfondimenti personalizzati.	21 giugno 2022
Funzionalità aggiornate	In questa versione è stata aggiunta la possibilità di accedere alla community AWS Well-Architected su AWS re:POST.	31 maggio 2022
Funzionalità aggiornate	In questa versione è stato aggiunto il pilastro della sostenibilità e altri aggiornamenti minori al Tutorial.	31 marzo 2022
Supporto EventBridge aggiunto	AWS WA Tool ora invia un evento ad Amazon EventBridge quando si verificano modifiche a una risorsa Well-Architected.	3 marzo 2022

Funzionalità aggiornate	Ora è possibile contrassegnare le singole best practice come non applicabili.	14 luglio 2021
Tagging delle risorse disponibile	In questa versione è stata aggiunta la possibilità di applicare tag ai carichi di lavoro.	3 marzo 2021
API ora disponibile	Questa versione aggiunge l'API AWS WA Tool. Aggiunte le informazioni sulla registrazione di AWS CloudTrail.	16 dicembre 2020
Funzionalità aggiornate	In questa versione sono stati aggiunti gli approfondimenti FTR e SaaS allo strumento.	3 dicembre 2020
Protezione dei dati aggiornata	Informazioni aggiornate sulla protezione dei dati.	5 novembre 2020
Aggiornamento dei contenuti	È stato chiarito che dopo aver aggiornato un carico di lavoro per utilizzare un nuovo obiettivo non è possibile tornare alla versione precedente.	8 luglio 2020
Aggiornamento dei contenuti	È stata chiarita la condivisione nelle Regioni AWS introdotta dopo il 20 marzo 2019.	24 giugno 2020

Funzionalità aggiornate	L'accesso a una condivisione del carico di lavoro viene rimosso immediatamente quando viene rifiutato un invito alla condivisione del carico di lavoro. L'accesso condiviso viene concesso quando la condivisione viene accettata.	17 giugno 2020
Aggiornamento dei contenuti	Aggiunte definizioni per problemi ad alto rischio (HRIS) e problemi a rischio medio (MRI).	12 giugno 2020
Aggiornamento dei contenuti	È stata aggiunta la sezione su come AWS utilizza i tuoi dati.	21 maggio 2020
Funzionalità aggiornate	Questa versione aggiunge un proprietario revisione al carico di lavoro.	1 Aprile 2020
Funzionalità aggiornate	Questa versione aggiunge un collegamento di diagramma architettonico al carico di lavoro.	10 marzo 2020
Aggiornamento dei contenuti	È stato chiarito che le condivisioni dei carichi di lavoro sono specifiche della Regione AWS.	10 gennaio 2020
Funzionalità aggiornate	Questa versione aggiunge la condivisione dei carichi di lavoro.	9 gennaio 2020
Aggiornamento dei contenuti	Sezione Sicurezza aggiornata con le ultime linee guida.	6 dicembre 2019

Funzionalità aggiornate	Questa versione rende i campi relativi al settore facoltativi durante la definizione di un carico di lavoro.	19 agosto 2019
Funzionalità aggiornate	Questa release aggiunge piani di miglioramento al report dei carichi di lavoro.	29 luglio 2019
Funzionalità aggiornate	La release aggiunge l'operazione DeleteWorkload alla policy.	18 luglio 2019
Aggiornamento dei contenuti	Il contenuto di questa guida è stato aggiornato con piccole correzioni.	19 giugno 2019
Aggiornamento dei contenuti	Il contenuto di questa guida è stato aggiornato con piccole correzioni.	30 maggio 2019
Funzionalità aggiornate	Questa release supporta l'upgrade della versione del framework utilizzato per la revisione di un carico di lavoro.	1 maggio 2019
Funzionalità aggiornate	In questa versione è stata aggiunta la possibilità di specificare regioni non AWS durante la definizione di un carico di lavoro.	14 febbraio 2019
Disponibilità generale di AWS Well-Architected Tool	Questa versione introduce il AWS Well-Architected Tool.	29 novembre 2018

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.