Guida per l'utente

AWS Well-Architected Tool

AWS Well-Architected Tool: Guida per l'utente

Table of Contents

..... vii
Cos'è AWS Well-Architected Tool? 1
Il AWS Well-Architected Framework 2
Definizioni 2
Nozioni di base 4
Fornire l'accesso a AWS WA Tool 4
Attivazione delle integrazioni 5
Attivazione AppRegistry 6
Attivazione Trusted Advisor 6
Definizione di un carico di lavoro 14
Documentazione di un carico di lavoro 17
Rivedi la pagina del carico di lavoro 18
Trusted Advisor controlli 20
Salvare una pietra miliare 22
Tutorial 23
Fase 1: Definire un carico di lavoro 23
Fase 2: Documentare lo stato del carico di lavoro 24
Fase 3: Rivedere il piano di miglioramento 28
Fase 4: apportare miglioramenti e misurare i progressi 30
Carichi di lavoro 32
Problemi ad alto rischio (HRIS) e problemi a rischio medio (MRI) 33
Definizione di un carico di lavoro 34
Visualizzazione di un carico di lavoro 35
Modifica di un carico di lavoro 35
Condivisione di un carico di lavoro 36
Considerazioni sulla condivisione 38
Eliminazione dell'accesso condiviso 39
Modifica dell'accesso condiviso 40
Accettazione e rifiuto degli inviti al carico di lavoro 41
Eliminazione di un carico di lavoro 42
Generazione di un rapporto sul carico di lavoro 42
Dettagli del carico di lavoro 43
Scheda Overview (Panoramica) 43
Scheda Milestones 44

Scheda Proprietà ... 44
Scheda Condivisioni ... 45
Approfondimenti ... 47
Aggiungere un obiettivo ... 47
Rimuovere una lente ... 48
Dettagli della lente ... 48
Scheda Overview (Panoramica) ... 48
Scheda Piano di miglioramento ... 49
Scheda Condivisioni ... 49
Obiettivi personalizzati ... 49
Visualizzazione di obiettivi personalizzati ... 50
Creazione di una lente ... 51
Visualizzazione in anteprima di un obiettivo ... 52
Pubblicazione di un obiettivo ... 53
Pubblicazione di un aggiornamento dell'obiettivo ... 53
Condivisione di un obiettivo ... 55
Aggiungere tag a un obiettivo ... 56
Eliminazione di un obiettivo ... 57
Specifiche del formato delle lenti ... 57
Aggiornamenti dell'obiettivo ... 64
Selezione di un aggiornamento dell'obiettivo ... 65
Aggiornamento di un obiettivo ... 66
Catalogo Lens ... 67
Modelli di revisione ... 70
Creazione di un modello di recensione ... 70
Modifica di un modello di recensione ... 71
Condivisione di un modello di recensione ... 72
Definizione di un carico di lavoro da un modello ... 73
Eliminazione di un modello di recensione ... 74
Profili ... 76
Creazione di un profilo ... 76
Modifica di un profilo ... 77
Condivisione di un profilo ... 77
Aggiungere un profilo a un carico di lavoro ... 78
Rimuovere un profilo da un carico di lavoro ... 78
Eliminazione di un profilo ... 79

Jira 81
Configurazione del connettore 82
Configurazione del connettore 83
Sincronizzazione di un carico di lavoro 85
Disinstallazione del connettore 86
Milestone 88
Salvataggio di un milestone 88
Visualizzazione di milestone 88
Generazione di un report milestone 89
Condividi gli inviti 90
Accettazione di un invito alla condivisione 91
Rifiutare un invito alla condivisione 92
Notifiche 93
Notifiche sull'obiettivo 93
Notifiche sul profilo 93
Dashboard (Pannello di controllo) 95
Riepilogo 95
Wellate Framework, problemi del Wellato Framework Framework, ... 95
Problemi del Well-Well-Framework Framework di Well-Well- 96
I problemi del Well-Framework Framework di Well-Well-Framework 97
Sicurezza 99
Protezione dei dati 100
Crittografia dei dati a riposo 100
Crittografia in transito 101
Come AWS utilizza i tuoi dati 101
Identity and Access Management 101
Destinatari 102
Autenticazione con identità 103
Gestione dell'accesso con policy 106
Come AWS Well-Architected Tool funziona con IAM 109
Esempi di policy basate su identità 117
AWS politiche gestite 121
Risoluzione dei problemi 128
Risposta all'incidenza 128
Convalida della conformità 128
Resilienza 130

Sicurezza dell'infrastruttura 130
Analisi della configurazione e delle vulnerabilità 131
Prevenzione del confused deputy tra servizi 131
Condivisione delle tue risorse 133
Attiva la condivisione delle risorse all'interno AWS Organizations 133
Tagging delle risorse 136
Nozioni di base sui tag 136
Tagging delle risorse 137
Limitazioni applicate ai tag 138
Utilizzo di tag tramite la console 138
Aggiunta di tag a una singola risorsa alla creazione 138
Aggiunta ed eliminazione di tag in una singola risorsa 138
Lavorare con i tag utilizzando l'API 140
Registrazione 142
AWS WA Toolinformazioni in CloudTrail 142
Comprensione delle voci dei file di log di AWS WA Tool 143
EventBridge 146
Eventi di esempioAWS WA Tool 147
Cronologia dei documenti 151
Glossario per AWS 158

Puoi utilizzare AWS Well-Architected Tool Connector for Jira per collegare il tuo account Jira e sincronizzare gli elementi di AWS Well-Architected Tool miglioramento tra i tuoi carichi di lavoro e i progetti Jira.

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

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 Toolti aiuta durante l'intero ciclo di vita del prodotto attraverso:

- 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 revisione di Well-Architected.

Questo servizio è destinato a coloro che sono coinvolti nello sviluppo tecnico dei prodotti, come i Chief Technology Officer (CTO), gli architetti, gli sviluppatori e i membri del team operativo. AWSi 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

- Il AWS Well-Architected Framework
- Definizioni

Il AWS Well-Architected Framework

Il AWSWell-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. Il canone 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 AWSWell-Architected.

Definizioni

In AWS WA Tool e il 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 pietre miliari 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 daAWS, puoi anche creare e utilizzare obiettivi personalizzati o utilizzare obiettivi che sono stati condivisi con te.

- I problemi ad alto rischio (HRI) sono scelte architettoniche e operative AWS che, secondo noi, potrebbero avere un impatto negativo significativo su un'azienda. Questi HRI possono influenzare le operazioni organizzative, le risorse e gli individui.
- I problemi a rischio medio (MRI) sono scelte architettoniche e operative che, secondo quanto AWS rilevato, potrebbero avere un impatto negativo sulle attività aziendali, ma in misura minore rispetto agli HRI.

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

Guida introduttiva con AWS Well-Architected Tool

Questa sezione descrive come iniziare AWS WA Tool.

Argomenti

- Fornire a utenti, gruppi o ruoli l'accesso a AWS WA Tool
- Attivazione del supporto per altri servizi AWS
- Definizione di un carico di lavoro
- Documentazione di un carico di lavoro
- Salvare una pietra miliare

Fornire a utenti, gruppi o ruoli l'accesso a AWS WA Tool

In questa fase, concedi l'accesso a AWS WA Tool.

Fornisci l'accesso a AWS WA Tool

1. Per fornire l'accesso, aggiungi autorizzazioni ai tuoi 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 Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

   - Utenti IAM:

     - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di 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 di IAM.

2. Per concedere il controllo completo, applica la politica WellArchitectedConsoleFullAccessgestita al set di autorizzazioni o al ruolo.

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

Per ulteriori informazioni su queste politiche, vedereAWS politiche gestite per AWS Well-Architected Tool.

Attivazione del supporto per altri servizi AWS

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

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

Per attivare il supporto per altri servizi con cui è AWS WA Tool possibile interagire, accedi a Impostazioni.

1. Per raccogliere informazioni da AWS Organizations, attiva l' AWS Organizations assistenza di Activate.
2. Attiva il supporto di Activate Discovery per raccogliere informazioni da altri AWS servizi e risorse.
3. Seleziona Visualizza le autorizzazioni dei ruoli per visualizzare le autorizzazioni dei ruoli collegati ai servizi o le politiche sulle relazioni di fiducia.
4. Seleziona Salva impostazioni.

Attivazione AppRegistry per un carico di lavoro

L'utilizzo AppRegistry è facoltativo e i clienti AWS Business and Enterprise Support possono attivarlo in base al carico di lavoro.

Ogni volta che il supporto Discovery è attivato e AppRegistry associato a un carico di lavoro nuovo o esistente, AWS WA 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 Discovery è attivato, ogni volta che viene apportata una modifica al carico di lavoro, il gruppo di attributi viene aggiornato.
- Quando il supporto Discovery è disattivato o l'applicazione viene rimossa dal carico di lavoro, le informazioni sul carico di lavoro vengono rimosse da. AWS Service Catalog

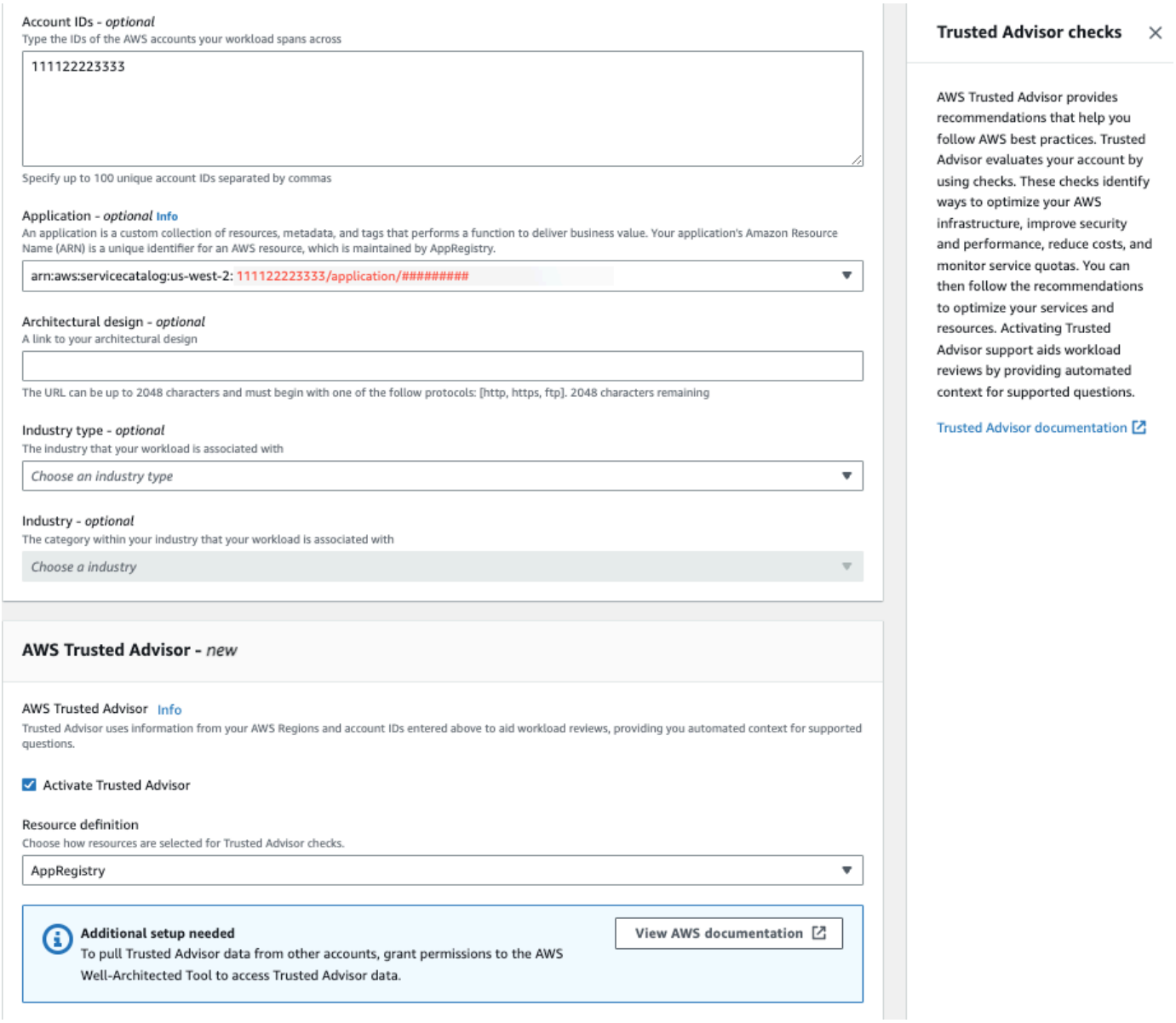
Se desideri che un' AppRegistry applicazione gestisca i dati recuperati Trusted Advisor, imposta la definizione delle risorse del carico di lavoro su o Tutti. AppRegistry Crea ruoli per tutti gli account che possiedono le risorse della tua applicazione seguendo le linee guida contenute in. the section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

Attivazione AWS Trusted Advisor per un carico di lavoro

L'integrazione con AWS Trusted Advisor è facoltativa e può essere attivata in base al carico di lavoro per i clienti AWS Business ed Enterprise Support. L'integrazione Trusted Advisor non prevede costi AWS WA Tool, ma per i dettagli Trusted Advisor sui prezzi, consulta AWS Support Plans.

Per attivare Trusted Advisor per un carico di lavoro

1. Per attivarlo Trusted Advisor, i proprietari del carico di lavoro possono AWS WA Tool aggiornare un carico di lavoro esistente o creare un nuovo carico di lavoro scegliendo Definisci carico di lavoro.
2. Immettete un ID account utilizzato da Trusted Advisor nel campo Account ID, selezionate l'ARN dell'applicazione nel campo Applicazione o entrambi per attivarli. Trusted Advisor
3. Nella AWS Trusted Advisorsezione, seleziona Attiva Trusted Advisor.



4. Una notifica che indica che il ruolo di servizio IAM verrà creato viene visualizzata la prima volta che Trusted Advisor viene attivato 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 fiducia create automaticamente da JSON per te in IAM. Dopo la creazione del ruolo, per l'attivazione successiva dei carichi di lavoro Trusted Advisor, viene mostrata solo la notifica relativa alla configurazione aggiuntiva necessaria.
5. Nel menu a discesa Definizione della risorsa, puoi selezionare Metadati del carico di lavoro o Tutti. AppRegistry La selezione della definizione della risorsa definisce da cosa AWS WA Tool recuperare i dati 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 dell'account e specificato nel carico di lavoro. Regioni AWS

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

Tutto: il carico di lavoro è definito sia dai metadati del carico di lavoro che dalle risorse. AppRegistry

6. Seleziona Successivo.
7. Applica il AWS Well-Architected Framework al tuo carico di lavoro e scegli Define workload. Trusted Advisor i controlli sono collegati solo al AWS Well-Architected Framework e non ad altri obiettivi.

AWS WA Tool Periodicamente ottiene dati Trusted Advisor utilizzando i ruoli creati in IAM. Il ruolo IAM viene creato automaticamente per il proprietario del carico di lavoro. Tuttavia, per visualizzare Trusted Advisor le informazioni, i proprietari di qualsiasi account associato al carico di lavoro devono accedere a IAM e creare un ruolo, vedi ??? per maggiori dettagli. Se questo ruolo non esiste, non AWS WA Tool può ottenere Trusted Advisor informazioni per quell'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 IAM User Guide.

Attivazione Trusted Advisor per un carico di lavoro in IAM

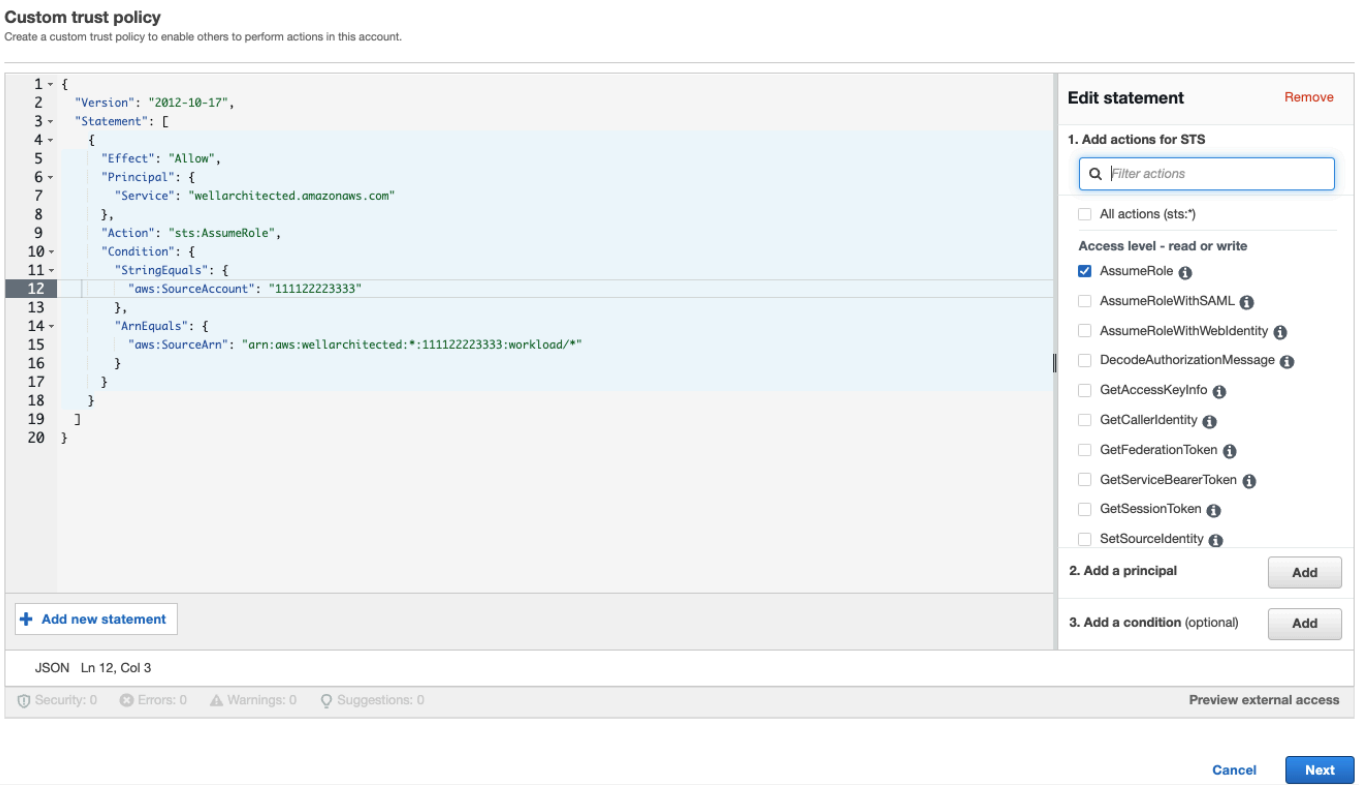
> **Note**
>
> I proprietari dei carichi di lavoro devono attivare il supporto Discovery per il proprio account prima di creare un carico di lavoro. Trusted Advisor La scelta di attivare il supporto Discovery crea il ruolo richiesto per il proprietario del carico di lavoro. Utilizza la procedura seguente per tutti gli altri account associati.

I proprietari degli account associati per i carichi di lavoro attivati Trusted Advisor devono creare un ruolo in IAM in cui visualizzare Trusted Advisor le informazioni. AWS WA Tool

Creare un ruolo in IAM AWS WA Tool da cui ottenere informazioni Trusted Advisor

1. Accedi a AWS Management Console e apri la console IAM all'indirizzohttps://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegli Ruoli, quindi scegli Crea ruolo.
3. In Tipo di entità affidabile, scegli Politica di fiducia personalizzata.
4. Copia e incolla la seguente politica di fiducia personalizzata nel campo JSON della console IAM, come mostrato nell'immagine seguente. *WORKLOAD_OWNER_ACCOUNT_ID*Sostituiscila con l'ID dell'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 `aws:sourceArn` blocco delle condizioni della precedente politica di fiducia personalizzata è`"arn:aws:wellarchitected:*:`*WORKLOAD_OWNER_ACCOUNT_ID*`:workload/*"`, che è una condizione generica che indica che questo ruolo può essere utilizzato da AWS WA Tool per tutti i carichi di lavoro del proprietario del carico di lavoro. Tuttavia, l'accesso può essere limitato a un ARN del carico di lavoro specifico o a un set di ARN per carichi di lavoro. Per specificare più ARN, vedi il seguente esempio di policy di fiducia.

```
{
    "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 Criteri di autorizzazione scegli Crea politica da cui concedere AWS WA Tool l'accesso ai dati di lettura. Trusted Advisor Selezionando Crea politica si apre una nuova finestra.

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

6. Copia e incolla la seguente politica di autorizzazione nel campo JSON. Nell'**`Resource`**ARN, sostituiscilo ***`YOUR_ACCOUNT_ID`***con il tuo ID account, specifica la regione o un asterisco (**`*`**) e scegli Avanti: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 la definizione della risorsa è impostata su AppRegistryo Tutti, tutti gli account che possiedono una risorsa nell' AppRegistry applicazione allegata al carico di lavoro devono aggiungere la seguente autorizzazione alla politica 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. Rivedi la politica, assegnale un nome e seleziona Crea politica.

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

    Dovresti ricevere un messaggio di successo nella parte superiore della pagina che ti avvisa che il ruolo è stato creato.
12. Per visualizzare il ruolo e la politica di autorizzazione associata, nel riquadro di navigazione a sinistra in Gestione degli accessi, scegli Ruoli e cerca il `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* nome. Seleziona il nome del ruolo per verificare che le relazioni tra Autorizzazioni e Trust siano corrette.

Disattivazione per Trusted Advisor un carico di lavoro

Per disattivare Trusted Advisor per un carico di lavoro

Puoi disattivarlo Trusted Advisor per qualsiasi carico di lavoro da AWS WA 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 di un carico di lavoro”

La disattivazione Trusted Advisor da AWS WA Tool non elimina i 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 sono disattivati in AWS WA Tool o interrompere la raccolta di Trusted Advisor dati per il carico AWS WA Tool di lavoro.

Per eliminare i file in IAM **`WellArchitectedRoleForTrustedAdvisor`**

1. Accedi a AWS Management Console e apri la console IAM all'indirizzohttps://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 Eliminazione di un ruolo IAM (console) nella Guida per l'utente IAM.

Definizione di un carico di lavoro

La fase successiva consiste nel definire un carico di lavoro.

Per definire 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. Se è la prima volta che lo utilizzi AWS WA Tool, viene visualizzata una pagina che illustra le funzionalità 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 vengono AWS utilizzati i dati del carico di lavoro, scegli Perché sono AWS necessari 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:
   - Produzione: il carico di lavoro viene eseguito in un ambiente di produzione.
   - Preproduzione: il carico di lavoro viene eseguito in un ambiente di preproduzione.
7. Nella sezione Regions (Regioni), scegliere le regioni per il carico di lavoro:

- Regioni AWS— Scegli Regioni AWS dove eseguire il tuo carico di lavoro, uno alla volta.
- Non AWS regioni: inserisci i nomi delle regioni al di fuori di quelle AWS in cui viene eseguito il carico di lavoro. Puoi specificare fino a cinque 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 Account AWS associati al tuo carico di lavoro. È possibile specificare fino a 100 ID account univoci, separati da virgole.

   Se Trusted Advisor è attivato, tutti gli ID di account specificati vengono utilizzati per ottenere dati da Trusted Advisor. Vedi Attivazione AWS Trusted Advisor per un carico di lavoro per concedere AWS WA Tool le autorizzazioni per ottenere Trusted Advisor dati per tuo conto all'interno di IAM.
9. (Facoltativo) Nella casella Applicazione, immettete l'ARN dell'applicazione da associare a questo carico di lavoro. AWS Service Catalog AppRegistry È possibile specificare un solo ARN per carico di lavoro e 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 Trusted Advisorsezione, per attivare i Trusted Advisor controlli del carico di lavoro, seleziona Attiva. Trusted Advisor Potrebbe essere necessaria una configurazione aggiuntiva per gli account associati al carico di lavoro. Vedi the section called “Attivazione Trusted Advisor” per concedere AWS WA Tool le autorizzazioni per raccogliere Trusted Advisor dati per tuo conto. Seleziona tra Metadati del carico di lavoro o Tutto in Definizione della risorsa per definire quali risorse AWS WA Tool utilizzare per eseguire i controlli. AppRegistry Trusted Advisor
14. (Facoltativo) Nella sezione Jira, per attivare le impostazioni di sincronizzazione Jira a livello di carico di lavoro per il carico di lavoro, seleziona Ignora le impostazioni a livello di account. Potrebbe essere necessaria una configurazione aggiuntiva per gli account associati al carico di lavoro. Vedi AWS Well-Architected Tool Connector for Jira per iniziare a configurare e configurare il connettore. Seleziona tra Non sincronizzare il carico di lavoro, Sincronizza il carico di lavoro - Manuale e Sincronizza carico di lavoro - Automatico e, facoltativamente, inserisci una chiave di progetto Jira con cui sincronizzarti.

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

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

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

16. Seleziona 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 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 AWS obiettivi ufficiali, vedi Obiettivi.

    Le lenti possono essere selezionate tra Lenti personalizzate (lenti che hai creato o che sono state condivise con te Account AWS), Lens Catalog (lenti AWS ufficiali disponibili per tutti gli utenti) o entrambi.

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

    > **Dichiarazione di non responsabilità**
    >
    > Accedendo e/o applicando lenti personalizzate create da un altro AWS utente o account, riconosci che le lenti personalizzate create da altri utenti e condivise con te sono Contenuti di terze parti come definito nel Contratto con il AWS cliente.

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

Dopo aver definito un carico di lavoro, è necessario documentarne lo stato.

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 riquadro di navigazione a sinistra contiene un elenco di domande di revisione del carico di lavoro con priorità che puoi utilizzare per velocizzare il processo di revisione del 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, scegli Informazioni e visualizza le informazioni nel riquadro 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 elemento, scegli Informazioni e visualizza le informazioni nel riquadro di aiuto.

   b. (Facoltativo) Se una o più best practice non si applicano al tuo carico di lavoro, scegli Contrassegna le best practice che non si applicano a questo carico di lavoro e selezionale.

Per ogni best practice selezionata, puoi facoltativamente 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.

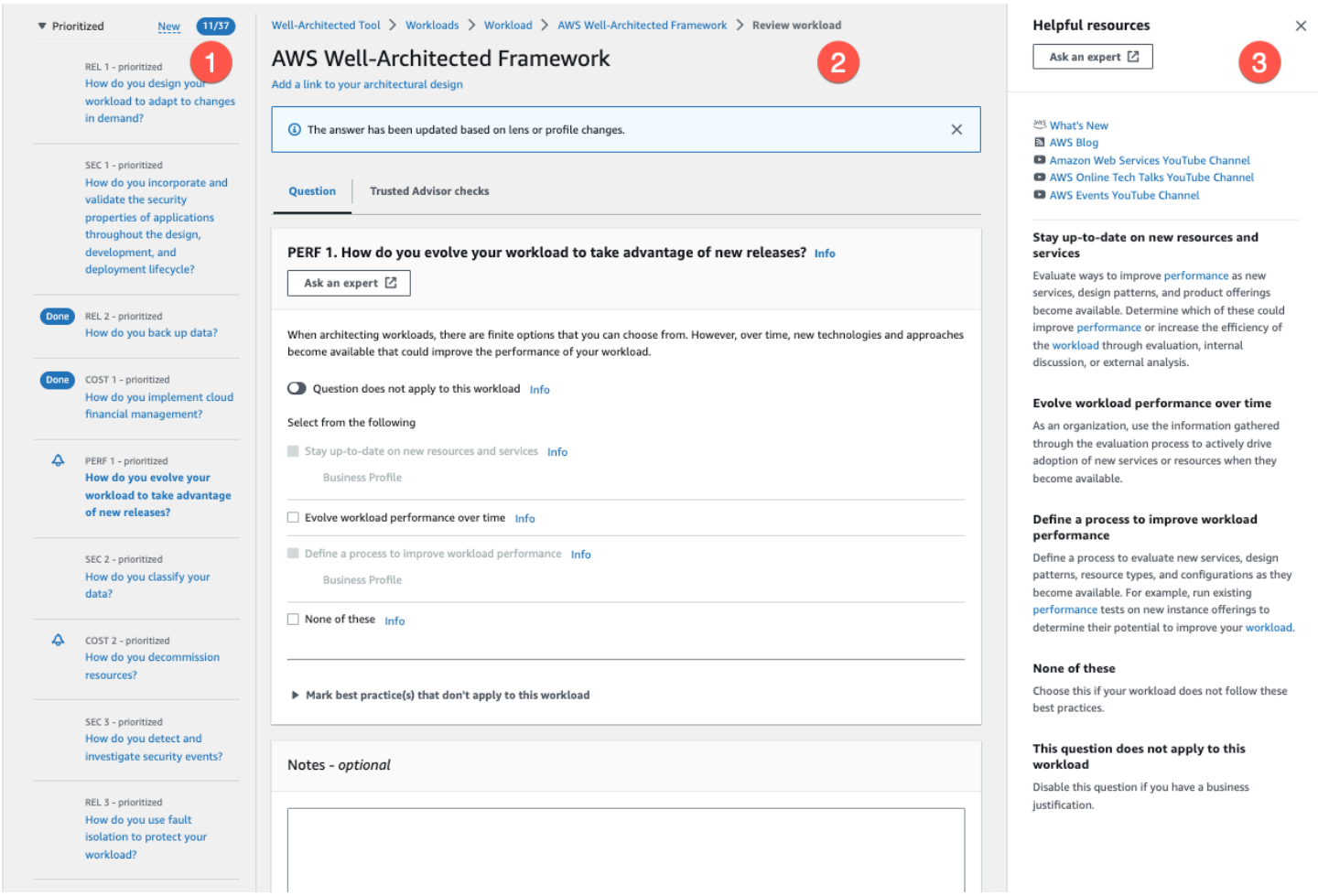
Ripeti questi passaggi per ogni domanda in ogni pilastro.

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

Per tornare alle domande, passare alla pagina dei dettagli del carico di lavoro e scegliere Continue review (Continua la revisione).

Rivedi la pagina del carico di lavoro

La pagina del carico di lavoro di revisione ha tre riquadri.



1. Il riquadro 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, AWS WA Tool utilizza le informazioni del profilo per determinare a quali domande della revisione del carico di lavoro viene data priorità e quali domande non sono applicabili alla tua attività. Nel riquadro di navigazione a sinistra puoi utilizzare le domande con priorità 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 con priorità.
2. Il riquadro centrale mostra 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 di AWS re:POST dedicata a Well-

Architected AWS . AWS re:POST è una community che sostituisce i forum basata su argomenti. question-and-answer 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.

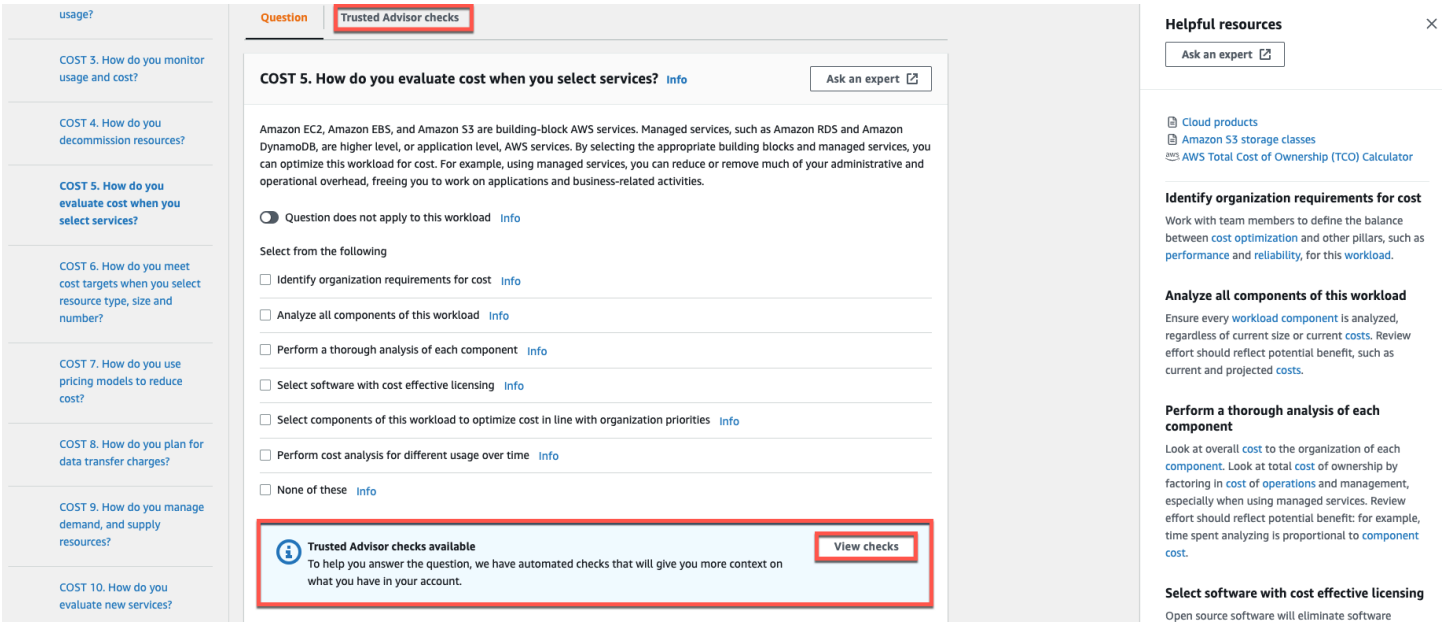
(Facoltativo) Per contrassegnare una o più best practice come non applicabili, scegli Contrassegna le best practice che non si applicano a questo carico di lavoro e selezionale.

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

3. Il riquadro di aiuto destro mostra informazioni aggiuntive e risorse utili. 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

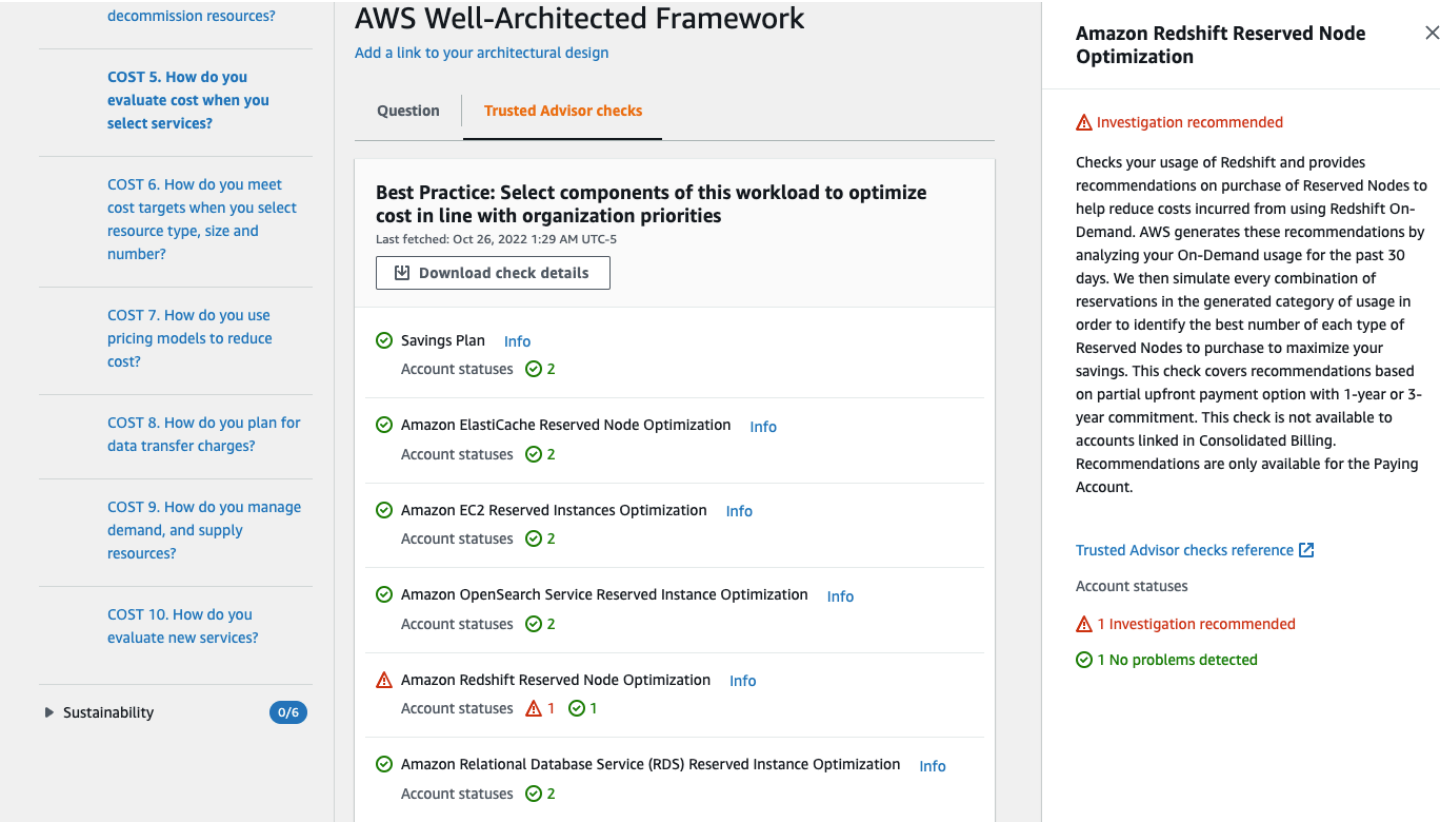
Trusted Advisor controlli

Se Trusted Advisor è attivata per il tuo carico di lavoro, viene visualizzata una scheda Trusted Advisor controlli accanto a Domanda. Se sono disponibili controlli relativi alla migliore pratica, dopo la selezione della domanda viene visualizzata una notifica che indica che sono disponibili Trusted Advisor controlli. Selezionando Visualizza controlli si accede alla scheda Trusted Advisor Controlli.



Nella scheda Trusted Advisor controlli, è possibile visualizzare informazioni più dettagliate sui controlli basati sulle migliori pratiche Trusted Advisor, visualizzare i collegamenti alla Trusted Advisor

documentazione nel riquadro delle risorse di aiuto o Scaricare i dettagli del controllo, che fornisce un rapporto dei Trusted Advisor controlli e degli stati di ciascuna best practice in un file CSV.



Le categorie di assegni di Trusted Advisor sono visualizzate come icone colorate e il numero accanto a ciascuna icona mostra il numero di account con quello stato.

- Azione consigliata (rosso): Trusted Advisor consiglia un'azione per il controllo.
- Indagine consigliata (giallo): Trusted Advisor rileva un possibile problema durante il controllo.
- Nessun problema rilevato (verde): Trusted Advisor non rileva alcun problema durante 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 Trusted Advisor forniti, consulta Visualizza le categorie di controllo nella Guida per l'AWS Support utente.

Selezionando il collegamento Informazioni accanto a ciascun Trusted Advisor controllo vengono visualizzate le informazioni relative al controllo nel riquadro Risorse di aiuto. Per ulteriori informazioni, consulta AWS Trusted Advisor il riferimento di controllo nella Guida AWS Support per l'utente.

Salvare una pietra miliare

È possibile salvare un milestone 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. Selezionare Salva.

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

Per ulteriori informazioni, consulta Milestone.

Tutorial

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: Rivedere 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 "Definizione di un carico di lavoro"

Per definire 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/.

   > **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.

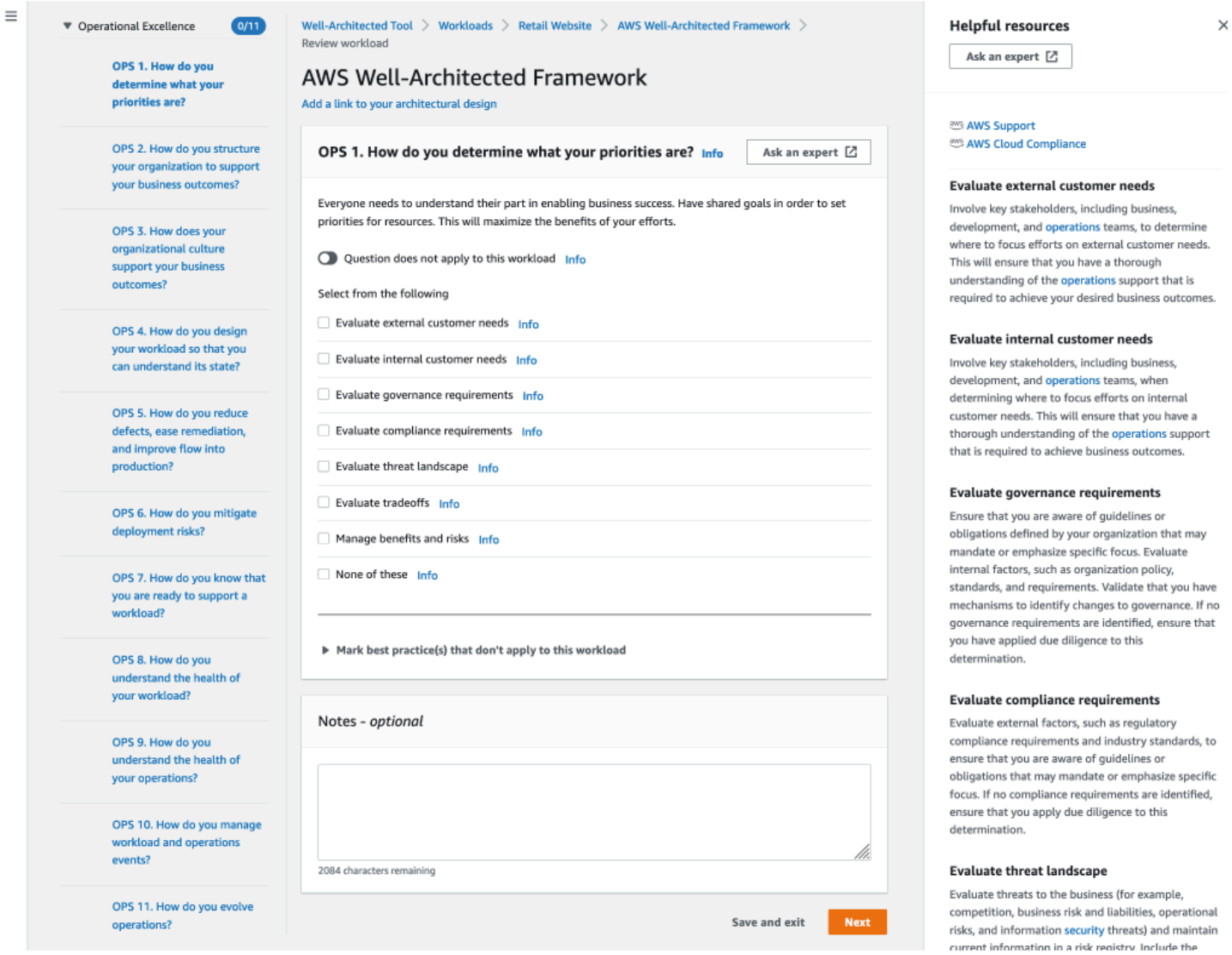
6. Nella casella Ambiente, indica che il carico di lavoro si trova in un ambiente di produzione.
7. Il nostro carico di lavoro viene eseguito su entrambi AWS e presso il nostro data center locale:
    a. Seleziona Regioni AWSe scegli le due regioni del Nord America in cui viene eseguito il carico di lavoro.
    b. Seleziona anche aree non AWS geografiche e inserisci un nome per il data center locale.
8. La casella Account ID è facoltativa. Non associarne nessuno Account AWS a questo carico di lavoro.
9. La casella Applicazione è facoltativa. Non inserire un ARN dell'applicazione 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. Seleziona Successivo.
15. Il passaggio Applica profilo è facoltativo. Non applicare un profilo per questo carico di lavoro. Seleziona 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.

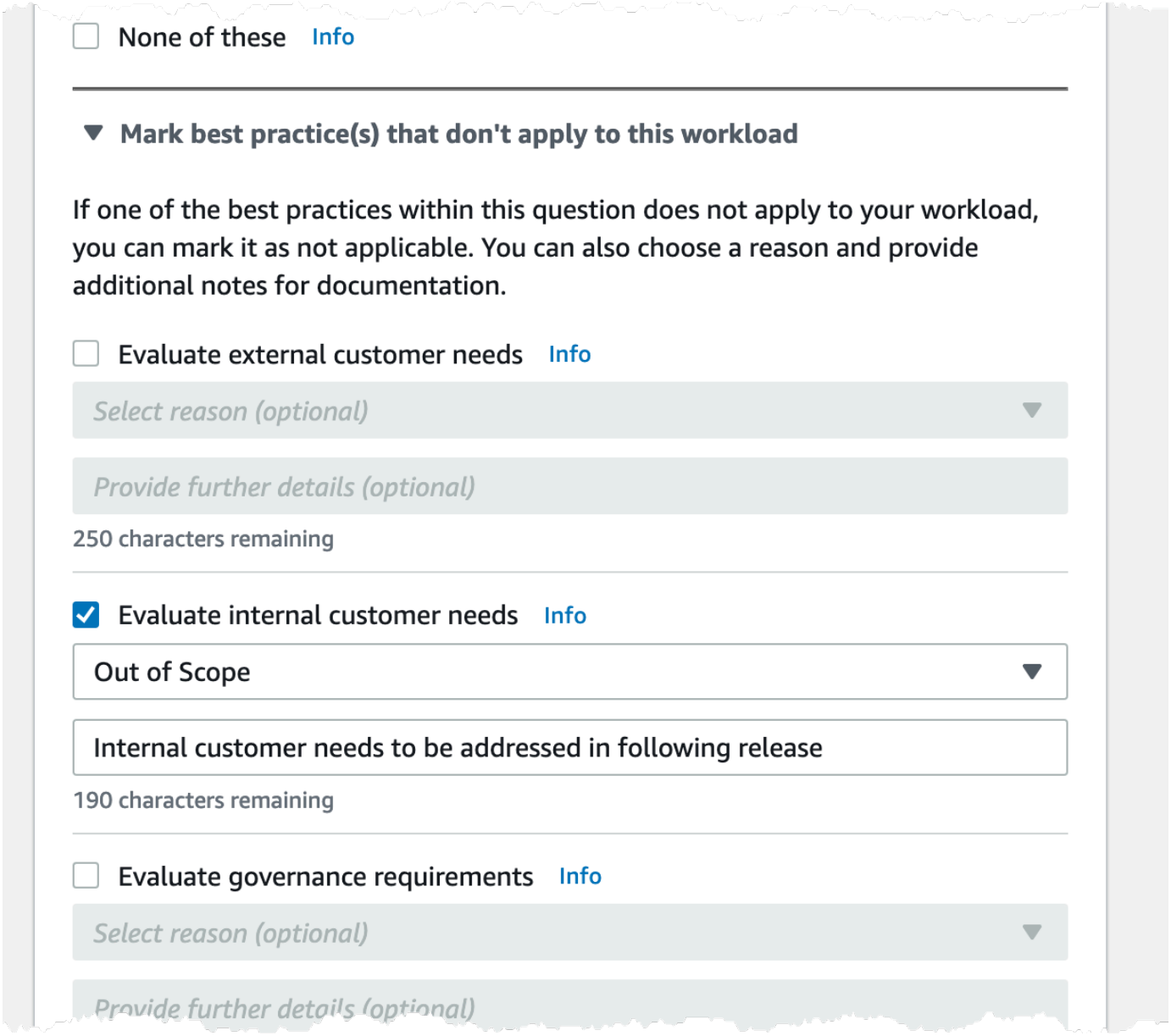
Scegli Chiedi a un esperto per accedere alla community di AWS re:POST dedicata a Well-Architected AWS . In questa community puoi porre domande relative alla progettazione, alla creazione, all'implementazione e al funzionamento dei carichi di lavoro. AWS



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. Selezionare Salva.
4. Per generare un report del carico di lavoro, selezionare l'approfondimento desiderato e scegliere Generate report (Genera report). Viene creato un file PDF. Questo file contiene lo stato del carico di lavoro, il numero di rischi identificati e un elenco di miglioramenti suggeriti.

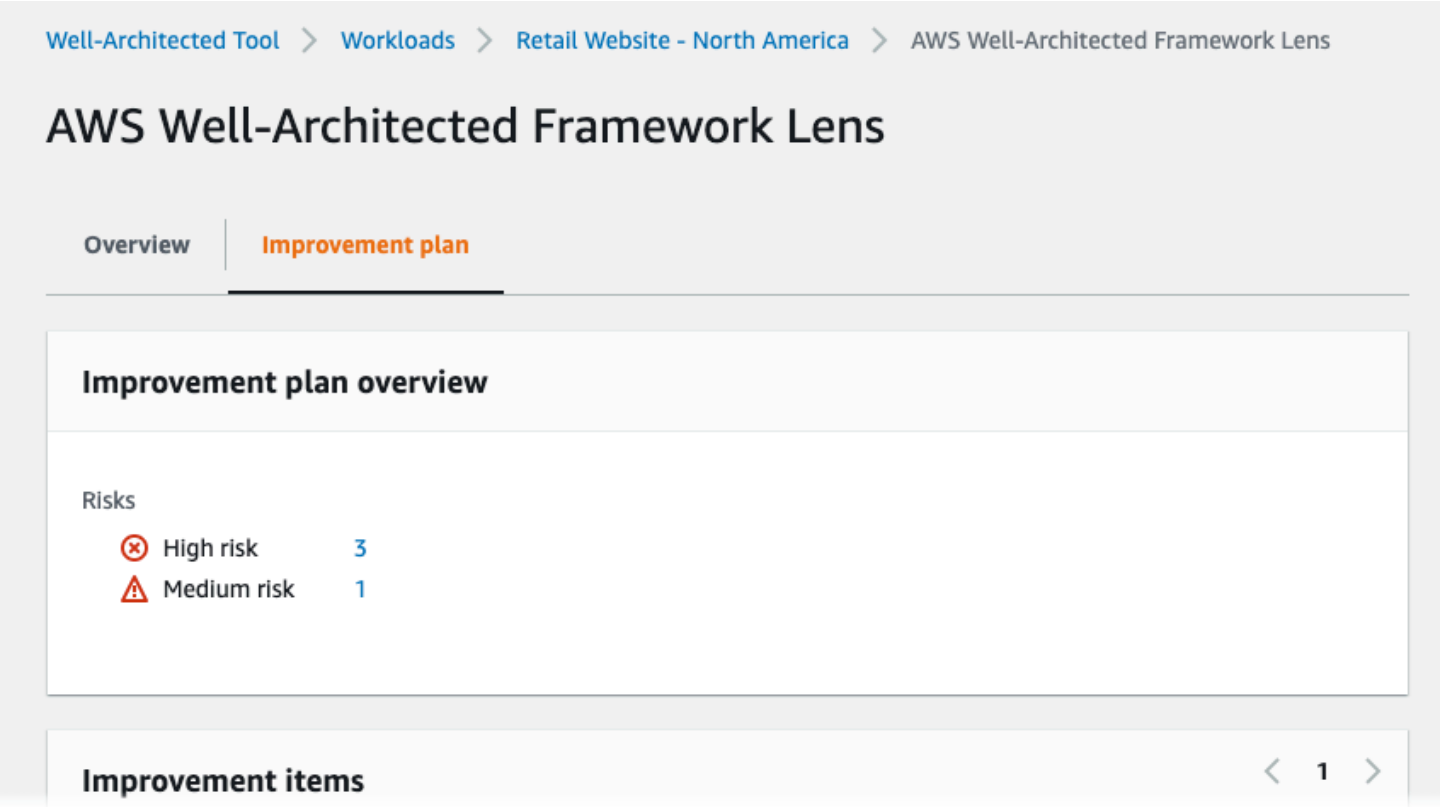
Fase 3: Rivedere il piano di miglioramento

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).

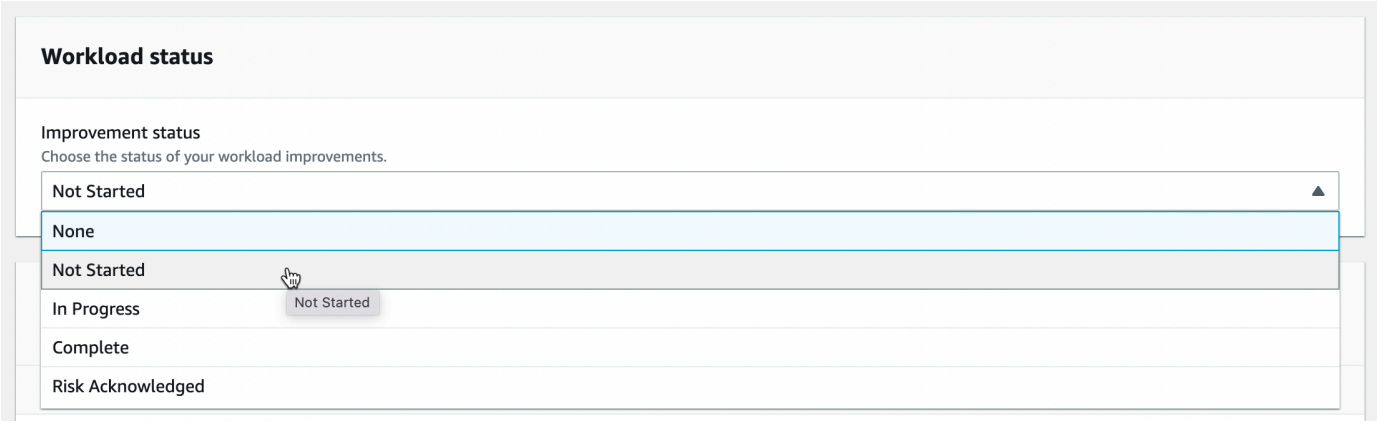
Per questo particolare esempio di carico di lavoro, il AWS Well-Architected Framework Lens ha identificato tre problemi ad alto rischio e uno a rischio medio.



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.

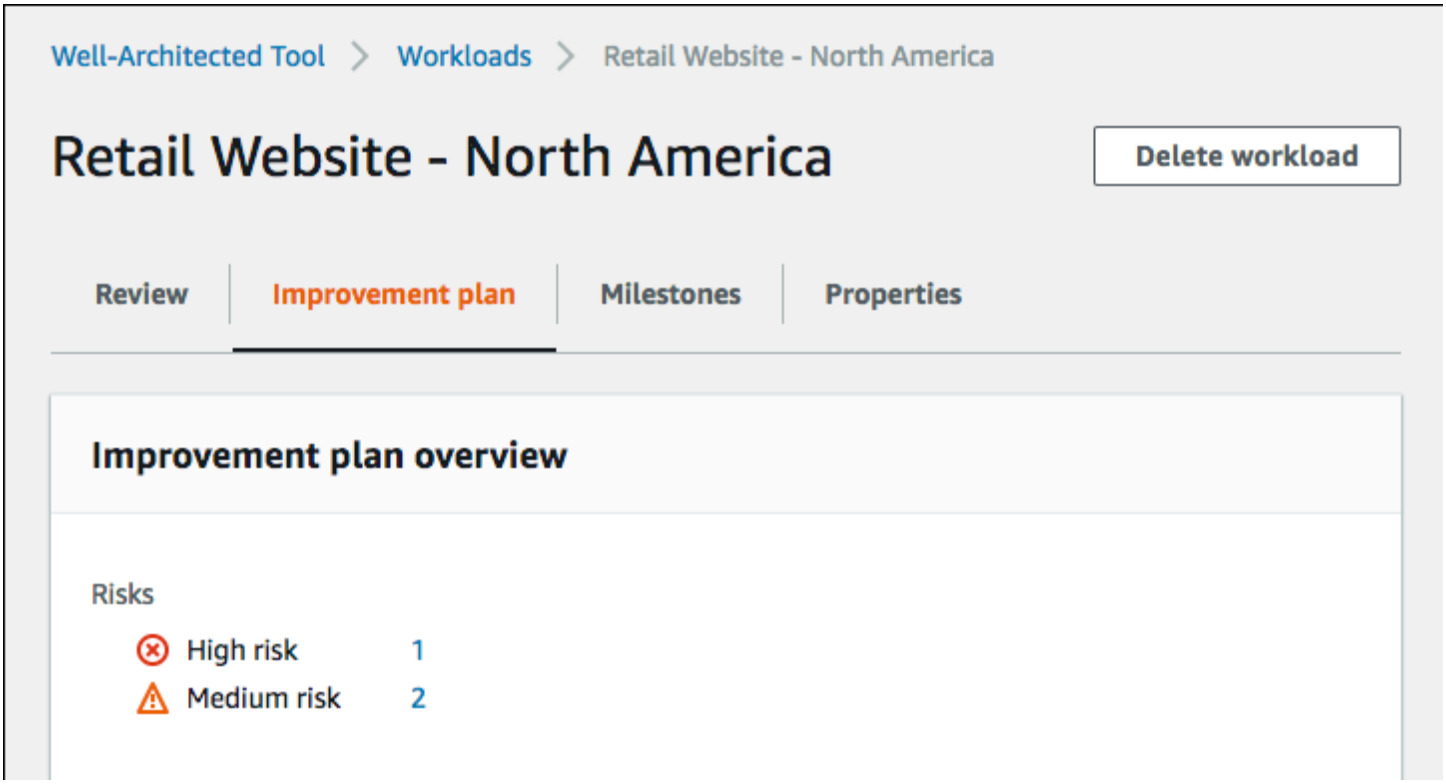
Se al carico di lavoro è associato un profilo, nella sezione Panoramica del piano di miglioramento viene visualizzato un conteggio dei rischi con priorità ed è possibile filtrare l'elenco degli elementi di miglioramento selezionando Assegna priorità per profilo. L'elenco degli elementi di miglioramento 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 una singola Account AWS o essere una raccolta di più risorse che si estendono 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 AWSID 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 a rischio elevato identificati (HRI).

Rischi medi

Numero di problemi a rischio medio identificati (MRI).

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 (OU), 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 (MRI)

I problemi ad alto rischio (HRI) AWS Well-Architected Tool identificati nelle scelte architettoniche e operative che AWS ha rilevato potrebbero avere un impatto negativo significativo su un'azienda. Questi HRI possono influenzare le operazioni organizzative, le risorse e gli individui. Anche i problemi a rischio medio (MRI) potrebbero avere un impatto negativo sulle 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 AWS clienti AWS e 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. AWSsuggerisce ai clienti di documentare questi motivi e il modo in cui influiscono sulle best practice nelle note sul carico di lavoro. Per tutti gli HRI e le risonanze magnetiche identificati, AWS suggerisce ai clienti di implementare

le migliori pratiche 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.

Definizione di un carico di lavoro

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.

Visualizzazione di un carico di lavoro

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 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 di un carico di lavoro

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

Per modificare 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. 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.

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

Condivisione di un carico di lavoro

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

> **Note**
>
> Puoi condividere i carichi di lavoro solo all'interno degli stessi. Regione AWS
> Quando condivide un carico di lavoro con un altroAccount AWS, se il destinatario non dispone dell'`wellarchitected:UpdateShareInvitation`autorizzazione, non può accettare l'invito alla condivisione. the section called "Fornire l'accesso a 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 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'Account AWSID a 12 cifre o l'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 le unità organizzative (OU), è necessario abilitare l'accesso. AWS Organizations

Per condividere un carico di lavoro con l'organizzazione o le unità organizzative

1. Accedi 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 unità organizzative.
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 Dettagli del carico di lavoro.

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

Puoi anche condividere gli obiettivi personalizzati che possiedi con altri utentiAccount AWS, la tua organizzazione e le unità organizzative all'interno della stessa Regione AWS unità. Per i dettagli, fare riferimento aCondivisione di un obiettivo personalizzato.

Considerazioni sulla condivisione

Un carico di lavoro può essere condiviso con un massimo di 20 diversi Account AWS utenti. 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 AWSGlobal Infrastructure.

Puoi condividere un carico di lavoro con singoli utenti in un account o entrambi. Account AWS Quando condividi un carico di lavoro con un utenteAccount 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 (OU), è necessario abilitare l'accesso. AWS Organizations

Se condividi un carico di lavoro sia con un'organizzazione che con una o più unità organizzative, 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. Accedere AWS Management Console e aprire 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).

Eliminazione dell'accesso condiviso

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 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 Delete (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 dell'accesso condiviso

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 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.

Accettazione e rifiuto degli inviti al carico di lavoro

Un invito per 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 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 Dettagli del carico di lavoro relativa al carico di lavoro.

Eliminazione di un carico di lavoro

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 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`.

Generazione di un rapporto sul carico di lavoro

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

Dettagli del carico di lavoro

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

- Scheda Overview (Panoramica)
- Scheda Milestones
- Scheda Proprietà
- Scheda Condivisioni

Scheda Overview (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.

Scheda 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).

Scheda 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.

Scheda 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 Account AWS utente con accesso condiviso al carico di lavoro:

Principale

L'Account AWSID o l'ARN dell'utente con accesso condiviso al carico di lavoro.

Stato

Lo stato dell'invito al carico di lavoro.

- Pending (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 utenteRegione AWS, scegli Crea. Un carico di lavoro può essere condiviso con un massimo di 20 utenti EA diversiAccount 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.

Approfondimenti

Gli approfondimenti offrono un metodo per misurare con coerenza le proprie architetture rispetto alle best practice e individuare le aree di miglioramento. Il AWS Well-Architected Framework Lens 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: obiettivi Lens Catalog e obiettivi personalizzati.

- Lens Catalog: obiettivi ufficiali creati e gestiti da AWS. Il Lens Catalog è disponibile per tutti gli utenti e non richiede alcuna installazione aggiuntiva per essere utilizzato.
- Obiettivi personalizzati: obiettivi definiti dall'utente che non sono contenuti AWS ufficiali. Puoi creare lenti personalizzate basandoti sui tuoi pilastri, sulle tue domande, sulle migliori pratiche e sui tuoi piani di miglioramento, oltre a condividere lenti personalizzate con altri. Account AWS

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

Aggiungere un obiettivo a un carico di lavoro

Per aggiungere un approfondimento a 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. 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. Seleziona l'obiettivo da aggiungere, scegli Salva.

   Le lenti possono essere selezionate da Custom lens, Lens Catalog o entrambi.

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

Per ulteriori informazioni sul catalogo delle AWS lenti, visita AWS Well-Architected Lenses. Tieni presente che non tutti i white paper sugli obiettivi vengono forniti come obiettivi nel catalogo degli obiettivi.

> **Dichiarazione di non responsabilità**
>
> Accedendo e/o applicando lenti personalizzate create da un altro AWS utente o account, l'utente riconosce che le lenti personalizzate create da altri utenti e condivise con l'utente sono Contenuti di terze parti come definito nel Contratto con il AWS cliente.

Rimuovere un obiettivo da un carico di lavoro

Come rimuovere un approfondimento da un carico di lavoro

1. Accedere AWS Management Console e aprire 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 desiderato e scegliere View details (Visualizza dettagli).
4. Deseleziona l'obiettivo che desideri rimuovere e scegli Salva.

   La lente AWS Well-Architected Framework non può essere rimossa 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.

Dettagli della lente

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 un elenco dei principali IAM con cui l'obiettivo è stato condiviso.

Obiettivi personalizzati

Puoi creare lenti personalizzate con i tuoi pilastri, le tue domande, le tue migliori pratiche e il tuo piano di miglioramento. Applichi lenti personalizzate a un carico di lavoro nello stesso modo in cui applichi le lenti AWS fornite. Puoi anche condividere obiettivi personalizzati che crei con altri Account AWS e gli obiettivi personalizzati di proprietà di altri possono essere condivisi con te.

È possibile personalizzare le domande in modo che siano specifiche per una particolare tecnologia, aiutarvi a soddisfare le esigenze di governance all'interno della vostra organizzazione o estendere le linee guida fornite dal Well-Architected Framework e dagli obiettivi. AWS Analogamente agli obiettivi esistenti, è possibile monitorare i progressi nel tempo creando traguardi e fornire uno stato periodico generando report.

Argomenti

- Visualizzazione di obiettivi personalizzati
- Creazione di un obiettivo personalizzato
- Visualizzazione in anteprima di una lente personalizzata
- Pubblicazione di un obiettivo personalizzato per la prima volta
- Pubblicazione di un aggiornamento per un obiettivo personalizzato
- Condivisione di un obiettivo personalizzato
- Aggiungere tag a un obiettivo personalizzato
- Eliminazione di un obiettivo personalizzato
- Specifiche del formato delle lenti

Visualizzazione di obiettivi personalizzati

Puoi visualizzare i dettagli delle lenti personalizzate che possiedi e delle lenti personalizzate che sono state condivise con te.

Per visualizzare un obiettivo

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

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

3. Scegli quali obiettivi personalizzati vuoi visualizzare:
   - Owned by me: mostra le lenti personalizzate che hai creato.
   - Condiviso con me: mostra le lenti personalizzate che sono state condivise con te.
4. Seleziona l'obiettivo personalizzato da visualizzare in uno dei seguenti modi:
   - Scegli il nome dell'obiettivo.
   - Seleziona l'obiettivo e scegli Visualizza dettagli.

Viene visualizzata la Dettagli della lente pagina.

La pagina Lenti personalizzate contiene i seguenti campi:

Nome

Il nome dell'obiettivo.

Owner

L' Account AWS ID che possiede l'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 DRAFT 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 delle lenti personalizzate.

Creazione di un obiettivo personalizzato

Per creare una lente personalizzata

1. Accedi 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, scegli Obiettivi personalizzati.
3. Scegli Crea obiettivo personalizzato.
4. Scegli Scarica file per scaricare il file modello JSON.
5. Apri il file modello JSON con il tuo editor di testo preferito e aggiungi i dati per il tuo obiettivo personalizzato. Questi dati includono i pilastri, le domande, le migliori pratiche e i link ai piani di miglioramento.

   Fare riferimento a Specifiche del formato delle lenti per ulteriori dettagli. Una lente personalizzata non può superare le dimensioni di 500 KB.
6. Scegli il file per selezionare il tuo file JSON.
7. (Facoltativo) Nella sezione Tag, aggiungi i tag che desideri associare all'obiettivo personalizzato.
8. Scegliete Invia e anteprima per visualizzare l'anteprima dell'obiettivo personalizzato o Invia per inviare l'obiettivo personalizzato senza visualizzarlo in anteprima.

   Se scegli di Invia e visualizza in anteprima l'obiettivo personalizzato, puoi selezionare Avanti per navigare nell'anteprima dell'obiettivo o selezionare Esci dall'anteprima dell'obiettivo per tornare a Obiettivi personalizzati.

Se la convalida fallisce, modifica il file JSON e prova a creare nuovamente l'obiettivo personalizzato.

Dopo aver AWS WA Tool convalidato il file JSON, l'obiettivo personalizzato viene visualizzato in Obiettivi personalizzati.

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

Puoi creare fino a 15 obiettivi personalizzati in un Account AWS.

> **Dichiarazione di non responsabilità**
>
> Non includete o raccogliete informazioni personali identificabili (PII) degli utenti finali o di altre persone identificabili nelle o tramite le vostre lenti personalizzate. Se le tue lenti personalizzate o quelle condivise con te e utilizzate nel tuo account includono o raccolgono informazioni personali, sei responsabile di: garantire che le PII incluse vengano trattate in conformità alla legge applicabile, fornire adeguate informative sulla privacy e ottenere i consensi necessari per il trattamento di tali dati.

Visualizzazione in anteprima di una lente personalizzata

Per visualizzare l'anteprima di 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. Nel riquadro di navigazione a sinistra, scegli Obiettivi personalizzati.
3. È possibile visualizzare in anteprima solo gli obiettivi con stato DRAFT. Seleziona l'obiettivo personalizzato DRAFT desiderato e scegli Esperienza di anteprima.
4. Scegliete Avanti per navigare nell'anteprima dell'obiettivo.
5. (Facoltativo) Puoi rivedere il tuo piano di miglioramento selezionando le migliori pratiche all'interno di ogni domanda nell'anteprima e scegliendo Aggiorna in base alle risposte per testare la tua logica di rischio. Se sono necessarie modifiche, puoi aggiornare le regole di rischio nel modello JSON prima della pubblicazione.
6. Scegli Exit Preview per tornare all'obiettivo personalizzato.

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

Pubblicazione di un obiettivo personalizzato per la prima volta

Per pubblicare 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. Nel riquadro di navigazione a sinistra, scegli Obiettivi personalizzati.
3. Seleziona l'obiettivo personalizzato desiderato e scegli Pubblica obiettivo.
4. Nella casella Nome versione, inserisci un identificatore univoco per la modifica della versione. Questo valore può contenere fino a 32 caratteri e deve contenere solo caratteri e punti alfanumerici («.»).
5. Scegli Pubblica lente personalizzata.

   Dopo la pubblicazione, un obiettivo personalizzato passa allo stato PUBBLICATO.

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

Pubblicazione di un aggiornamento per un obiettivo personalizzato

Per pubblicare un aggiornamento di un obiettivo personalizzato esistente

1. Accedi 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, scegli Obiettivi personalizzati.
3. Seleziona l'obiettivo personalizzato desiderato e scegli Modifica.
4. Se non hai un file JSON aggiornato pronto, scegli Scarica file per scaricare una copia dell'obiettivo personalizzato corrente. Modifica il file JSON scaricato con il tuo editor di testo preferito e apporta le modifiche desiderate.

5. Scegli il file per selezionare il file JSON aggiornato e scegli Invia e visualizza in 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 i 500 KB di dimensione.

   Dopo aver AWS WA Tool convalidato il file JSON, l'obiettivo personalizzato viene visualizzato in Obiettivi personalizzati con lo stato DRAFT.
6. Seleziona nuovamente l'obiettivo personalizzato e scegli Pubblica obiettivo.
7. Scegli Rivedi le modifiche prima della pubblicazione per verificare che le modifiche apportate all'obiettivo personalizzato siano corrette. Ciò include la convalida di:

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

   Seleziona Successivo.
8. Specificare il tipo di modifica della versione.

   Versione principale

   Indica che sono state apportate modifiche sostanziali all'obiettivo. Utilizzatelo 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 principali modifiche alla versione non vengono applicate automaticamente ai carichi di lavoro che utilizzano l'obiettivo.

   Versione secondaria

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

   Le modifiche di versione minori vengono applicate automaticamente ai carichi di lavoro utilizzando l'obiettivo personalizzato.

   Seleziona Successivo.

9. Nella casella Nome versione, inserisci un identificatore univoco per la modifica della versione. Questo valore può contenere fino a 32 caratteri e deve contenere solo caratteri e punti alfanumerici («.»).
10. Scegli Pubblica lente personalizzata.

    Dopo la pubblicazione, un obiettivo personalizzato passa allo stato PUBBLICATO.

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

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

Gli aggiornamenti delle versioni minori vengono applicati automaticamente senza alcuna notifica.

Puoi creare fino a 100 versioni di un obiettivo personalizzato.

Condivisione di un obiettivo personalizzato

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

Per condividere un obiettivo personalizzato con Account AWS altri utenti

1. Accedi 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, scegli Obiettivi personalizzati.
3. Seleziona l'obiettivo personalizzato da condividere e scegli Visualizza dettagli.
4. Nella Dettagli della lente pagina, scegli Condivisioni. Quindi scegli Crea e crea condivisioni per utenti o account per creare un invito a Lens Share.
5. Inserisci l' Account AWS ID a 12 cifre o l'ARN dell'utente con cui desideri condividere l'obiettivo personalizzato.
6. Scegli Crea per inviare un invito alla condivisione dell'obiettivo all'utente o all'utente specificato Account AWS .

Puoi condividere lenti personalizzate con un massimo di 300 Account AWS o più utenti.

Se l'invito a Lens Share non viene accettato entro sette giorni, l'invito scade automaticamente.

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

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

1. Accedere AWS Management Console e aprire la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegli Obiettivi personalizzati.
3. Seleziona l'obiettivo personalizzato da condividere.
4. Nella Dettagli della lente pagina, scegli Condivisioni. Quindi scegli Create and Create shares to Organizations.
5. Nella pagina Crea condivisione lenti personalizzate, scegli se concedere le autorizzazioni all'intera organizzazione o a una o più unità organizzative.
6. Scegli Crea per condividere l'obiettivo personalizzato.

Per vedere chi ha accesso condiviso a un obiettivo personalizzato, scegli Condivisioni dalla Dettagli della lente pagina.

> **Dichiarazione di non responsabilità**
>
> Condividendo le tue lenti personalizzate con altri Account AWS, riconosci che le tue lenti personalizzate AWS saranno disponibili per quegli altri account. Questi altri account possono continuare ad accedere e utilizzare le tue lenti personalizzate condivise anche se elimini le lenti personalizzate dai tuoi Account AWS o chiudi le tue Account AWS.

Aggiungere tag a un obiettivo personalizzato

Per aggiungere tag a 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. Nel riquadro di navigazione a sinistra, scegli Obiettivi personalizzati.
3. Seleziona l'obiettivo personalizzato che desideri aggiornare.
4. Nella sezione Tag, scegli Gestisci tag.
5. Seleziona Aggiungi nuovo tag e inserisci la chiave e il valore per ogni tag che desideri aggiungere.
6. Seleziona Salva.

Per rimuovere un tag, scegli Rimuovi accanto al tag che desideri rimuovere.

Eliminazione di un obiettivo personalizzato

Per eliminare un obiettivo personalizzato

1. Accedere AWS Management Console e aprire la AWS Well-Architected Tool console all'indirizzo https://console.aws.amazon.com/wellarchitected/.
2. Nel riquadro di navigazione a sinistra, scegli Obiettivi personalizzati.
3. Seleziona l'obiettivo personalizzato da eliminare e scegli Elimina.
4. Scegli Elimina.

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

> **Dichiarazione di non responsabilità**
>
> Condividendo le tue lenti personalizzate con altri Account AWS, riconosci che le AWS renderai disponibili a tali altri account. Questi altri account possono continuare ad accedere e utilizzare le tue lenti personalizzate condivise anche se elimini le lenti personalizzate dai tuoi Account AWS o chiudi le tue Account AWS.

Specifiche del formato delle lenti

Le lenti sono definite utilizzando un formato JSON specifico. Quando inizi a creare un obiettivo personalizzato, hai la possibilità di scaricare un file JSON modello. Puoi utilizzare questo file come

base per le tue lenti personalizzate in quanto definisce la struttura di base per i pilastri, le domande, le migliori pratiche e il piano di miglioramento.

Sezione Obiettivi

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

- `schemaVersion`: La versione dello schema di obiettivo personalizzato da utilizzare. Impostata in base al modello, non modificare.
- `name`: nome dell'obiettivo. Il nome può contenere fino a 128 caratteri.
- `description`: Descrizione testuale 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. Puoi mappare le tue domande sui pilastri del AWS Well-Architected Framework, definire i tuoi pilastri o entrambi.

È possibile definire fino a 10 pilastri in un obiettivo personalizzato.

- `id`: ID per il pilastro. L'ID può contenere da 3 a 128 caratteri e contenere solo caratteri alfanumerici e caratteri di sottolineatura («_»). Gli ID utilizzati in un pilastro devono essere univoci.

  Quando associ le tue domande ai pilastri del Framework, usa 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.

Puoi definire fino a 20 domande in un pilastro in una lente personalizzata.

- `id`: ID per la domanda. L'ID può contenere da 3 a 128 caratteri e contenere solo caratteri alfanumerici e caratteri 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 specificato se `helpfulResource url` è specificato.
- `helpfulResource url`: facoltativo. Una risorsa URL che spiega la domanda in modo più dettagliato. L'URL deve iniziare con `http://` o`https://`.

> **Note**
>
> Quando sincronizzi il carico di lavoro di un obiettivo personalizzato con Jira, le domande mostrano sia l' «id» che il «titolo» della domanda.
> 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.

Puoi definire fino a 15 scelte per una domanda in un obiettivo personalizzato.

- `id`: ID per la scelta. L'ID può essere compreso tra 3 e 128 caratteri e contenere solo caratteri alfanumerici e caratteri di sottolineatura («_»). È necessario specificare un ID univoco per ogni scelta in una domanda. L'aggiunta di una scelta con il suffisso di _no fungerà da `None of these` scelta 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 `helpfulResource url` specificato.
- `helpfulResource url`: facoltativo. Una 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. Un `improvementPlan` è obbligatorio per ogni scelta, ad eccezione di una `None of these` scelta.
- `improvementPlan url`: facoltativo. Una 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 uno dei due `HELPFUL_RESOURCE`IMPROVEMENT_PLAN.
- `additionalResources content`: facoltativo. Speciifica i `url` valori `displayText` e per la risorsa aggiuntiva. A scelta è possibile specificare fino a cinque risorse utili aggiuntive e fino a cinque elementi aggiuntivi del piano di miglioramento.
  - `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 `url` specificato.
  - `url`: facoltativo. Una risorsa URL per la risorsa utile o il piano di miglioramento. L'URL deve iniziare con `http://` o`https://`.

> **Note**
>
> Quando sincronizzi un carico di lavoro personalizzato con Jira, le scelte mostrano l' «id» della domanda e della scelta, oltre al «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 domanda, una per ogni livello di rischio.

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

  Deve esserci una regola di `default` rischio 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 valuta `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 prevede tre scelte (`choice_1`, e`choice_3`)`choice_2`, queste regole di rischio determinano il comportamento seguente:

- Se sono selezionate tutte e tre le scelte, non vi è alcun rischio.
- Se una delle due `choice_1` `choice_2` opzioni è selezionata ed `choice_3` è selezionata, il rischio è medio.
- Se non **`choice_1`** è selezionato ma `choice_3` è selezionato, esiste anche un rischio medio.
- Se nessuna di queste condizioni precedenti era vera, il rischio è elevato.

Aggiornamenti dell'obiettivo

Il AWS Well-Architected Framework Lens e gli altri obiettivi forniti AWS da vengono aggiornati man mano che vengono introdotti nuovi servizi, le best practice esistenti per i sistemi basati su cloud vengono perfezionate e vengono aggiunte nuove best practice. Quando viene resa disponibile una

nuova versione di una lente, AWS WA Tool viene aggiornata in base alle migliori pratiche più recenti. Tutti i nuovi carichi di lavoro definiti utilizzano la nuova versione dell'obiettivo.

Un aggiornamento dell'obiettivo si verifica anche quando viene pubblicata una nuova versione principale di un obiettivo personalizzato applicato a un carico di lavoro o a un modello di recensione.

Un aggiornamento dell'obiettivo può consistere in 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
- Aggiungere o rimuovere pilastri

Le tue risposte alle domande esistenti vengono mantenute.

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

Selezione di un aggiornamento dell'obiettivo

La pagina Notifiche mostra le informazioni per ogni carico di lavoro che non utilizza la versione più recente dell'obiettivo.

Le seguenti informazioni vengono visualizzate per ogni carico di lavoro:

Risorsa

Il nome del carico di lavoro o del modello di revisione.

Tipo di risorsa

Il tipo di risorsa. Può essere un modello di carico di lavoro o di revisione.

Risorsa associata

Il 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.
- Obsoleto: il carico di lavoro consiste nell'utilizzare una versione dell'obiettivo che non rispecchia 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 Nessuna 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

Le lenti possono essere aggiornate per carichi di lavoro e modelli di revisione.

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

Aggiornamento di un obiettivo per un carico di lavoro

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

> **Note**
>
> Puoi anche scegliere Visualizza gli aggiornamenti disponibili dalla scheda Panoramica del carico di lavoro.

2. Prima di aggiornare un obiettivo per un carico di lavoro, viene creata una pietra miliare per salvare lo stato del carico di lavoro esistente per riferimenti futuri. Inserisci un nome univoco per la pietra miliare nel campo Nome cardine.
3. Seleziona la casella di conferma accanto a Comprendo e accetto queste modifiche e scegli Salva.

Una volta aggiornato l'obiettivo, puoi visualizzare la versione precedente dell'obiettivo dalla scheda Milestones.

Aggiornamento di un obiettivo per un modello di recensione

1. Per aggiornare l'obiettivo per un modello di recensione, scegli
2. Nella pagina Notifiche, seleziona un modello di recensione da aggiornare e scegli Aggiorna la versione dell'obiettivo. Vengono visualizzate le informazioni su ciò che è cambiato in ogni pilastro.

> **Note**
>
> Puoi anche scegliere Visualizza gli upgrade disponibili dalla scheda Panoramica del modello di revisione.

3. Seleziona la casella di conferma accanto a Comprendo e accetto le modifiche e scegli Aggiorna e modifica le risposte del modello per modificare le risposte alle domande sulle migliori pratiche per il tuo modello di recensione, oppure Aggiorna per aggiornare l'obiettivo senza modificare le risposte del modello.

Catalogo delle lenti

Il Lens Catalog è una raccolta di obiettivi ufficiali AWS creati per offrire up-to-date tecnologie e best practice incentrate sul settore. AWS WA Tool 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 nel Lens Catalog.

Nome	Descrizione
AWS Well-Architected Framework	Applicato per impostazione predefinita a tutti i carichi di lavoro. Raccolta di best practice architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili nel cloud.
Mobilità connessa	Le migliori pratiche per integrare la tecnologia nei sistemi di trasporto e migliorare l'esperienza di mobilità complessiva.
Costruzione di container	Fornisce le migliori pratiche per la progettaz ione e il processo di costruzione dei container.
Analisi dei dati	Contiene informazioni raccolte da case study reali e ti aiuta a conoscere gli elementi di progettazione chiave dei carichi di lavoro di analisi Well-Architected, insieme a consigli per il miglioramento. AWS
DevOps	Descrive un approccio strutturato che le organizzazioni di tutte le dimensioni possono seguire per coltivare una cultura ad alta velocità e incentrata sulla sicurezza, in grado di fornire un valore aziendale sostanziale utilizzando tecnologie e best practice moderne. DevOps
Pubblica amministrazione	Le migliori pratiche per la progettazione e la fornitura di servizi governativi su AWS.
Settore sanitario	Procedure ottimali e linee guida su come progettare, implementare e gestire i carichi di lavoro sanitari nel. Cloud AWS

Nome	Descrizione
IoT	Le migliori pratiche per la gestione dei carichi di lavoro dell'Internet of Things (IoT) in AWS.
Creazione di valore in operazioni di M&A	Fornisce una serie di domande aggiuntive da considerare quando si cercano modi per promuovere la crescita aziendale, ad esempio per le attività di fusioni e acquisizioni di private equity.
Machine Learning	Le migliori pratiche per la gestione delle risorse e dei carichi di lavoro di Machine Learning in AWS.
Migrazione	Le migliori pratiche per la migrazione a. Cloud AWS
SaaS	Incentrato sulla progettazione, implement azione e architettura dei carichi di lavoro SaaS (Software as a Service) in. Cloud AWS
SAP	Principi di progettazione e best practice per i carichi di lavoro SAP in. Cloud AWS
Applicazioni serverless	Le migliori pratiche per creare carichi di lavoro serverless su. AWS Copre scenari come microservizi RESTful, backend di app mobili, elaborazione di stream e applicazioni web.

Modelli di revisione

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 quando si esegue 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 utente o account IAM o con un'organizzazione o un'unità organizzativa dello stesso. Regione AWS Puoi definire un carico di lavoro a partire da un modello di revisione, che aiuta a scalare le migliori pratiche comuni e a ridurre la ridondanza tra i carichi di lavoro.

Creazione di un modello di recensione

Per creare un modello di recensione

1. Seleziona Modelli di revisione nel riquadro di navigazione a sinistra.
2. Scegliere Create template (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. Seleziona Avanti.
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. Scegliere Create template (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

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 consigliate che desideri modificare.
   c. Scegli Salva ed esci per salvare le modifiche.

Condivisione di un modello di recensione

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 utenti o account IAM. Nella casella Invia inviti, specifica gli ID utente o account 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

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 delle autorizzazioni IAM 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 autorizzazioni IAM, consulta la AWSIdentity and Access Management User Guide.

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. Seleziona Avanti.

   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

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 utenti, account o organizzazioni IAM, questi non saranno in grado di creare carichi di lavoro a partire da esso.

Profili

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

È possibile creare un profilo dalla pagina Profili e associarlo a un nuovo carico di lavoro oppure 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, inserisci un nome e una descrizione per il tuo profilo.
4. Per definire le informazioni prioritarie per la tua azienda nel piano di revisione e miglioramento del carico di lavoro, seleziona le risposte più pertinenti alla tua azienda nella sezione Domande sul profilo.
5. (Facoltativo) Nella sezione Tag, aggiungi i tag che desideri associare al profilo.

   Per ulteriori informazioni sui tag, vedereTagging 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 descrizione, l'ARN, le date di creazione e aggiornamento e le risposte alle domande sul profilo. Dalla pagina panoramica del profilo puoi modificare, eliminare o condividere il tuo profilo.

Modifica di un profilo

Per modificare un profilo

1. Seleziona Profili nel riquadro di navigazione a sinistra o scegli Visualizza profilo dalla 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 gli aggiornamenti necessari alle domande del profilo.
5. Seleziona Salva.

Condivisione di un profilo

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 su utenti o account IAM. Nella casella Invia inviti, specifica gli ID utente o account e scegli Crea.
5. Per condividere con un'organizzazione o un'unità organizzativa, scegli Crea e seleziona Crea condivisioni 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), è necessario abilitare AWS Organizations l'accesso.

Aggiungere un profilo a un carico di lavoro

È possibile aggiungere un profilo a un carico di lavoro esistente o, quando si definisce un carico di lavoro, per velocizzare il processo di revisione del carico di lavoro. AWS WA Toolutilizza le informazioni raccolte dal tuo profilo per dare priorità alle domande pertinenti 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, vederethe 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 risposte alle domande prioritarie e ai rischi prioritari 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 descrizione, l'ARN, la versione e la data dell'ultimo aggiornamento del profilo associato al carico di lavoro.

Rimuovere un profilo da un carico di lavoro

La rimozione di un profilo dal carico di lavoro ripristina il carico di lavoro alla versione precedente a quando il profilo era associato e le domande e i rischi di 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. Scegliere Remove (Rimuovi).

Viene visualizzata una notifica che indica che il profilo è stato rimosso con successo dal carico di lavoro. La rimozione di un profilo ripristina il carico di lavoro alla versione precedente a quando il profilo 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 dei profili disponibili inAWS 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 del carico di lavoro utilizzando profili eliminati.

> **Dichiarazione di non responsabilità**
>
> Condividendo i tuoi profili con altriAccount AWS, riconosci che i tuoi profili AWS saranno disponibili per quegli altri account. Questi altri account possono continuare ad accedere e utilizzare i tuoi profili condivisi anche se elimini il profilo dal tuo Account AWS o interrompi il tuoAccount AWS.

Per rimuovere 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. Scegliere Elimina.
4. Per confermare la rimozione, inserisci il nome del profilo nel campo di immissione del testo.
5. Scegliere 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 Scaricala ora.
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 la tua AccessKeyIdchiave 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 una chiave segreta AccessKeyIde segreta per l'utente Account AWS, vedere Gestione delle chiavi di accesso (console) e per informazioni dettagliate sull'utilizzo di credenziali a breve termine, vedere Richiesta di credenziali temporanee.

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

Non sono necessarie ulteriori azioni nel tuo account Jira per installare il connettore.

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, vedi 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 quando definisci 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 il 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,

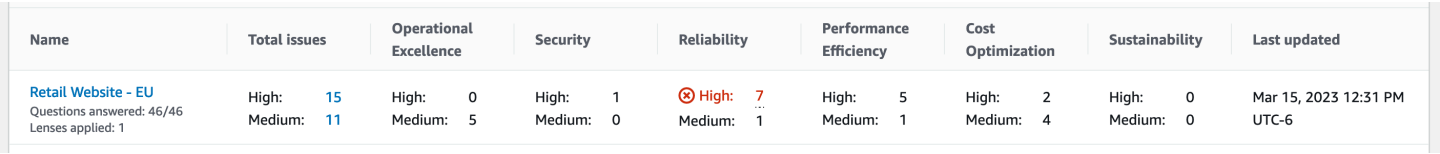
La sezione Problemi per pilastro del Well-Architected Framework mostra una rappresentazione grafica del numero di problemi ad alto e medio rischio per pilastro per tutti i carichi di lavoro.

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 in AWS Well-Architected Tool

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

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

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

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

Argomenti

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

Protezione dei dati in AWS Well-Architected Tool

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

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

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

Crittografia dei dati a riposo

Tutti i dati archiviati da AWS WA Tool vengono crittografati quando sono inattivi.

Crittografia in transito

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

Come AWS utilizza i tuoi dati

Il team AWS Well-Architected raccoglie dati aggregati per fornire e migliorare AWS Well-Architected Tool il servizio ai clienti. AWS WA Tool I dati dei singoli clienti possono essere condivisi con i Account AWS team per supportare gli sforzi dei nostri clienti volti a 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 dall'esterno di AWS WA Tool . 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 AWS Well-Architected Tool

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS WA Tool IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come AWS Well-Architected Tool funziona con IAM
- AWS Well-Architected Tool esempi di politiche basate sull'identità
- AWS politiche gestite per AWS Well-Architected Tool
- Risoluzione dei problemi di AWS Well-Architected Tool identità e accesso

Destinatari

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

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

Amministratore del servizio: se sei responsabile delle AWS WA Tool risorse della tua azienda, probabilmente hai pieno accesso a AWS WA Tool. È tuo compito determinare a quali AWS WA Tool funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS WA Tool, consultaCome AWS Well-Architected Tool funziona con IAM.

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

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

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

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

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

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle 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 di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per 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 di 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 Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

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

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

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

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

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

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

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

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

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

Policy basate su identità

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

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su 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 utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle 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 su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF 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 tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

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

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Well-Architected Tool funziona con IAM

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

Funzionalità IAM che puoi utilizzare con AWS Well-Architected Tool

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

Per avere una panoramica di alto livello su come AWS WA Tool e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Policy AWS WA Tool basate su identità

Supporta le azioni di policy	Sì

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

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

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

Politiche basate sulle risorse all'interno 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. Gli esempi più comuni di policy basate su 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 utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. 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 il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad 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 Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per AWS WA Tool

Supporta le azioni di policy	Sì

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

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

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

Le azioni politiche AWS WA Tool utilizzano il seguente prefisso prima dell'azione:`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 Tool definisce un proprio set di operazioni che descrivono le attività che puoi eseguire con questo servizio.

Per visualizzare un elenco di AWS WA Tool azioni, vedere Azioni definite da AWS Well-Architected Tool nel riferimento di autorizzazione del servizio.

Risorse di policy

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, 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'azione. 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). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco dei tipi di AWS WA Tool risorse e dei relativi ARN, consulta Resources defined by AWS Well-Architected Tool nel Service Authorization Reference. 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 AWS WA Tool carico di lavoro ha il seguente ARN:

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

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

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 AWS WA Tool azioni, come quelle per la creazione e l'elenco dei 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 dei tipi di AWS WA Tool risorse e dei relativi ARN, consulta Resources Defined by AWS Well-Architected Tool nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS Well-Architected Tool.

Chiavi relative alle condizioni delle politiche per AWS WA Tool

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

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

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

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

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi 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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

AWS WA Tool non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, vedere AWS Global Condition Context Keys nel Service Authorization Reference.

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

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

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

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi 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 del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

ACL 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 ad 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, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. 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 Che cos'è ABAC? nella Guida per l'utente di 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, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente 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 Cambio di un ruolo (console) nella Guida per l'utente di IAM.

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

Autorizzazioni principali multiservizio per AWS WA Tool

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

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 Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

Ruoli collegati ai servizi per AWS WA Tool

Supporta i ruoli collegati ai servizi	No

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

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.

AWS Well-Architected Tool esempi di politiche basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS WA Tool . Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o. AWS Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore 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
- Accedere a un carico di lavoro

Best practice delle policy

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

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzionalità dei processi nella Guida per l'utente di IAM.

- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi 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. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio 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 di 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 IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'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 Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

Utilizzo della console di AWS WA Tool

Per accedere alla AWS Well-Architected Tool console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS WA Tool risorse del 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 AWS WA Tool console, allega anche la seguente politica AWS gestita 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 è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Concessione dell'accesso completo ai carichi di lavoro

In questo esempio, vuoi concedere a un utente l'accesso Account AWS completo ai tuoi carichi di lavoro. L'accesso completo consente all'utente di eseguire tutte le azioni 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, vuoi concedere a un utente in Account AWS sola lettura l'accesso ai tuoi 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": "*"
     }
   ]
}
```

Accedere a un carico di lavoro

In questo esempio, vuoi concedere a un utente in sola lettura l'accesso in Account AWS sola lettura a uno dei tuoi carichi di lavoro99999999999955555555555566666666, 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"
     }
   ]
}
```

AWS politiche gestite per AWS Well-Architected Tool

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

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

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

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

AWS politica gestita: WellArchitectedConsoleFullAccess

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

Questa politica garantisce l'accesso completo a. AWS Well-Architected Tool

Dettagli dell'autorizzazione

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

AWS politica gestita: WellArchitectedConsoleReadOnlyAccess

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

Questa politica garantisce 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": "*"
      }
   ]
}
```

AWS politica gestita: AWSWellArchitectedOrganizationsServiceRolePolicy

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

Questa politica concede le autorizzazioni amministrative necessarie per supportare AWS Well-Architected Tool l'integrazione con Organizations. AWS 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 responsabili di verificare se l'accesso al AWS servizio è abilitato. AWS WA Tool
- `organizations:DescribeAccount`— Consente ai responsabili di recuperare informazioni su un account dell'organizzazione.
- `organizations:DescribeOrganization`— Consente ai dirigenti di recuperare informazioni sulla configurazione dell'organizzazione.
- `organizations:ListAccounts`— Consente ai responsabili di recuperare l'elenco degli account che appartengono a un'organizzazione.
- `organizations:ListAccountsForParent`— Consente ai responsabili di recuperare l'elenco degli account che appartengono a un'organizzazione da un determinato nodo principale dell'organizzazione.
- `organizations:ListChildren`— Consente ai responsabili di recuperare l'elenco degli account e delle unità organizzative che appartengono a un'organizzazione da un determinato nodo principale dell'organizzazione.

- `organizations:ListParents`— Consente ai responsabili di recuperare l'elenco dei genitori diretti specificati dall'unità organizzativa o dall'account all'interno di un'organizzazione.
- `organizations:ListRoots`— Consente ai responsabili di recuperare l'elenco di tutti i nodi principali 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": "*"
        }
    ]
}
```

AWS politica gestita: AWSWellArchitectedDiscoveryServiceRolePolicy

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

Questa politica consente di accedere AWS Well-Architected Tool ai AWS servizi e alle risorse che si riferiscono alle AWS WA Tool risorse.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `trustedadvisor:DescribeChecks`— Elenca Trusted Advisor i controlli disponibili.
- `trustedadvisor:DescribeCheckItems`— Recupera i dati di Trusted Advisor controllo, inclusi lo stato e le risorse contrassegnate da. Trusted Advisor

- `servicecatalog:GetApplication`— Recupera i dettagli di un'applicazione. AppRegistry
- `servicecatalog:ListAssociatedResources`— Elenca le risorse associate a un' AppRegistry applicazione.
- `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`— Richiesto 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-*"
   ]
  }
 ]
}
```

AWS WA Tool aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS WA Tool da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS WA Tool documenti.

Modifica	Descrizione	Data
AWS WA Tool politica gestita modificata	È stato aggiunto `"wellarchitected:Export*"` a `WellArchitectedConsoleReadOnlyAccess` .	22 giugno 2023
AWS WA Tool politica del ruolo di servizio aggiunta	`AWSWellArchitectedDiscoveryServiceRolePolicy` Aggiunto AWS Well-Architected Tool per consentire l'accesso a AWS servizi e risorse correlati alle AWS WA Tool risorse.	3 maggio 2023
AWS WA Tool autorizzazioni aggiunte	È stata aggiunta una nuova azione da `ListAWSServiceAccessForOrganization` concedere AWS WA Tool per consentire di verificare se l'accesso al AWS servizio è abilitato. AWS WA Tool	22 luglio 2022
AWS WA Tool ha iniziato a tenere traccia delle modifiche	AWS WA Tool ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	22 luglio 2022

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

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS WA Tool IAM.

Argomenti

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

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

Se ti AWS Management Console dice 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'errore di esempio seguente si verifica quando l'utente *mateojackson* tenta di utilizzare la console per eseguire l'`DeleteWorkload`azione, ma non dispone delle autorizzazioni.

```
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 all'incidente in AWS Well-Architected Tool

La risposta agli incidenti AWS Well-Architected Tool è una AWS responsabilità. AWS ha una politica e un programma formali e documentati che regolano la risposta agli incidenti.

AWS i problemi operativi di ampio impatto sono pubblicati nel AWS Service Health Dashboard.

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

Convalida della conformità per AWS Well-Architected Tool

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma

di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

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

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

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

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza in AWS Well-Architected Tool

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, 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 zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS Well-Architected Tool

In quanto servizio gestito, AWS Well-Architected Tool è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS WA Tool attraverso 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

La configurazione e i controlli IT sono una responsabilità condivisa tra te AWS e te, nostro cliente. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. 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.

Si consiglia di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che AWS Well-Architected Tool forniscono 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 come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition AWS WA Tool per evitare il confuso problema del vice.

```
{
  "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 Toolè integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unAWS servizio inAWS WA Tool. CloudTrail acquisisce tutte le chiamate API perAWS 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 CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi perAWS WA Tool. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella CloudTrail console di in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail, consentono di determinare la richiesta effettuata aAWS WA Tool, l'indirizzo IP di origine da cui è stata eseguita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida perAWS CloudTrail l'utente.

AWS WA Toolinformazioni in CloudTrail

CloudTrail è abilitato sul tuo alAccount AWS momento della sua creazione. Quando si verifica un'attività inAWS WA Tool, questa viene registrata in un CloudTrail evento insieme ad altri eventi diAWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS WA Tool, crea un trail. Un trail consente di CloudTrail 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 altriAWS servizi per analizzare con maggiore dettaglio e usare i dati eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

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

TutteAWS WA Tool le azioni vengono registrate CloudTrail e documentate in Azioni definite daAWS Well-Architected Tool. Ad esempio, le chiamate a`CreateWorkloadDeleteWorkload`, e`CreateWorkloadShare` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce del log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle 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 dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia stack ordinata delle chiamate API pubbliche e di conseguenza non vengono visualizzati in base a un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail log di che illustra l'`CreateWorkload`operazione.

```
   {
    "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 Toolinvia eventi ad Amazon EventBridge quando vengono intraprese azioni su risorse Well-Architected. È possibile utilizzare EventBridge e questi eventi per scrivere regole che eseguono operazioni, ad esempio la notifica, quando si verifica un cambiamento. Per ulteriori informazioni, consulta Che cos'è Amazon EventBridge?.

> **Note**
>
> Gli eventi vengono distribuiti sulla base del miglior tentativo.

Le seguenti azioni hanno come risultato EventBridge eventi:

- Relativo al carico di lavoro
  - Creazione o eliminazione di un carico di lavoro
  - Creazione di un milestone
  - Aggiornamento delle proprietà di un carico di lavoro
  - Condivisione o annullamento di una condivisione di un carico di lavoro
  - Aggiornare lo stato di un invito a condividere
  - Aggiunta o rimozione di tag
  - Aggiornare una risposta
  - Aggiornamento delle note di revisione
  - Aggiunta o rimozione di un approfondimento da un carico di lavoro
- Relativo agli approfondimenti
  - Importazione o esportazione di un obiettivo personalizzato
  - Pubblicato un approfondimento personalizzato
  - Eliminazione di un approfondimento personalizzato
  - Condivisione o annullamento di un approfondimento personalizzato
  - Aggiornare lo stato di un invito a condividere
  - Aggiunta o rimozione di un approfondimento da un carico di lavoro

Eventi di esempioAWS WA Tool

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"
   }
}
```


Pubblicato un approfondimento 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: 16 aprile 2024

Modifica	Descrizione	Data
Jira	Questa versione ha aggiunto il AWS Well-Architected Tool Connector for Jira.	16 aprile 2024
Nuovi obiettivi	Questa versione ha aggiunto nuovi obiettivi al Lens Catalog.	26 marzo 2024
Funzionalità aggiornate	Questa versione aggiunge la funzionalità Lens Catalog a AWS WA Tool.	26 novembre 2023
Funzionalità aggiornate	Questa versione aggiunge la funzionalità Review Templates a AWS WA Tool.	3 ottobre 2023
WellArchitectedConsoleReadOnlyAccess politica gestita aggiornata	È stato aggiunto `"wellarchitected:ExportLens"` a `WellArchitectedConsoleReadOnlyAccess` .	22 giugno 2023
Funzionalità aggiornate	Questa versione aggiunge la funzionalità Profili a AWS WA Tool.	13 giugno 2023
Funzionalità aggiornate	Questa versione migliora l' AWS Service Catalog AppRegistry integrazione	3 maggio 2023

	AWS Trusted Advisor e la aggiunge `AWS WellArchitectedDiscoveryServiceRolePolicy` alle politiche AWS gestite.	
Aggiornamento dei contenuti	Pagina del pannello di controllo aggiornata per includere informazioni dettagliate sui rischi e sui piani di miglioramento. È stata inoltre aggiunta la possibilità di creare un rapporto consolidato sul carico di lavoro.	30 marzo 2023
Aggiornamento dei contenuti	Nome corretto della WellArchitectedConsoleReadOnlyAccess politica.	19 gennaio 2023
È stata aggiornata la guida IAM per AWS WA Tool	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta la sezione Best practice per la sicurezza in IAM	4 gennaio 2023
Funzionalità aggiornate	Questa versione rimuove l'obiettivo FTR dallo strumento.	14 dicembre 2022
Funzionalità aggiornate	Questa versione aggiunge l' AWS Service Catalog AppRegistry integrazione AWS Trusted Advisor and.	7 novembre 2022
Aggiornamento dei contenuti	È stato corretto un problema nell'esempio JSON dell'obiettivo personalizzato per. `choices`	29 settembre 2022

Aggiornamento dei contenuti	La `choices` sezione della specifica JSON dell'obiettivo personalizzato è stata aggiornata.	2 agosto 2022
Funzionalità aggiornate	Questa versione aggiunge il tracciamento delle modifiche per le relative politiche AWS gestite e ha aggiunto una nuova azione per concedere l'`ListAWSServiceAccessForOrganization` autorizzazione a. `AWSWellArchitectedOrganizationsServiceRolePolicy`	22 luglio 2022
È stata aggiunta la condivisione dell'organizzazione	Questa versione aggiunge la possibilità di condividere carichi di lavoro e obiettivi personalizzati con un'organizzazione e unità organizzative (OU).	30 giugno 2022
Funzionalità aggiornate	Questa versione aggiunge la possibilità di specificare risorse aggiuntive per le scelte in un obiettivo personalizzato, di visualizzare in anteprima un obiettivo personalizzato prima di pubblicarlo e di aggiungere tag agli obiettivi personalizzati.	21 giugno 2022
Funzionalità aggiornate	Questa versione aggiunge la possibilità di accedere alla community AWS Well-Architected su re:POST. AWS	31 maggio 2022

Funzionalità aggiornate	Questa versione aggiunge il pilastro della sostenibilità e aggiornamenti minori a Tutorial.	31 marzo 2022
EventBridge supporto aggiunto	AWS WA Tool ora invia un evento ad Amazon EventBridge quando viene apportata una modifica a una risorsa Well-Architected.	3 marzo 2022
Lenti personalizzate aggiunte	È stata aggiunta la possibilità di aggiungere obiettivi personalizzati.	29 novembre 2021
Funzionalità aggiornate	Le best practice individuali possono ora essere contrassegnate come non applicabili.	14 luglio 2021
Etichettatura delle risorse disponibile	Questa versione aggiunge la possibilità di aggiungere tag ai carichi di lavoro.	3 marzo 2021
API ora disponibile	Questa versione aggiunge l' AWS WA Tool API. AWS CloudTrail informazioni di registrazione aggiunte.	16 dicembre 2020
Funzionalità aggiornate	Questa versione aggiunge gli obiettivi FTR e SaaS allo strumento.	3 dicembre 2020
Protezione dei dati aggiornata	Informazioni sulla protezione dei dati aggiornate.	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	La condivisione chiarita è Regioni AWS stata introdotta dopo il 20 marzo 2019.	24 giugno 2020
Funzionalità aggiornate	L'accesso a una condivisi one 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 sull' AWS utilizzo dei 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 del carico di lavoro sono specifiche 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 versione aggiunge l' DeleteWorkload azione alla politica.	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	Questa versione aggiunge la possibilità di specificare un valore non-Regioni AWS durante la definizione di un carico di lavoro.	14 febbraio 2019
AWS Well-Architected Tool disponibilità generale	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.