User Guide

AWS Well-Architected Tool

AWS Well-Architected Tool: User Guide

Table of Contents

Wir haben eine neue Version des Well-Architected Framework veröffentlicht. Wir haben dem Lens-Katalog auch neue und aktualisierte Lenses hinzugefügt. Erfahre mehr über die Änderungen.

Was ist AWS Well-Architected Tool?

AWS Well-Architected Tool (AWS WA Tool) ist ein Service in der Cloud, der einen konsistenten Prozess zur Messung Ihrer Architektur anhand von AWS Best Practices bietet. AWS WA Tool hilft Ihnen während des gesamten Produktlebenszyklus, indem es wie folgt vorgeht:

- Unterstützung bei der Dokumentation der von Ihnen getroffenen Entscheidungen
- Bereitstellen von Empfehlungen zur Verbesserung Ihres Workloads basierend auf bewährten Methoden
- Unterstützung, Ihre Workloads zuverlässiger, sicherer, effizienter und kostengünstiger zu machen.

Sie können AWS WA Tool Ihre Arbeitslast anhand der Best Practices aus dem AWS Well-Architected Framework dokumentieren und messen. Diese Best Practices wurden von AWS Solutions Architects auf der Grundlage ihrer jahrelangen Erfahrung in der Entwicklung von Lösungen für eine Vielzahl von Unternehmen entwickelt. Das Framework bietet ein konsistentes Konzept für die Messung von Architekturen und stellt Anleitungen zur Implementierung von Entwürfen bereit, die sich Ihren wachsenden Anforderungen anpassen.

Zusätzlich zu den AWS bewährten Methoden können Sie benutzerdefinierte Objektive verwenden, um Ihre Arbeitslast anhand Ihrer eigenen Best Practices zu messen. Sie können die Fragen in einem benutzerdefinierten Objektiv so anpassen, dass sie spezifisch auf eine bestimmte Technologie zugeschnitten sind oder Sie dabei unterstützen, die Governance-Anforderungen in Ihrem Unternehmen zu erfüllen. Maßgefertigte Brillengläser erweitern die durch die AWS Objektive gebogene Orientierung.

Integriert in AWS Trusted Advisorund AWS Service Catalog AppRegistryhilft Ihnen dabei, die Informationen, die Sie zur Beantwortung von AWS Well-Architected Tool Bewertungsfragen benötigen, leichter zu finden.

Dieser Service richtet sich an Personen, die an der technischen Produktentwicklung beteiligt sind, z. B. Chief Technology Officers (CTOs), Architekten, Entwickler und Mitglieder des Betriebsteams. AWS Kunden nutzen diese AWS WA Tool Methode, um ihre Architekturen zu dokumentieren, die Produkteinführungen zu kontrollieren und die Risiken in ihrem Technologieportfolio zu verstehen und zu managen.

Themen

- Was ist AWS Well-Architected Framework?

- AWS Well-Architected Tool Glossar

Was ist AWS Well-Architected Framework?

Das AWS Well-Architected Framework dokumentiert eine Reihe grundlegender Fragen, anhand derer Sie verstehen können, wie eine bestimmte Architektur mit den Best Practices der Cloud übereinstimmt. Das Framework bietet einen konsistenten Ansatz für die Bewertung von Systemen im Hinblick auf die Qualitäten, die von modernen cloud-basierten Systemen erwartet werden. Basierend auf dem Status Ihrer Architektur schlägt das Framework Verbesserungen vor, die Sie vornehmen können, um diese Qualitäten besser zu erreichen.

Mithilfe des Frameworks lernen Sie bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter und kostengünstiger Systeme in der Cloud kennen. Es bietet Ihnen die Möglichkeit, Ihre Architekturen konsequent an bewährten Methoden zu messen und Verbesserungspotenzial zu identifizieren. Das Framework basiert auf sechs Säulen: betriebliche Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz, Kostenoptimierung und Nachhaltigkeit.

Beim Entwerfen eines Workloads treffen Sie Kompromisse zwischen diesen Säulen, basierend auf Ihren Geschäftsanforderungen. Diese Geschäftsentscheidungen unterstützen Sie bei der Umsetzung Ihrer technischen Prioritäten. In Entwicklungsumgebungen werden die Optimierungen zur Kostensenkung möglicherweise auf Kosten der Zuverlässigkeit vorgenommen. In geschäftskritische Lösungen optimieren Sie womöglich die Zuverlässigkeit und sind bereit, höhere Kosten zu akzeptieren. In E-Commerce-Lösungen spielt die Leistung eventuell die wichtigste Rolle, da die Kundenzufriedenheit den Umsatz steigern kann. Sicherheit und Operational Excellence werden in der Regel nicht gegen die anderen Säulen abgewogen.

Weitere Informationen zum Framework finden Sie auf der AWS Well-Architected-Website.

AWS Well-Architected Tool Glossar

Im Folgenden werden allgemeine Begriffe definiert, die in AWS WA Tool und im AWS Well-Architected Framework verwendet werden.

- Ein Workload identifiziert eine Reihe von Komponenten, die einen geschäftlichen Mehrwert bieten. Der Workload ist in der Regel die Detailstufe, über die sich Unternehmens- und Technologieexperten austauschen. Beispiele für Workloads sind Marketing-Websites, E-Commerce-Websites, das Backend für eine mobile App und analytische Plattformen. Workloads unterscheiden sich in ihrem Grad an architektonischer Komplexität. Sie können einfach sein, wie

z. B. eine statische Website, oder komplex, wie bei Microservices-Architekturen mit mehreren Datenspeichern und vielen Komponenten.

- Meilensteine kennzeichnen wichtige Veränderungen in Ihrer Architektur, die sich während des gesamten Produktlebenszyklus — Design, Test, Inbetriebnahme und Produktion — weiterentwickelt.
- Linsen bieten Ihnen die Möglichkeit, Ihre Architekturen konsequent an bewährten Methoden zu messen und Verbesserungspotenzial zu identifizieren.

  Zusätzlich zu den von AWS bereitgestellten Objektiven können Sie auch Ihre eigenen Objektive erstellen und verwenden oder Objektive verwenden, die mit Ihnen geteilt wurden.
- Bei Problemen mit hohem Risiko (HRIs) handelt es sich um architektonische und betriebliche Entscheidungen, bei denen festgestellt AWS wurde, dass sie erhebliche negative Auswirkungen auf ein Unternehmen haben können. Diese HRIs können sich auf organisatorische Abläufe, Vermögenswerte und Einzelpersonen auswirken.
- Bei Problemen mit mittlerem Risiko (MRIs) handelt es sich um architektonische und betriebliche Entscheidungen, von denen festgestellt AWS wurde, dass sie sich negativ auf das Geschäft auswirken könnten, jedoch in geringerem Maße alsHRIs.

  Weitere Informationen finden Sie unter Probleme mit hohem Risiko (HRIs) und Probleme mit mittlerem Risiko (MRIs).

Erste Schritte mit AWS Well-Architected Tool

Um mit der Verwendung von AWS Well-Architected Tool zu beginnen, geben Sie zunächst den Benutzern, Gruppen und Rollen die entsprechenden Berechtigungen und aktivieren die Unterstützung für die AWS-Services, die Sie mit AWS WA Tool verwenden möchten. Als Nächstes definieren und dokumentieren Sie einen Workload. Sie können auch einen Meilenstein des aktuellen Status eines Workloads speichern.

In den folgenden Themen werden die ersten Schritte bei der Verwendung von AWS WA Tool erläutert. Eine schrittweise Anleitung zur Verwendung von AWS Well-Architected Tool finden Sie unter Tutorial: Einen AWS Well-Architected Tool-Workload dokumentieren.

Themen

Benutzern, Gruppen oder Rollen Zugriff auf AWS WA Tool gewähren

Sie können Benutzern, Gruppen oder Rollen einen vollen oder einen schreibgeschützten Zugriff auf AWS Well-Architected Tool gewähren.

Zugriff auf AWS WA Tool bereitstellen

1. Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

   - Benutzer und Gruppen in AWS IAM Identity Center:

     Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

2. Um Vollzugriff zu gewähren, wenden Sie die verwaltete Richtlinie WellArchitectedConsoleFullAccessauf den Berechtigungssatz oder die Rolle an.

   Der Vollzugriff ermöglicht dem Prinzipal die Ausführung aller Aktionen in AWS WA Tool. Dieser Zugriff ist erforderlich, um Workloads zu definieren, zu löschen, anzuzeigen, zu aktualisieren und freizugeben sowie benutzerdefinierte Lenses zu erstellen und freizugeben.
3. Um schreibgeschützten Zugriff zu gewähren, wenden Sie die verwaltete Richtlinie WellArchitectedConsoleReadOnlyAccess auf den Berechtigungssatz oder die Rolle an. Prinzipale mit dieser Rolle können nur Ressourcen anzeigen.

Weitere Informationen zu diesen Richtlinien finden Sie unter Von AWS verwaltete Richtlinien für AWS Well-Architected Tool.

Unterstützung in AWS WA Tool für andere AWS-Services aktivieren

Die Aktivierung des Organization-Zugriffs ermöglicht AWS Well-Architected Tool die Sammlung von Informationen über die Struktur Ihrer Organisation, um Ressourcen leichter freigeben zu können (siehe the section called “Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations” für weitere Informationen). Die Aktivierung der Discovery-Unterstützung ermöglicht die Sammlung von Informationen aus AWS Trusted Advisor, AWS Service Catalog AppRegistry und verwandten Ressourcen (z. B. AWS CloudFormation-Stapeln in AppRegistry-Ressourcensammlungen), sodass Sie die Informationen leichter entdecken können, die Sie zur Beantwortung von Well-Architected-Überprüfungsfragen benötigen. Außerdem können Sie die Trusted Advisor-Überprüfungen für einen Workload anpassen.

Wenn Sie die Unterstützung für AWS Organizations oder die Discovery-Unterstützung aktivieren, wird automatisch eine serviceverknüpfte Rolle für Ihr Konto erstellt.

Um die Unterstützung für andere Services zu aktivieren, mit denen AWS WA Tool interagieren kann, navigieren Sie zu Einstellungen.

1. Um Informationen aus AWS Organizations zu erfassen, aktivieren Sie AWS Organizations-Unterstützung aktivieren.
2. Aktivieren Sie Discovery-Unterstützung aktivieren, um Informationen aus anderen AWS-Services und -Ressourcen zu erfassen.
3. Wählen Sie Rollenberechtigungen anzeigen aus, um die Berechtigungen für die serviceverknüpfte Rolle oder die Richtlinien für Vertrauensbeziehungen anzuzeigen.
4. Wählen Sie Einstellungen speichern aus.

AppRegistry für einen Workload aktivieren

Die Verwendung von AppRegistry ist optional. Kunden von AWS Business Support und Enterprise Support können die Lösung pro Workload aktivieren.

Wenn die Discovery-Unterstützung aktiviert ist und AppRegistry einem neuen oder vorhandenen Workload zugeordnet wird, erstellt AWS Well-Architected Tool eine serviceverwaltete Attributgruppe. Die Attributgruppe Metadata in AppRegistry enthält den Workload-ARN, den Workload-Namen und die mit dem Workload verbundenen Risiken.

- Wenn die Discovery-Unterstützung aktiviert ist, wird die Attributgruppe bei jeder Änderung des Workloads aktualisiert.
- Wenn die Discovery-Unterstützung deaktiviert ist oder die Anwendung aus dem Workload entfernt wird, werden die Workload-Informationen aus AWS Service Catalog entfernt.

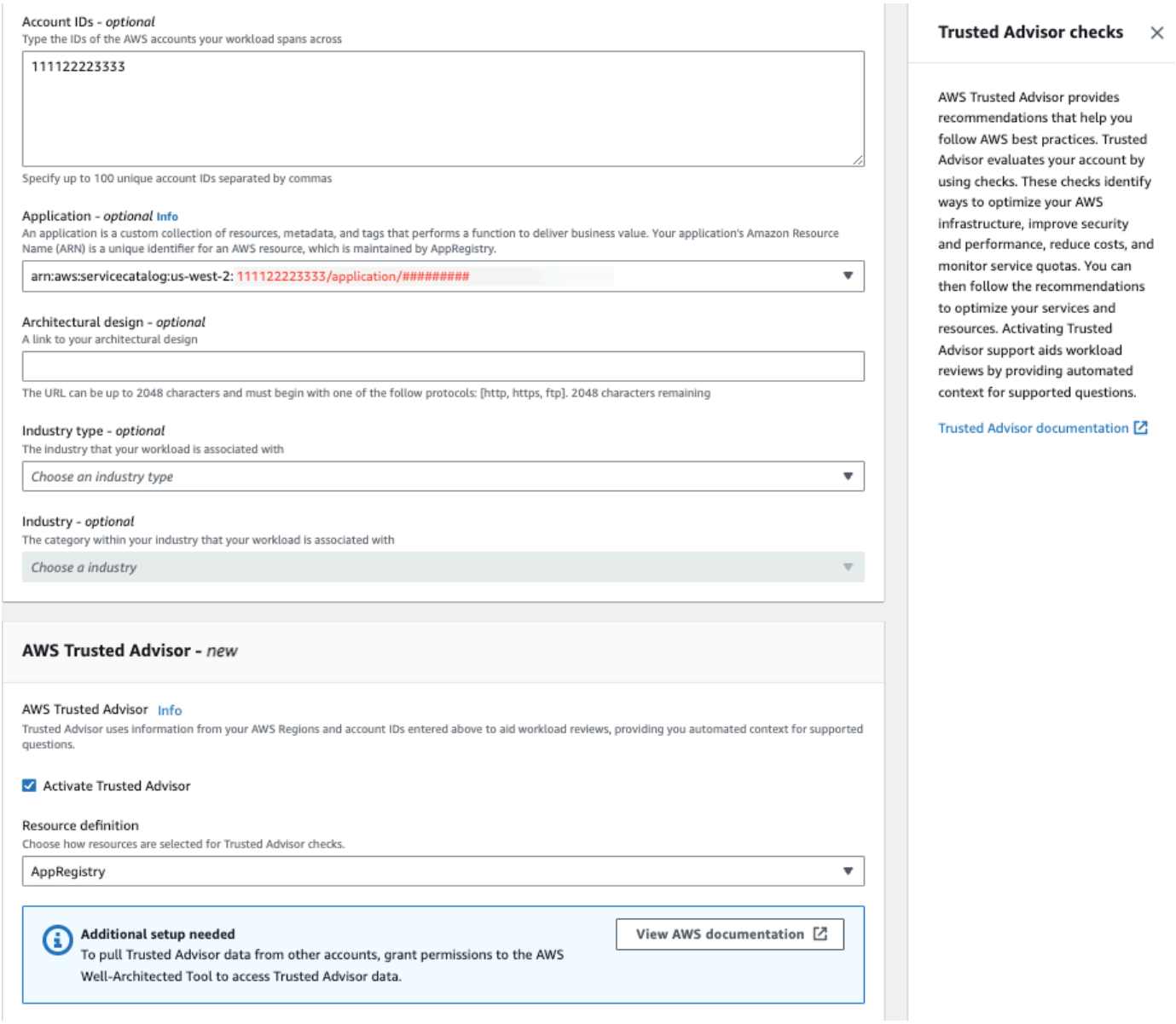
Wenn eine AppRegistry-Anwendung die Daten festlegen soll, die aus Trusted Advisor abgerufen werden, legen Sie die Ressourcendefinition als AppRegistry oder Alle fest. Erstellen Sie Rollen für alle Konten, die Ressourcen in Ihrer Anwendung besitzen. Folgen Sie dabei den Richtlinien unter the section called “Trusted Advisor in IAM aktivieren”.

AWS Trusted Advisor für einen Workload aktivieren

Sie können optional AWS Trusted Advisor integrieren und für Kunden von AWS Business Support und Enterprise Support auf Workload-Basis aktivieren. Die Integration von Trusted Advisor mit AWS WA Tool ist kostenlos. Preisdetails für Trusted Advisor finden Sie unter AWS-Supportpläne. Die Aktivierung von Trusted Advisor für Workloads bietet Ihnen einen umfassenderen, automatisierten und überwachten Ansatz für die Überprüfung und Optimierung Ihrer AWS-Workloads. Dies kann Ihnen helfen, die Zuverlässigkeit, Sicherheit, Leistung und Kostenoptimierung Ihrer Workloads zu verbessern.

So aktivieren Sie Trusted Advisor für einen Workload

1. Um Trusted Advisor zu aktivieren, können Workload-Besitzer AWS WA Tool zur Aktualisierung eines vorhandenen Workloads verwenden. Sie können auch einen neuen Workload erstellen, indem sie Workload definieren auswählen.
2. Geben Sie im Feld Konto-IDs eine Konto-ID ein, die von Trusted Advisor verwendet wird, wählen Sie eine Anwendungs-ARN in das Feld Anwendung aus, oder führen Sie beide Aktionen aus, um Trusted Advisor zu aktivieren.
3. Wählen Sie im Abschnitt AWS Trusted Advisor die Option Trusted Advisor aktivieren aus.



4. Bei der ersten Aktivierung von Trusted Advisor für einen Workload wird die Benachrichtigung IAM-Servicerolle wird erstellt angezeigt. Wenn Sie Berechtigungen anzeigen auswählen, werden die IAM-Rollenberechtigungen angezeigt. Sie können den Rollennamen sowie die Berechtigungen und Vertrauensbeziehungen anzeigen, die JSON automatisch für Sie in IAM erstellt hat. Nach der Erstellung der Rolle wird für folgende Workloads, die Trusted Advisoraktivieren, lediglich die Benachrichtigung Zusätzliche Einrichtung erforderlich angezeigt.
5. In der Dropdownliste Ressourcendefinition können Sie Workload-Metadaten, AppRegistry oder Alle auswählen. Die Auswahl der Ressourcendefinition legt die Daten fest, die AWS WA Tool aus Trusted Advisor abruft, um die Statusprüfungen in der Workload-Überprüfung bereitzustellen, die bewährten Well-Architected-Methoden entsprechen.

Workload-Metadaten – Der Workload wird durch die Konto-IDs und AWS-Regionen definiert, die im Workload angegeben werden.

AppRegistry – Der Workload wird von den Ressourcen definiert (z. B. AWS CloudFormation-Stapeln), die in der dem Workload zugeordneten AppRegistry-Anwendung enthalten sind.

Alle – Der Workload wird sowohl von den Workload-Metadaten als auch von den AppRegistry-Ressourcen definiert.

6. Wählen Sie Weiter.
7. Wenden Sie das AWS Well-Architected Framework auf Ihren Workload an und wählen Sie Workload definieren aus. Trusted Advisor-Überprüfungen sind nur mit dem AWS Well-Architected Framework verknüpft, nicht mit anderen Lenses.

Das AWS WA Tool ruft regelmäßig mithilfe der in IAM erstellten Rollen Daten aus Trusted Advisor ab. Die IAM-Rolle wird automatisch für den Workload-Besitzer erstellt. Um Trusted Advisor-Informationen anzuzeigen, müssen die Besitzer von Konten, die mit dem Workload verknüpft sind, zu IAM navigieren und eine Rolle erstellen. Weitere Informationen finden Sie unter ???. Wenn diese Rolle nicht vorhanden ist, kann AWS WA Tool keine Trusted Advisor-Informationen für dieses Konto abrufen und zeigt eine Fehlermeldung an.

Weitere Informationen zum Erstellen einer IAM-Rolle in AWS Identity and Access Management (IAM) finden Sie unter Eine Rolle für einen AWS-Service erstellen (Konsole) im IAM-Benutzerhandbuch.

Trusted Advisor für einen Workload in IAM aktivieren

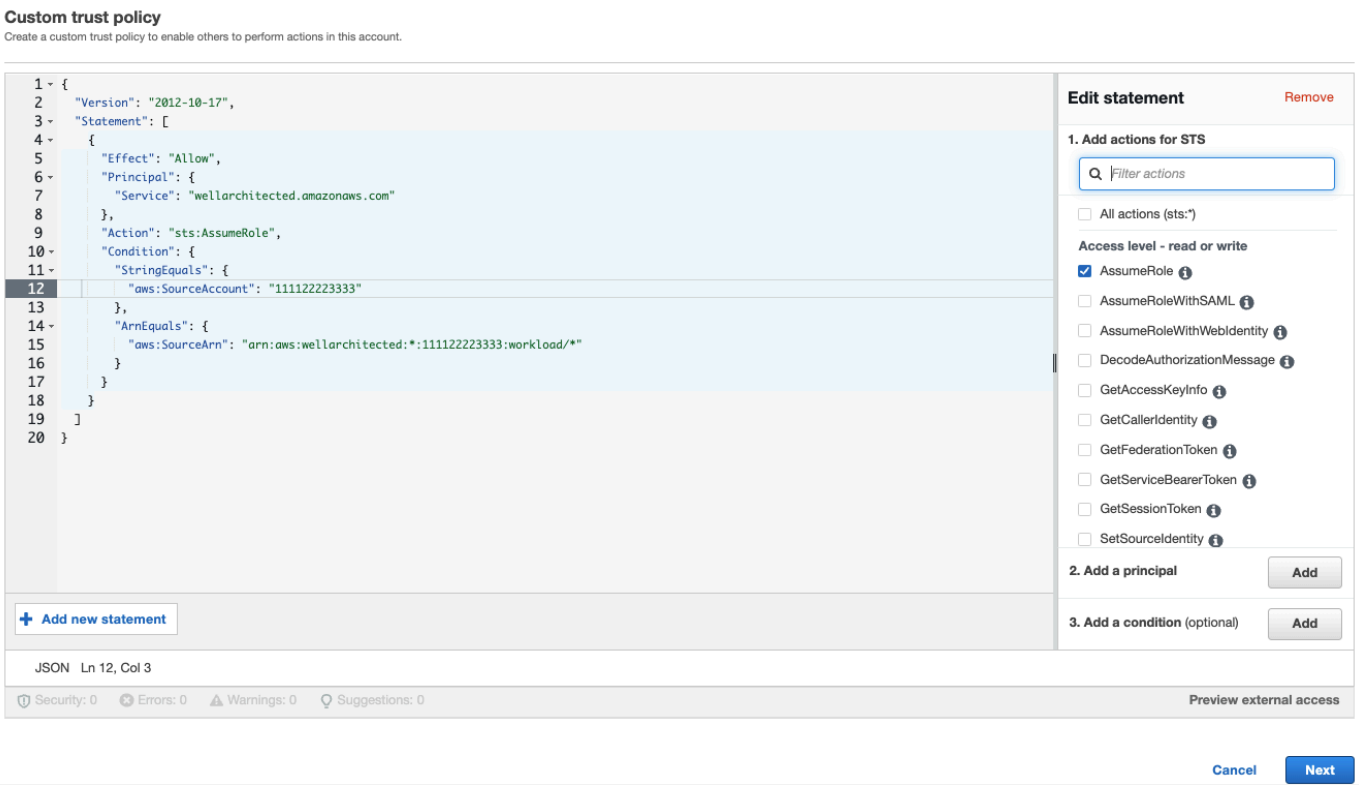
> **Note**
>
> Workload-Besitzer sollten Discovery-Unterstützung auswählen aktivieren, bevor sie einen Trusted Advisor-Workload erstellen. Durch die Auswahl von Discovery-Unterstützung aktivieren wird die Rolle erstellt, die für den Workload-Besitzer erforderlich ist. Führen Sie für alle anderen zugehörigen Konten die folgenden Schritte aus.

Die Besitzer der zugehörigen Konten für Workloads, für die Trusted Advisor aktiviert ist, müssen eine Rolle in IAM erstellen, um Trusted Advisor-Informationen in AWS Well-Architected Tool anzuzeigen.

So erstellen Sie eine Rolle in IAM für AWS WA Tool, um Informationen aus Trusted Advisor abzurufen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole in https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen und wählen Sie dann Rolle erstellen aus.
3. Wählen Sie in Vertrauenstyp der Entität die Option Benutzerdefinierte Vertrauensrichtlinie aus.
4. Kopieren Sie die folgende benutzerdefinierte Vertrauensrichtlinie und fügen Sie diese in das JSON-Feld in der IAM-Konsole ein, wie in der folgenden Abbildung gezeigt. Ersetzen Sie *WORKLOAD_OWNER_ACCOUNT_ID* durch die Konto-ID des Workload-Besitzers und wählen Sie Weiter aus.

```
{
  "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

Der `aws:sourceArn` im Bedingungsblock der vorhergehenden benutzerdefinierten Vertrauensrichtlinie ist `"arn:aws:wellarchitected:*:`*`WORKLOAD_OWNER_ACCOUNT_ID`*`:workload/*"`. Dies ist eine generische Bedingung, die angibt, dass diese Rolle von AWS WA Tool für alle Workloads des Workload-Besitzers verwendet werden kann. Der Zugriff kann jedoch auf einen bestimmten Workload-ARN oder einen Satz von Workload-ARNs eingeschränkt werden. Sehen Sie sich das folgende Beispiel für eine Vertrauensrichtlinie an, um zu erfahren, wie Sie mehrere ARNs angeben können.

```
{
    "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. Wählen Sie auf der Seite Berechtigungen hinzufügen in Berechtigungsrichtlinien die Option Richtlinie erstellen aus, um AWS WA Tool Lesezugriff auf Daten in Trusted Advisor zu gewähren. Wenn Sie Richtlinie erstellen auswählen, wird ein neues Fenster geöffnet.

> **Note**
>
> Darüber hinaus können Sie die Erstellung der Berechtigungen während der Rollenerstellung überspringen und nach dem Erstellen der Rolle eine Inline-Richtlinie erstellen. Wählen Sie in der Nachricht zur erfolgreichen Rollenerstellung Rolle anzeigen aus. Wählen Sie dann Inline-Richtlinie erstellen in der Dropdown-Liste Berechtigungen hinzufügen auf der Registerkarte Berechtigungen aus.

6. Kopieren Sie die folgende Berechtigungsrichtlinie und fügen Sie diese in das JSON-Feld ein. Ersetzen Sie im `Resource`-ARN *YOUR_ACCOUNT_ID* durch die ID Ihres eigenen Kontos, geben Sie die Region oder ein Sternchen (*) an und wählen Sie Weiter:Tags aus.

   Weitere Informationen zu ARN-Formaten finden Sie unter Amazon-Ressourcenname (ARN) im AWS Allgemeine Referenz-Handbuch.

```
{
    "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. Wenn Trusted Advisor für einen Workload aktiviert ist und die Ressourcendefinition auf AppRegistry oder Alle festgelegt ist, müssen alle Konten, die eine Ressource in der AppRegistry-Anwendung besitzen, die dem Workload angefügt ist, der Berechtigungsrichtlinie ihrer Trusted Advisor-Rolle die folgende Berechtigung hinzufügen.

```
{
    "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. (Optional) Fügen Sie Tags hinzu. Wählen Sie Weiter: Prüfen aus.
9. Überprüfen Sie die Richtlinie, geben Sie ihr einen Namen und wählen Sie Richtlinie erstellen aus.
10. Wählen Sie auf der Seite Berechtigungen hinzufügen für die Rolle den Namen der Richtlinie aus, die Sie gerade erstellt haben. Wählen Sie dann Weiter aus.
11. Geben Sie den Rollennamen ein, der die folgende Syntax verwenden muss: `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*. Wählen Sie dann Rolle erstellen aus. Ersetzen Sie *`WORKLOAD_OWNER_ACCOUNT_ID`* durch die Konto-ID des Workload-Besitzers.

    Sie sollten oben auf der Seite eine Erfolgsmeldung sehen, die Sie darüber informiert, dass die Rolle erstellt wurde.
12. Um die Rolle und die zugehörige Berechtigungsrichtlinie anzuzeigen, wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Rollen aus und suchen nach dem `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*-Namen. Wählen Sie den Namen der Rolle aus, um zu überprüfen, ob die Berechtigungen und Vertrauensbeziehungen korrekt sind.

Trusted Advisor für einen Workload deaktivieren

So deaktivieren Sie Trusted Advisor für einen Workload

Sie können Trusted Advisor für jeden Workload im AWS Well-Architected Tool deaktivieren, indem Sie den Workload bearbeiten und die Auswahl von Trusted Advisor aktivieren aufheben. Weitere Informationen zum Bearbeiten von Workloads finden Sie unter the section called “Bearbeiten Sie einen Workload”.

Durch die Deaktivierung von Trusted Advisor im AWS WA Tool werden die in IAM erstellten Rollen nicht gelöscht. Das Löschen von Rollen in IAM erfordert eine getrennte Bereinigungsmaßnahme. Workload-Besitzer oder Besitzer verknüpfter Konten sollten die erstellten IAM-Rollen löschen, wenn Trusted Advisor in AWS WA Tool deaktiviert wird. Alternativ können sie die Erfassung on Trusted Advisor-Daten für den Workload durch AWS WA Tool beenden.

So löschen Sie den **`WellArchitectedRoleForTrustedAdvisor`** in IAM

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole in https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen aus.

3. Suchen Sie nach `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* und wählen Sie den Rollennamen aus.
4. Wählen Sie Löschen aus. Geben Sie im Popup-Fenster den Namen der Rolle ein, um das Löschen zu bestätigen. Wählen Sie dann erneut Löschen aus.

Weitere Informationen zum Löschen von Rollen in IAM finden Sie unter Eine IAM-Rolle löschen (Konsole) im IAM-Benutzerhandbuch.

Einen Workload in AWS WA Tool definieren

Ein Workload ist ein Satz von Komponenten, die Geschäftswert bieten. Beispiele für Workloads sind Marketing-Websites, E-Commerce-Websites, Backends für mobile Apps und Analytikplattformen. Die genaue Definition eines Workloads hilft, eine umfassende Überprüfung anhand der Säulen des AWS Well-Architected Framework-sicherzustellen.

So definieren Sie einen Workload

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wenn Sie AWS WA Tool zum ersten Mal verwenden, wird eine Seite mit einer Einführung in die Funktionen des Service angezeigt. Wählen Sie im Abschnitt Define a workload (Einen Workload definieren) die Option Define workload (Workload definieren) aus.

   Alternativ können Sie im linken Navigationsbereich die Option Workloads und anschließend Define workload (Workload definieren) auswählen.

   Weitere Informationen zur Verwendung Ihrer Workload-Daten durch AWS finden Sie unter Warum benötigt AWS diese Daten und wie werden sie verwendet?.
3. Geben Sie im Feld Name einen Namen für Ihren Workload ein.

> **Note**
>
> Der Name muss zwischen 3 und 100 Zeichen lang sein. Mindestens drei Zeichen dürfen keine Leerzeichen sein. Namen von Workloads müssen eindeutig sein. Leerzeichen und Groß-/Kleinschreibung werden ignoriert, wenn auf Eindeutigkeit geprüft wird.

4. Geben Sie im Feld Description (Beschreibung) eine Beschreibung des Workloads ein. Die Beschreibung muss zwischen drei und 250 Zeichen lang sein.
5. Geben Sie im Feld Review owner (Prüfeigentümer) den Namen, die E-Mail-Adresse oder den Bezeichner für die primäre Gruppe oder die primäre Person ein, die Eigentümer des Workload-Überprüfungsprozesses ist.
6. Wählen Sie im Feld Environment (Umgebung) die Umgebung für Ihren Workload aus:
   - Produktion – Der Workload wird in einer Produktionsumgebung ausgeführt.
   - Vorproduktion – Der Workload wird in einer Vorproduktionsumgebung ausgeführt.
7. Wählen Sie im Abschnitt Regionen die Regionen für Ihren Workload aus:
   - AWS-Regionen – Wählen Sie nacheinander die AWS-Regionen aus, in denen Ihr Workload ausgeführt wird.
   - Andere als AWS-Regionen – Geben Sie die Namen der Regionen außerhalb von AWS ein, in denen Ihr Workload ausgeführt wird. Sie können bis zu fünf verschiedene Regionen angeben, jeweils durch Komma getrennt.

   Verwenden Sie beide Optionen, falls dies für Ihren Workload angemessen ist.
8. (Optional) Geben Sie im Feld Konto-IDs die IDs der AWS-Konten-Konten ein, die mit Ihrem Workload verknüpft sind. Sie können bis zu 100 eindeutige Konto-IDs angeben, getrennt durch Kommas.

   Wenn Trusted Advisor aktiviert ist, werden alle angegebenen Konto-IDs zum Abrufen von Daten aus Trusted Advisor verwendet. Informationen zum Erteilen von AWS WA Tool-Berechtigungen zum Abrufen von Trusted Advisor-Daten in Ihrem Namen innerhalb von IAM finden Sie unter AWS Trusted Advisor für einen Workload aktivieren.
9. (Optional) Geben Sie im Feld Anwendung den Anwendungs-ARN einer Anwendung aus dem AWS Service Catalog AppRegistry ein, den Sie diesem Workload zuordnen möchten. Pro Workload kann nur ein ARN angegeben werden. Anwendung und Workload müssen sich in derselben Region befinden.
10. (Optional) Geben Sie im Feld Architectural design (Architekturentwurf) die URL für Ihren Architekturentwurf ein.
11. (Optional) Wählen Sie im Feld Industry type (Branchenart) die Art der Branche im Zusammenhang mit Ihrem Workload aus.
12. (Optional) Wählen Sie im Feld Industry (Branche) die Branche aus, die Ihrem Workload am besten entspricht.

13. (Optional) Wählen Sie im Abschnitt Trusted Advisor die Option Trusted Advisor aktivieren aus, um Trusted Advisor-Prüfungen für Ihren Workload zu aktivieren. Für Konten, die mit Ihrem Workload verknüpft sind, ist möglicherweise eine zusätzliche Einrichtung erforderlich. Weitere Informationen zum Erteilen von AWS WA Tool-Berechtigungen zum Abrufen von Trusted Advisor-Daten in Ihrem Namen finden Sie unter the section called “Trusted Advisor aktivieren”. Wählen Sie in Ressourcendefinition die Option Workload-Metadaten, AppRegistry oder Alle aus, um die Ressourcen zu definieren, die für die Ausführung von Trusted Advisor-Prüfungen durch AWS WA Tool verwendet werden sollen.
14. (Optional) Wählen Sie im Abschnitt Jira die Option Einstellungen auf Kontoebene außer Kraft setzen aus, um die Jira-Synchronisationseinstellungen auf Workload-Ebene für den Workload zu aktivieren. Für Konten, die mit Ihrem Workload verknüpft sind, ist möglicherweise eine zusätzliche Einrichtung erforderlich. Informationen zu den ersten Schritten mit Einrichtung und Konfiguration des Konnektors finden Sie in AWS Well-Architected Tool-Konnektor für Jira. Wählen Sie Workload nicht synchronisieren, Workload synchronisieren – Manuell oder Workload synchronisieren – Automatisch aus. Geben Sie optional einen Jira-Projektschlüssel zur Synchronisierung ein.

    > **Note**
    >
    > Wenn Sie die Einstellungen auf Kontoebene nicht überschreiben, verwenden Workloads standardmäßig die Jira-Synchronisationseinstellung auf Kontoebene.

15. (Optional) Fügen Sie im Abschnitt Tags alle Tags hinzu, die Sie dem Workload zuordnen möchten.

    Weitere Informationen zu Tags finden Sie unter Markieren Ihrer AWS WA Tool-Ressourcen.
16. Wählen Sie Weiter.

    Wenn ein erforderliches Feld leer oder ein angegebener Wert nicht gültig ist, müssen Sie das Problem zuerst beheben, bevor Sie fortfahren können.
17. (Optional) Ordnen Sie im Schritt Profil anwenden dem Workload ein Profil zu, indem Sie ein vorhandenes Profil auswählen, nach dem Profilnamen suchen oder Profil erstellen auswählen, um ein Profil zu erstellen. Wählen Sie Weiter.
18. Wählen Sie die Linsen aus, die für diesen Workload gelten. Einem Workload können bis zu 2 Lenses hinzugefügt werden. Eine Beschreibung der offiziellen AWS-Lenses finden Sie unter Lenses.

Lenses können im Bereich Benutzerdefinierte Lenses (Lenses, die Sie selbst erstellt haben oder die für Ihr AWS-Konto freigegeben wurden), im Lens-Katalog (offizielle AWSLenses, die für alle Benutzer verfügbar sind) oder in beiden Bereichen ausgewählt werden.

> **Note**
>
> Der Abschnitt Benutzerdefinierte Lenses ist leer, wenn Sie keine benutzerdefinierte Lens erstellt haben oder keine benutzerdefinierte Lens für Sie freigegeben wurde.

> **Haftungsausschluss**
>
> Mit dem Zugriff auf und/oder der Anwendung von benutzerdefinierten Lenses, die von anderen AWS-Benutzern oder -Konten erstellt wurden, bestätigen Sie, dass benutzerdefinierte Lenses, die von anderen Benutzern erstellt und für Sie freigegeben wurden, Inhalte Dritter sind wie in der AWS-Kundenvereinbarung definiert.

19. Wählen Sie Define workload (Workload definieren) aus.

    Wenn ein erforderliches Feld leer oder ein angegebener Wert nicht gültig ist, müssen Sie zuerst das Problem beheben, bevor Ihr Workload definiert wird.

Einen Workload in AWS WA Tool dokumentieren

Nach der Definition eines Workloads in AWS Well-Architected Tool können Sie dessen Status dokumentieren, indem Sie die Seite „Workload überprüfen“ öffnen. So können Sie Ihren Workload bewerten und dessen Fortschritte über die Zeit nachverfolgen.

So dokumentieren Sie den Status eines Workloads

1. Nachdem Sie einen Workload zum ersten Mal definiert haben, wird Ihnen eine Seite mit den aktuellen Details Ihres Workloads angezeigt. Wählen Sie Start reviewing (Überprüfung starten) aus, um zu beginnen.

   Andernfalls können Sie im linken Navigationsbereich die Option Workloads sowie den Namen des Workloads auswählen, um die Detailseite des Workloads zu öffnen. Wählen Sie Continue reviewing (Überprüfung fortsetzen) aus.

(Optional) Wenn Ihrem Workload ein Profil zugeordnet ist, enthält der linke Navigationsbereich eine Liste mit priorisierten Fragen zur Workload-Überprüfung, mit denen Sie den Workload-Überprüfungsprozess beschleunigen können.

2. Sie erhalten nun die erste Frage. Gehen Sie bei jeder Frage wie folgt vor:

   a. Lesen Sie die Frage und entscheiden Sie, ob sie auf Ihren Workload zutrifft.

      Weitere Anleitungen finden Sie unter Info. Die Informationen werden im Hilfebereich angezeigt.

      - Wenn Frage nicht auf Ihren Workload zutrifft, wählen Sie Question does not apply to this workload (Frage gilt nicht für diesen Workload) aus.
      - Andernfalls wählen Sie die bewährten Methoden, die Sie derzeit befolgen, aus der Liste aus.

        Wenn Sie derzeit keine dieser bewährten Methoden befolgen, wählen Sie None of these (Nichts davon) aus.

      Weitere Anleitungen zu den einzelnen Elementen finden Sie unter Info. Die Informationen werden im Hilfebereich angezeigt.

   b. (Optional) Wenn eine oder mehrere bewährte Methoden auf Ihren Workload nicht zutreffen, wählen Sie Bewährte Methode(n) markieren, die für diesen Workload nicht zutreffen und dann die jeweilige(n) bewährte(n) Methode(n) aus. Für jede ausgewählte bewährte Methode können Sie optional einen Grund auswählen und zusätzliche Details angeben.

   c. (Optional) Verwenden Sie das Feld Notes (Notizen), um Informationen im Zusammenhang mit der Frage hinzuzufügen.

      Sie können beispielsweise beschreiben, warum die Frage nicht zutrifft, oder zusätzliche Details zu den ausgewählten bewährten Methoden bereitstellen.

   d. Wählen Sie Next (Weiter) aus, um mit der nächsten Frage fortzufahren.

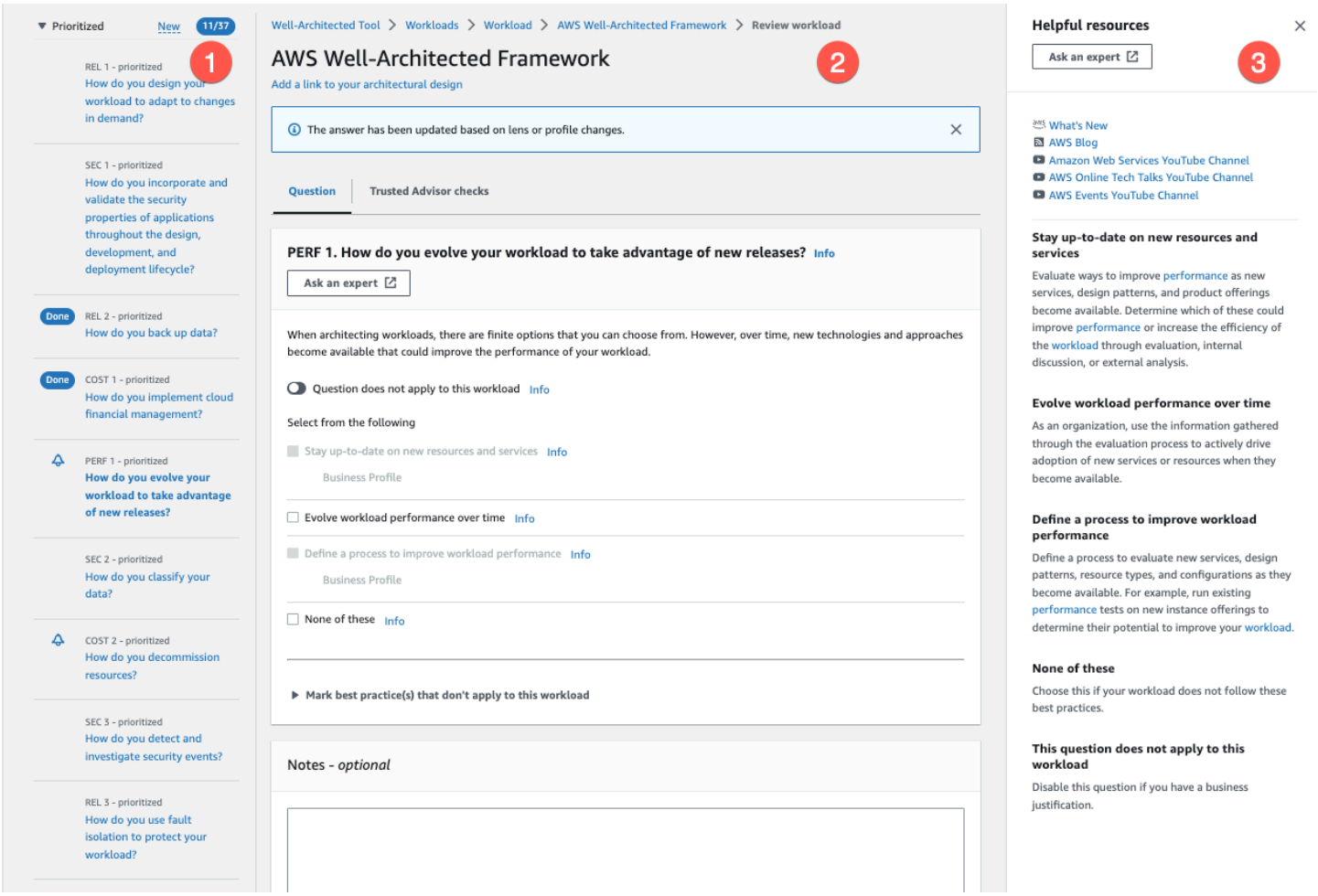
   Wiederholen Sie diese Schritte für jede Frage in jeder Säule.

3. Wählen Sie jederzeit Save and exit (Speichern und beenden) aus, um Ihre Änderungen zu speichern und die Dokumentation Ihres Workloads zu unterbrechen.

Nach der Dokumentierung Ihres Workloads können Sie zu den Fragen zurückkehren, um ihn jederzeit weiter zu überprüfen. Weitere Informationen finden Sie unter Einen Workload mit AWS Well-Architected Framework überprüfen.

Einen Workload mit AWS Well-Architected Framework überprüfen

Sie können Ihren Workload in der Konsole auf der Seite „Workload überprüfen“ überprüfen. Auf dieser Seite finden Sie bewährte Methoden und nützliche Ressourcen, um die Leistung Ihres Workloads zu verbessern.



1. Um die Seite „Workload überprüfen“ zu öffnen, wählen Sie auf der Seite „Workload-Details“ die Option Überprüfung fortsetzen aus. Im linken Navigationsbereich werden die Fragen für jede Säule angezeigt. Fragen, die Sie beantwortet haben, werden als Fertig markiert. Die Anzahl der Fragen, die in jeder Säule beantwortet wurden, werden neben dem Namen der Säule angezeigt.

   Sie können zu Fragen in anderen Säulen navigieren, indem Sie den Namen der Säule und anschließend die Frage auswählen, die Sie beantworten möchten.

(Optional) Wenn Ihrem Workload ein Profil zugeordnet ist, verwendet AWS WA Tool die Informationen im Profil, um zu ermitteln, welche Fragen in der Workload-Überprüfung priorisiert sind und welche Fragen für Ihr Unternehmen nicht relevant sind. Im linken Navigationsbereich können Sie die priorisierten Fragen verwenden, um die Überprüfung des Workloads zu beschleunigen. Neben Fragen, die der Liste der priorisierten Fragen neu hinzugefügt wurden, wird ein Benachrichtigungssymbol angezeigt.

2. Im mittleren Bereich wird die aktuelle Frage angezeigt. Wählen Sie die bewährten Methoden aus, die Sie befolgen. Wählen Sie Info aus, um zusätzliche Informationen zur Frage oder einer bewährten Methode zu erhalten. Wählen Sie Einen Experten fragen aus, um Zugang zur AWS-re:Post-Community für AWS Well-Architected zu erhalten. AWSre:Post ist ein themenbasierter Ersatz für Frage-und-Antwort-Communitys für AWS-Foren. Mit re:Post kannst du Antworten erhalten, Fragen beantworten, einer Gruppe beitreten, beliebten Themen folgen und über deine Lieblingsfragen und -antworten abstimmen.

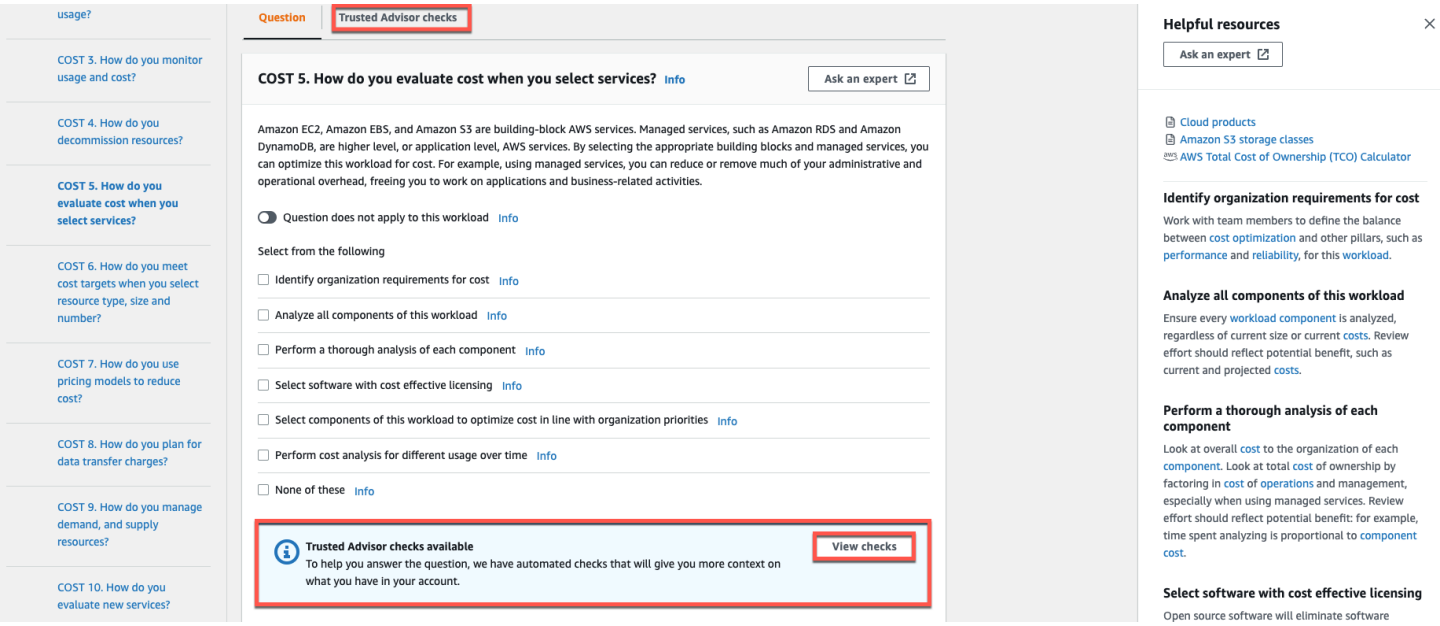
   (Optional) Um eine oder mehrere bewährte Methoden als nicht zutreffend zu markieren, wählen Sie Bewährte Methode(n) markieren, die für diesen Workload nicht zutreffen und dann die jeweilige(n) bewährte(n) Methode(n) aus.

   Über die Schaltflächen unten in diesem Bereich können Sie zur nächsten Frage wechseln, zur vorherigen Frage zurückkehren oder Ihre Änderungen speichern und beenden.

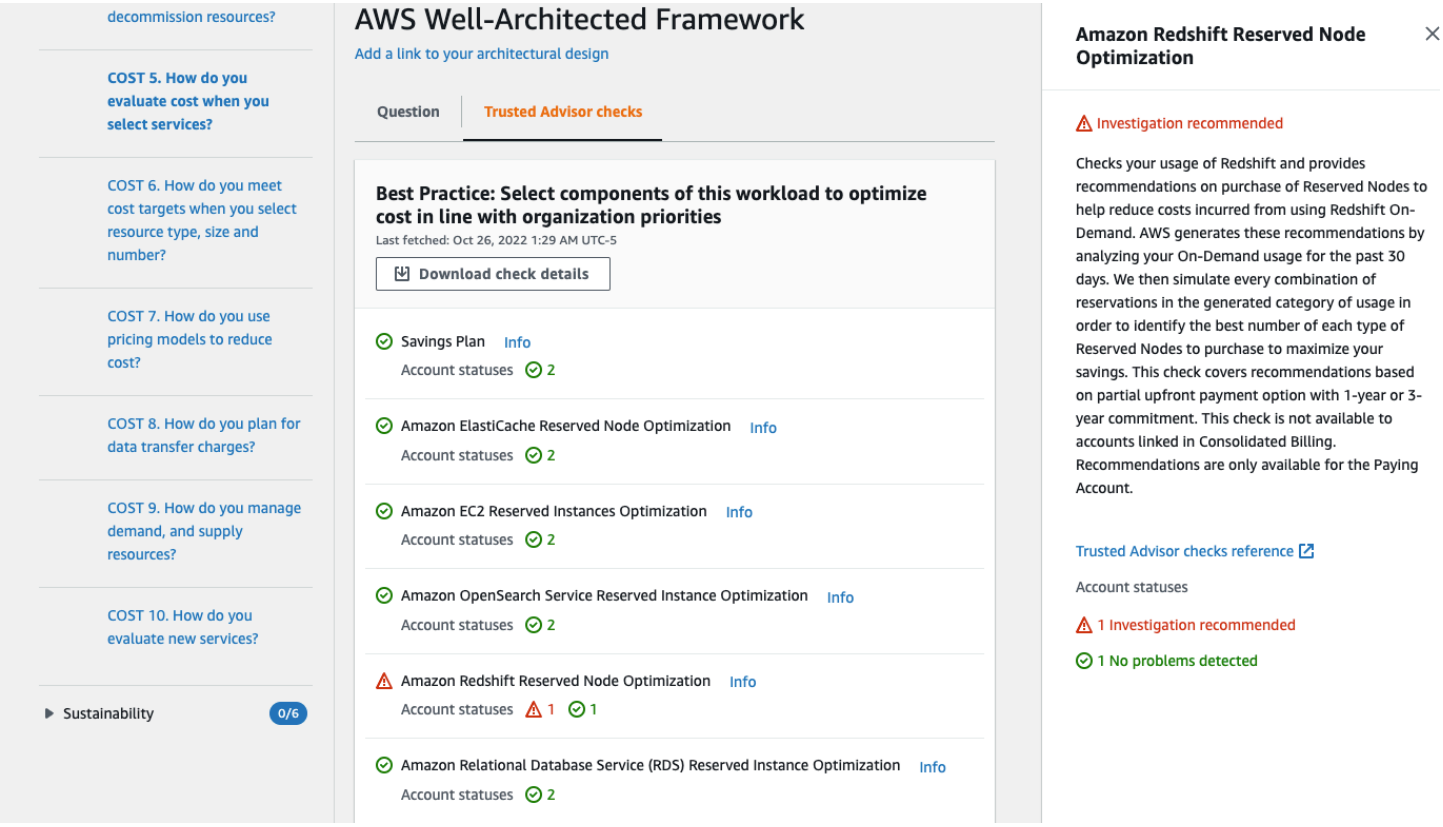
3. Im rechten Bereich werden zusätzliche Informationen und nützliche Ressourcen angezeigt. Wählen Sie Einen Experten fragen aus, um auf die AWS-re:Post-Community für AWS Well-Architected zuzugreifen. In dieser Community kannst du Fragen zum Entwerfen, Erstellen, Bereitstellen und Ausführen von Workloads in AWS stellen.

Trusted Advisor-Überprüfungen für Ihren Workload anzeigen

Wenn Trusted Advisor für Ihren Workload aktiviert ist, wird die Registerkarte Trusted Advisor-Überprüfungen neben Frage angezeigt. Wenn für die bewährte Methode Überprüfungen verfügbar sind, wird nach der Auswahl der Frage die Benachrichtigung angezeigt, dass Trusted Advisor-Überprüfungen verfügbar sind. Wenn Sie Überprüfungen anzeigen auswählen, gelangen Sie zur Registerkarte Trusted Advisor-Überprüfungen.



Auf der Registerkarte Trusted Advisor-Überprüfungen können Sie detailliertere Informationen zu den Überprüfungen bewährter Methoden in Trusted Advisor anzeigen, Links zur Trusted Advisor-Dokumentation im Bereich Hilferessourcen anzeigen oder Überprüfungsdetails herunterladen. So erhalten Sie einen Bericht zur Überprüfung und zum Status von Trusted Advisor für jede bewährte Methode in einer CSV-Datei.



Die Überprüfungskategorien von Trusted Advisor werden als farbige Symbole angezeigt. Die Zahl neben jedem Symbol gibt die Anzahl der Konten mit diesem Status an.

- Empfohlene Aktion (Rot) – Trusted Advisorempfiehlt eine Aktion für die Prüfung.
- Empfohlene Untersuchung (Gelb) – Trusted Advisor stellt ein mögliches Problem bei der Prüfung fest.
- Keine Probleme festgestellt (Grün) – Trusted Advisor keine Probleme bei der Prüfung feststellt.
- Ausgeschlossene Elemente (Grau) – Die Anzahl der Prüfungen, bei denen Elemente ausgeschlossen wurden, z. B. Ressourcen, die bei einer Prüfung nicht berücksichtigt werden sollen.

Weitere Informationen zu den Überprüfungen, die Trusted Advisor bereitstellt, finden Sie unter Überprüfungskategorien anzeigen im Support-Benutzerhandbuch.

Wenn Sie neben jeder Trusted Advisor-Überprüfung auf den Link Info klicken, werden im Bereich Hilferessourcen Informationen zur Überprüfung angezeigt. Weitere Informationen finden Sie unter AWS Trusted Advisor-Überprüfungsreferenz im Support-Benutzerhandbuch.

Einen Meilenstein für einen Workload in AWS WA Tool speichern

Sie können einen Meilenstein für einen Workload jederzeit speichern. Ein Meilenstein erfasst den aktuellen Status des Workloads.

So speichern Sie einen Meilenstein

1. Wählen Sie auf der Detailseite des Workloads Save milestone (Meilenstein speichern) aus.
2. Geben Sie im Feld Milestone name (Name des Meilensteins) einen Namen für den Meilenstein ein.

   > **Note**
   >
   > Der Name muss zwischen 3 und 100 Zeichen lang sein. Mindestens drei Zeichen dürfen keine Leerzeichen sein. Einem Workload zugeordnete Meilensteinnamen müssen eindeutig sein. Leerzeichen und Groß-/Kleinschreibung werden ignoriert, wenn auf Eindeutigkeit geprüft wird.

3. Wählen Sie Save (Speichern) aus.

Nach dem Speichern eines Meilensteins können Sie die Daten des Workloads, die in diesem Meilenstein erfasst wurden, nicht mehr ändern.

Weitere Informationen finden Sie unter Meilensteine.

Tutorial: Einen AWS Well-Architected Tool Workload dokumentieren

Dieses Tutorial beschreibt die Verwendung AWS Well-Architected Tool zur Dokumentation und Messung einer Arbeitslast. Dieses Beispiel veranschaulicht Schritt für Schritt, wie ein Workload für eine Einzelhandels-E-Commerce-Website definiert und dokumentiert wird.

Themen

Schritt 1: Definieren Sie einen Workload

Sie beginnen mit der Definition eines Workloads. Es gibt zwei Möglichkeiten, einen Workload zu definieren. In diesem Tutorial definieren wir einen Workload nicht anhand einer Bewertungsvorlage. Weitere Informationen zur Definition eines Workloads anhand einer Bewertungsvorlage finden Sie unterthe section called “Definieren Sie einen Workload”.

So definieren Sie einen Workload

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.

   > **Note**
   >
   > Der Benutzer, der den Workload-Status dokumentiert, muss über volle Zugriffsberechtigungen für verfügen AWS WA Tool.

2. Wählen Sie im Abschnitt Define a workload (Einen Workload definieren) die Option Define workload (Workload definieren) aus.
3. Im Feld Name geben Sie **`Retail Website - North America`** als Namen für den Workload ein.
4. Im Feld Description (Beschreibung) geben Sie eine Beschreibung für den Workload ein.

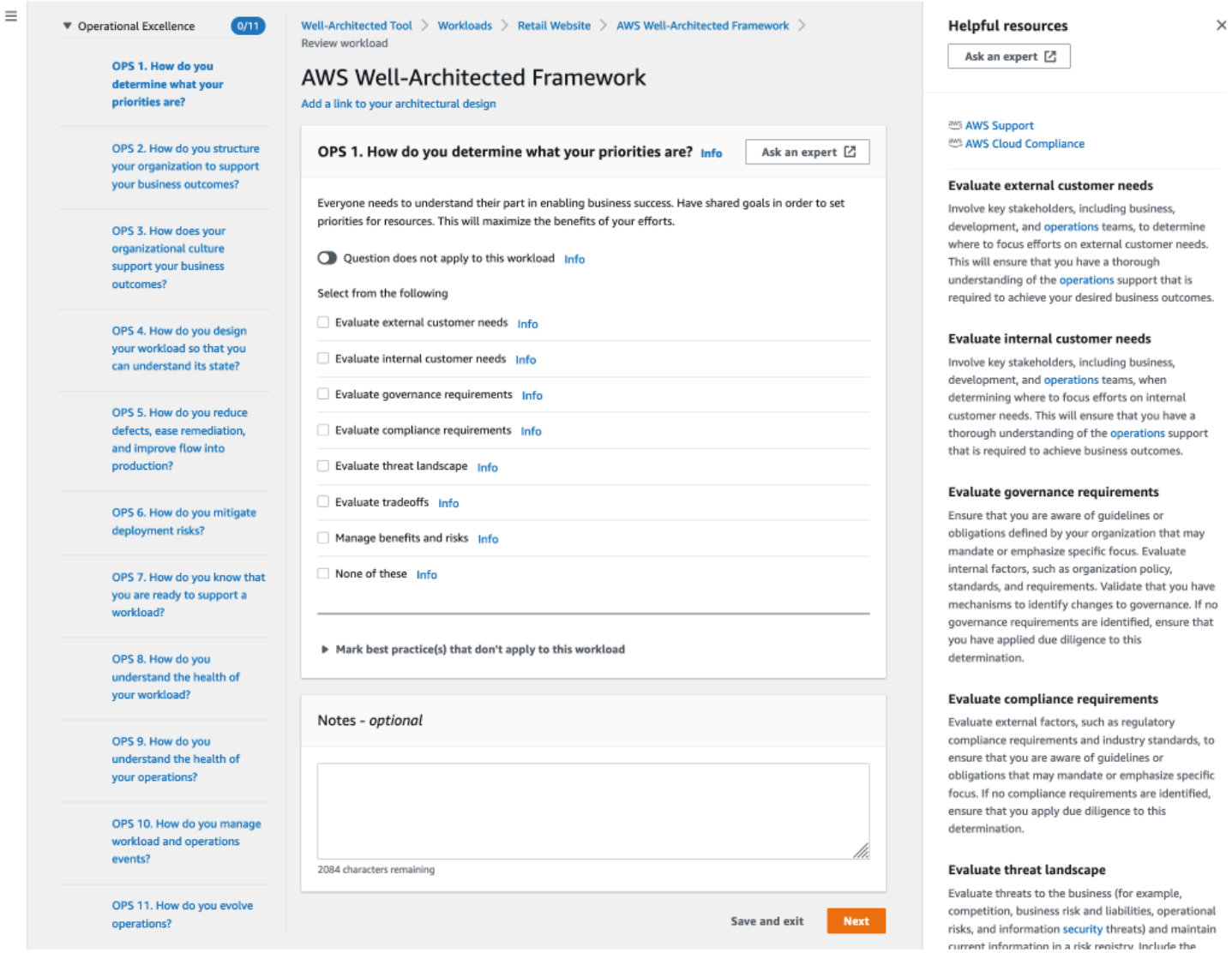
5. Geben Sie im Feld Eigentümer der Überprüfung den Namen der Person ein, die für den Workload-Überprüfungsprozess verantwortlich ist.
6. Geben Sie im Feld Umgebung an, dass sich der Workload in einer Produktionsumgebung befindet.
7. Unser Workload wird AWS sowohl in unserem lokalen Rechenzentrum als auch in unserem lokalen Rechenzentrum ausgeführt:
    a. Wählen Sie AWS-Regionendie beiden Regionen in Nordamerika aus, in denen der Workload ausgeführt wird.
    b. Wählen Sie außerdem AWS Nicht-Regionen aus und geben Sie einen Namen für das lokale Rechenzentrum ein.
8. Das IDs Feld Konto ist optional. Ordnen Sie diesem AWS-Konten Workload keine zu.
9. Das Anwendungsfeld ist optional. Geben Sie keine Anwendung ARN für diesen Workload ein.
10. Das Feld Architekturdiagramm ist optional. Ordnen Sie dieser Arbeitslast kein Architekturdiagramm zu.
11. Die Felder Industry type (Branchenart) und Industry (Branche) sind optional und werden für diesen Workload nicht angegeben.
12. Der Abschnitt Trusted Advisor ist optional. Aktivieren Sie den Trusted Advisor Support für diesen Workload nicht.
13. Der Jira-Abschnitt ist optional. Überschreiben Sie die Einstellungen auf Kontoebene im Jira-Bereich für diesen Workload nicht.
14. Wenden Sie in diesem Beispiel keine Tags auf den Workload an. Wählen Sie Weiter.
15. Der Schritt Profil anwenden ist optional. Wenden Sie kein Profil für diesen Workload an. Wählen Sie Weiter.
16. Wenden Sie für dieses Beispiel die Linse AWS Well-Architected Framework an, die automatisch ausgewählt wird. Wählen Sie Define workload (Workload definieren) aus, um diese Werte zu speichern und den Workload zu definieren.
17. Nachdem der Workload definiert wurde, wählen Sie Start review (Überprüfung starten) aus, um mit dem Dokumentieren des Workload-Status zu beginnen.

Schritt 2: Dokumentieren Sie den Workload-Status

Um den Stand der Arbeitslast zu dokumentieren, werden Ihnen Fragen zum ausgewählten Objektiv gestellt, die die Säulen des AWS Well-Architected Framework umfassen: betriebliche Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz, Kostenoptimierung und Nachhaltigkeit.

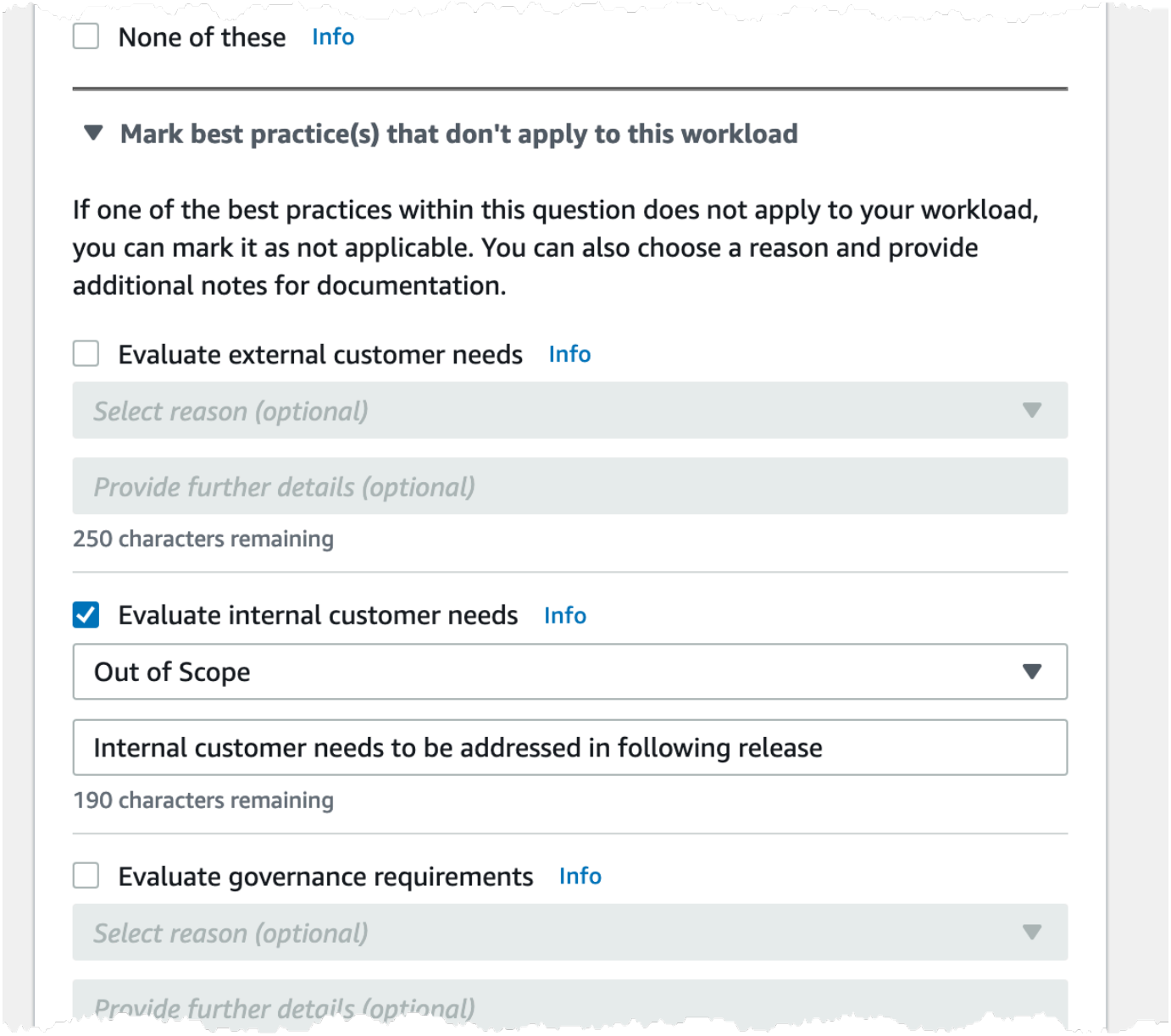
Wählen Sie für jede Frage die bewährten Methoden, die Sie befolgen, aus der bereitgestellten Liste aus. Wenn Sie Details zu einer bewährten Methode erhalten möchten, wählen Sie Info aus und zeigen Sie die zusätzlichen Informationen und Ressourcen im rechten Bereich an.

Wählen Sie Fragen Sie einen Experten, um Zugang zur AWS re:POST-Community zu erhalten, die Well-Architected gewidmet AWS ist. In dieser Community kannst du Fragen zum Entwerfen, Erstellen, Bereitstellen und Betreiben von Workloads stellen. AWS



1. Wählen Sie Next (Weiter) aus, um mit der nächsten Frage fortzufahren. Sie können über den linken Bereich zu einer anderen Frage in der gleichen Säule oder zu einer Frage in einer anderen Säule navigieren.
2. Wenn Sie „Frage gilt nicht für diesen Workload“ oder „Keine davon“ auswählen, AWS empfiehlt es sich, den Grund im Feld „Hinweise“ anzugeben. Diese Notizen werden als Teil des Workload-Berichts hinzugefügt und können hilfreich sein, wenn zukünftige Änderungen am Workload vorgenommen werden.

> **Note**
>
> Optional können Sie eine oder mehrere individuelle bewährte Methoden als nicht zutreffend markieren. Wählen Sie Bewährte Verfahren markieren, die für diesen Workload nicht zutreffen, und wählen Sie die bewährte Methode aus, die nicht zutrifft. Sie können optional einen Grund auswählen und zusätzliche Details angeben. Wiederholen Sie den Vorgang für jede bewährte Methode, die nicht zutrifft.



> **Note**
>
> Sie können diesen Vorgang jederzeit unterbrechen, indem Sie Speichern und beenden wählen. Um den Vorgang zu einem späteren Zeitpunkt fortzusetzen, öffnen Sie die AWS WA Tool Konsole und wählen im linken Navigationsbereich Workloads aus.

3. Wählen Sie den Namen des Workloads aus, um die Seite mit den Workload-Details zu öffnen.
4. Wählen Sie Continue review (Überprüfung fortsetzen) aus und navigieren Sie dann zu dem Ort, an dem Sie aufgehört haben.

5. Nachdem Sie alle Fragen abgeschlossen haben, wird eine Übersichtsseite für den Workload angezeigt. Sie können diese Details jetzt überprüfen oder zu einem späteren Zeitpunkt dorthin navigieren, indem Sie Workloads im linken Navigationsbereich und anschließend den Namen des Workloads auswählen.

Nachdem Sie den Status Ihres Workloads zum ersten Mal dokumentiert haben, sollten Sie einen Meilenstein speichern und einen Workload-Bericht erstellen.

Ein Meilenstein erfasst den aktuellen Status des Workloads und ermöglicht es Ihnen, künftigen Fortschritt zu messen, wenn Sie Änderungen basierend auf Ihrem Verbesserungsplan vornehmen.

Auf der Seite mit den Workload-Details:

1. Wählen Sie im Abschnitt Workload-Übersicht die Schaltfläche Meilenstein speichern.
2. Geben Sie **`Version 1.0 - initial review`** den Namen des Meilensteins ein.
3. Wählen Sie Save (Speichern) aus.
4. Um einen Workload-Bericht zu generieren, wählen Sie das gewünschte Objektiv aus und wählen Sie Bericht generieren. Daraufhin wird eine PDF Datei erstellt. Diese Datei enthält den Status des Workloads, die Anzahl der erkannten Risiken und eine Liste der empfohlenen Verbesserungen.

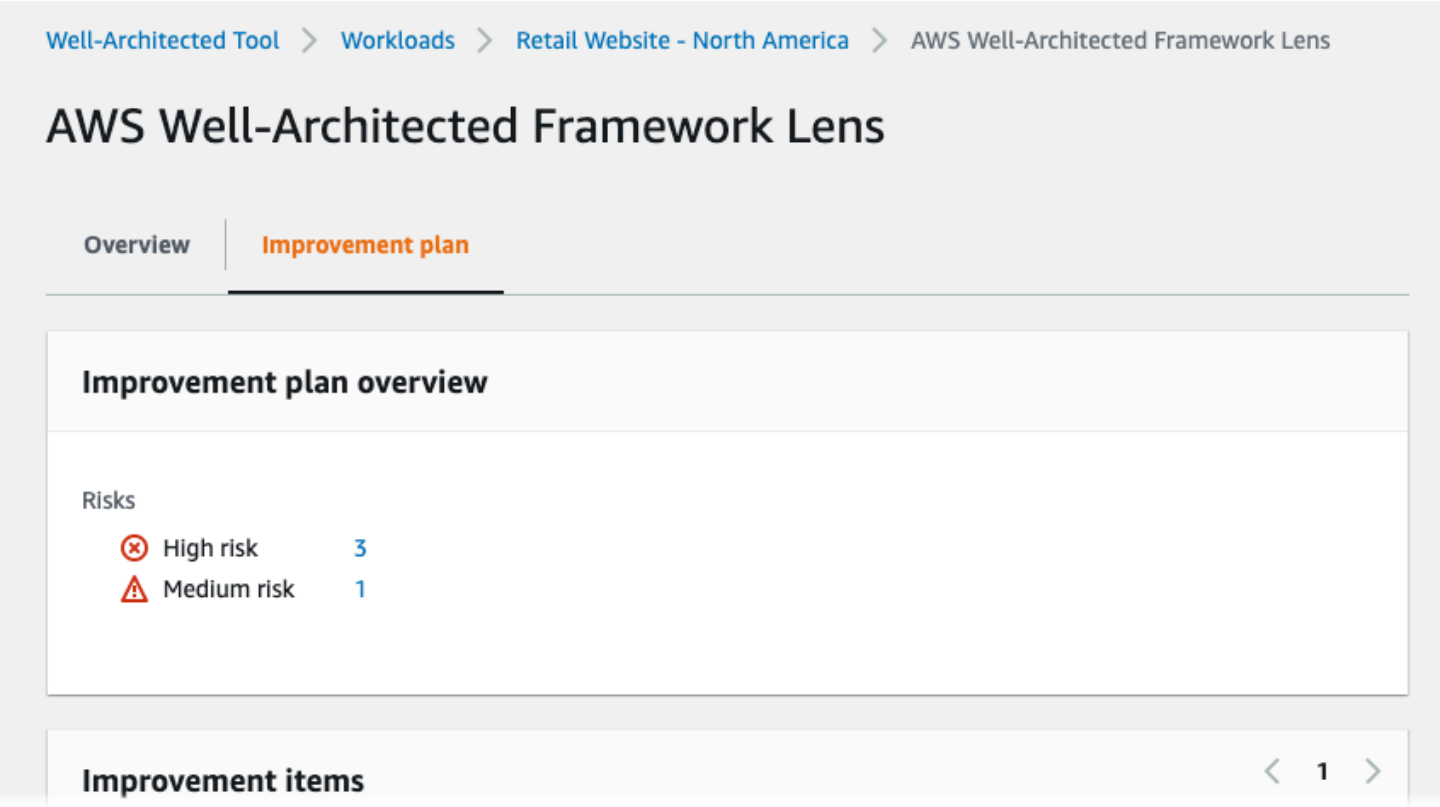
Schritt 3: Überprüfen Sie den Verbesserungsplan

AWS WA Tool Identifiziert auf der Grundlage der ausgewählten Best Practices Bereiche mit hohem und mittlerem Risiko, gemessen am AWS Well-Architected Framework Lens.

So überprüfen Sie den Verbesserungsplan:

1. Wählen Sie auf der Übersichtsseite im Bereich Objektive die Option AWS Well-Architected Framework aus.
2. Wählen Sie dann Improvement plan (Verbesserungsplan) aus.

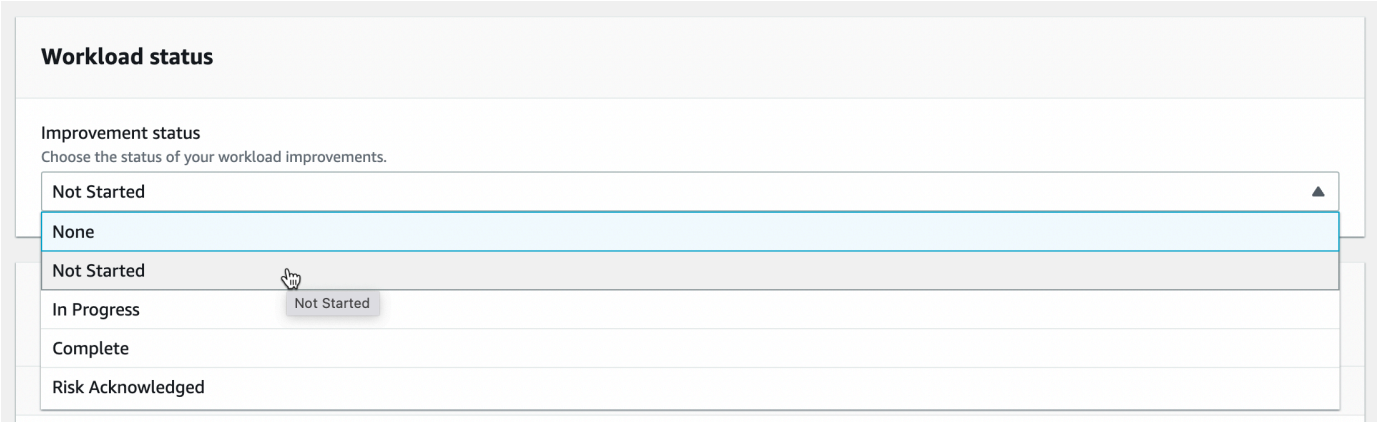
Für diesen speziellen Workload wurden drei Probleme mit hohem Risiko und ein Problem mit mittlerem Risiko durch die AWS Well-Architected Framework Lens identifiziert.



Aktualisieren Sie den Verbesserungsstatus für den Workload, sodass er darauf hinweist, dass mit der Verbesserung des Workloads noch nicht begonnen wurde.

So ändern Sie den Verbesserungsstatus:

1. Klicken Sie im Verbesserungsplan in den Breadcrumbs oben auf der Seite auf den Namen des Workloads (**`Retail Website - North America`**).
2. Klicken Sie auf den Tab Eigenschaften.
3. Navigieren Sie zum Abschnitt Workload-Status und wählen Sie in der Dropdownliste die Option Nicht gestartet aus.



4. Gehen Sie von der Registerkarte Eigenschaften zurück zum Verbesserungsplan, indem Sie auf die Registerkarte Übersicht und dann im Bereich Objektive auf den Link AWS Well-Architected Framework klicken. Klicken Sie dann oben auf der Seite auf den Tab Verbesserungsplan.

Der Abschnitt Improvement items (Verbesserungselemente) zeigt die empfohlenen Verbesserungselemente, die in unserem Workload identifiziert wurden. Die Fragen werden auf der Grundlage der festgelegten Säulenpriorität sortiert, wobei Probleme mit hohem Risiko zuerst aufgelistet werden, gefolgt von Problemen mit mittlerem Risiko.

Erweitern Sie Recommended improvement items (Empfohlene Verbesserungselemente), um die bewährten Methoden für eine Frage anzuzeigen. Jede empfohlene Verbesserungsaktion ist mit einer detaillierten Hilfestellung durch Experten verknüpft, um die identifizierten Risiken zu eliminieren oder zumindest zu verringern.

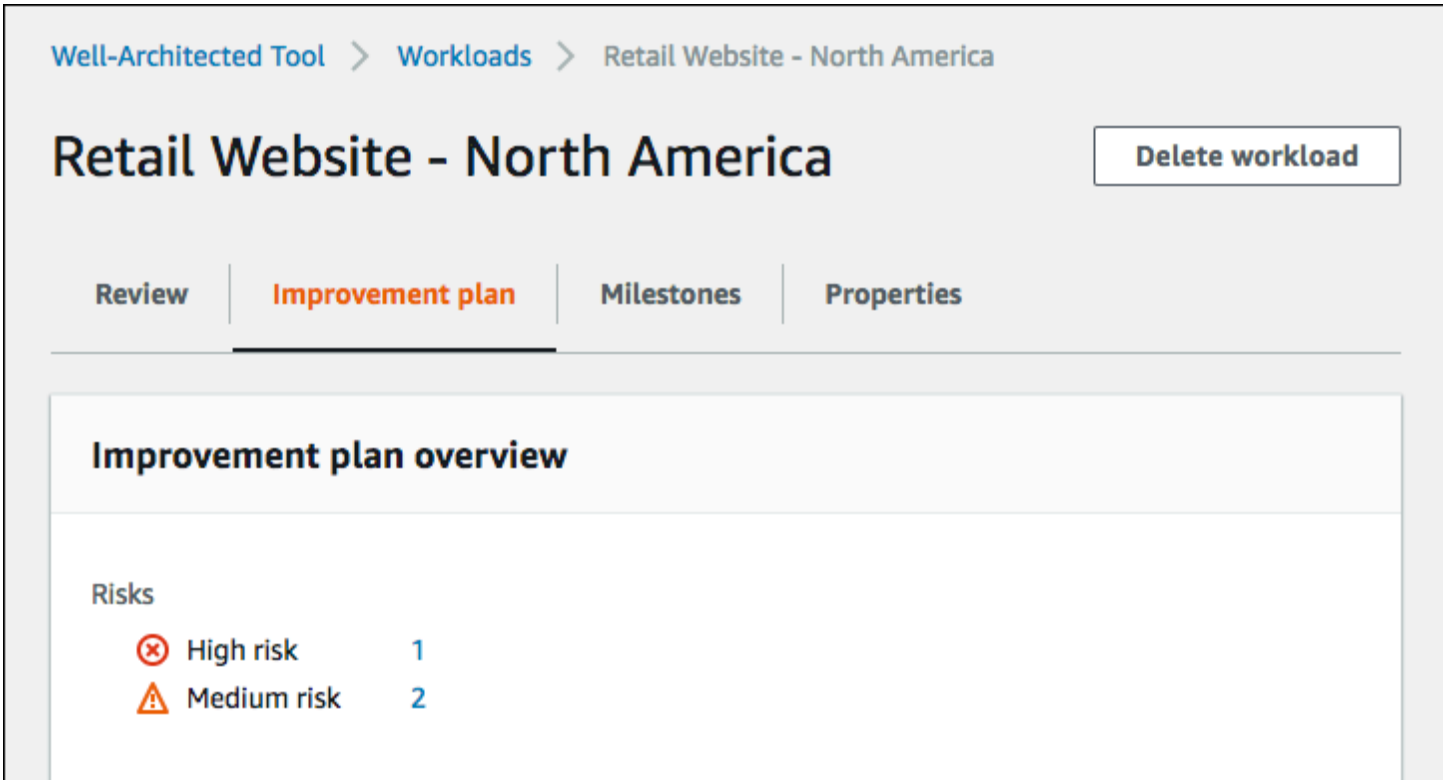
Wenn der Arbeitslast ein Profil zugeordnet ist, wird die Anzahl der priorisierten Risiken im Abschnitt Übersicht über den Verbesserungsplan angezeigt. Sie können die Liste der Verbesserungselemente filtern, indem Sie nach Profil priorisiert auswählen. In der Liste der Verbesserungselemente wird die Bezeichnung „Priorisiert“ angezeigt.

Schritt 4: Verbesserungen vornehmen und Fortschritte messen

Im Rahmen dieses Verbesserungsplans wurde eines der mit hohem Risiko verbundenen Probleme behoben, indem die Arbeitslast um Amazon CloudWatch und AWS Auto Scaling Support erweitert wurde.

Aus dem Bereich Verbesserungsvorschläge:

1. Wählen Sie die entsprechende Frage aus und aktualisieren Sie die ausgewählten Best Practices, um die Änderungen widerzuspiegeln. Es werden Notizen hinzugefügt, um die Verbesserungen aufzuzeichnen.
2. Wählen Sie dann Speichern und beenden, um den Status des Workloads zu aktualisieren.
3. Nachdem Sie Änderungen vorgenommen haben, können Sie zum Verbesserungsplan zurückkehren und sehen, welche Auswirkungen diese Änderungen auf den Workload hatten. In diesem Beispiel haben diese Maßnahmen das Risikoprofil verbessert und die Anzahl der Probleme mit hohem Risiko von drei auf nur eines reduziert.



Sie können an diesem Punkt einen Meilenstein speichern und dann zu Meilensteine wechseln, um zu sehen, wie sich der Workload verbessert hat.

Workloads

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder einen Backend-Prozess.

Eine Arbeitslast kann aus einer Teilmenge von Ressourcen in einer einzigen AWS-Konto oder aus einer Sammlung mehrerer Ressourcen bestehen, die sich über mehrere erstrecken. AWS-Konten Ein kleines Unternehmen hat möglicherweise nur wenige Workloads, während ein großes Unternehmen Tausende haben kann.

Die Seite Workloads, die über die linke Navigation verfügbar ist, enthält Informationen zu Ihren Workloads und zu allen Workloads, die für Sie freigegeben wurden.

Für jede Workload werden die folgenden Informationen angezeigt:

Name

Name der Workload.

Eigentümer

Die AWS-Konto ID, der der Workload gehört.

Beantwortete Fragen

Die Anzahl der beantworteten Fragen.

Hohe Risiken

Die Anzahl der identifizierten Probleme mit hohem Risiko (HRIs).

Mittlere Risiken

Die Anzahl der identifizierten Probleme mit mittlerem Risiko (MRIs).

Verbesserungsstatus

Der Verbesserungsstatus, den Sie für den Workload festgelegt haben:

- None
- Nicht begonnen
- In Bearbeitung
- Complete
- Risiko bestätigt

Letzte Aktualisierung

Datum und die Uhrzeit, zu dem/der der Workload zuletzt aktualisiert wurde.

Nachdem Sie einen Workload in der Liste ausgewählt haben:

- Um die Details der Workload zu überprüfen, wählen Sie View details (Details anzeigen) aus.
- Wählen Sie Edit (Bearbeiten) aus, um die Eigenschaften der Workload zu ändern.
- Um die gemeinsame Nutzung der Arbeitslast mit anderen AWS-Konten Benutzern oder Organisationseinheiten (OUs) zu verwalten, wählen Sie Details anzeigen und dann Freigaben aus. AWS Organizations
- Wählen Sie Delete (Löschen) aus, um die Workload und alle zugehörigen Meilensteine zu löschen. Nur der Besitzer des Workloads kann diesen löschen.

> **Warning**
>
> Das Löschen eines Workloads kann nicht rückgängig gemacht werden. Alle Daten, die dem Workload zuordnet sind, werden gelöscht.

Probleme mit hohem Risiko (HRIs) und Probleme mit mittlerem Risiko (MRIs)

Probleme mit hohem Risiko (HRIs), die in der identifiziert wurden, AWS Well-Architected Tool sind architektonische und betriebliche Entscheidungen, von denen festgestellt AWS wurde, dass sie erhebliche negative Auswirkungen auf ein Unternehmen haben könnten. Diese HRIs können sich auf organisatorische Abläufe, Vermögenswerte und Einzelpersonen auswirken. Probleme mit mittlerem Risiko (MRIs) könnten sich ebenfalls negativ auf das Geschäft auswirken, jedoch in geringerem Maße. Diese Probleme basieren auf Ihren Antworten in AWS Well-Architected Tool. Die entsprechenden bewährten Verfahren werden von AWS Kunden AWS und Kunden häufig angewendet. Diese Best Practices sind die Leitlinien, die durch das AWS Well-Architected Framework und die Objektive definiert werden.

> **Note**
>
> Dies sind nur Richtlinien. Kunden sollten die möglichen Auswirkungen einer eventuellen Nichteinführung der bewährten Methoden auf ihr Geschäft bewerten und messen. Wenn

es bestimmte technische oder geschäftliche Gründe gibt, die die Anwendung einer bewährten Methode auf die Arbeitslast verhindern, ist das Risiko möglicherweise geringer als angegeben. AWS schlägt vor, dass Kunden diese Gründe und ihre Auswirkungen auf die bewährten Verfahren in den Arbeitsauslastungsnotizen dokumentieren. Für alle identifizierten HRIs und AWS schlägt vorMRIs, dass Kunden die bewährte Methode anwenden, wie sie in der definiert ist AWS Well-Architected Tool. Wenn die bewährten Methode implementiert ist, geben Sie an, dass das Problem behoben wurde, indem Sie die bewährte Methode in AWS Well-Architected Tool als erfüllt kennzeichnen. Falls Kunden sich dafür entscheiden, das bewährte Verfahren nicht umzusetzen, AWS schlägt vor, dass sie die entsprechende Genehmigung auf Unternehmensebene und die Gründe für die Nichtumsetzung dokumentieren.

Definieren Sie einen Workload in AWS Well-Architected Tool

Es gibt zwei Möglichkeiten, einen Workload zu definieren. Auf der Seite Workloads in können AWS WA Tool Sie einen Workload ohne Vorlage definieren. Oder Sie können auf der Seite Vorlagen überprüfen eine vorhandene Bewertungsvorlage verwenden oder eine neue Vorlage erstellen, um einen Workload zu definieren.

Um einen Workload auf der Workloads-Seite zu definieren

1. Wählen Sie im linken Navigationsbereich Workloads aus.
2. Wählen Sie das Drop-down-Menü Workload definieren aus.
3. Wählen Sie Define workload (Workload definieren) aus. Oder, wenn Sie eine Bewertungsvorlage erstellt haben und daraus einen Workload definieren möchten, wählen Sie „Aus Bewertungsvorlage definieren“.
4. Folgen Sie den Anweisungen unterthe section called “Einen Workload definieren”, um die Workload-Eigenschaften anzugeben, oder wenden Sie (optional) Profile und Objektive an.

So definieren Sie einen Workload auf der Seite „Vorlagen überprüfen“

1. Wählen Sie im linken Navigationsbereich Vorlagen überprüfen aus.
2. Wählen Sie den Namen einer vorhandenen Bewertungsvorlage aus, oder folgen Sie den Anweisungen unter, the section called “Erstellen Sie eine Bewertungsvorlage” um eine neue Bewertungsvorlage zu erstellen.

3. Wählen Sie „Arbeitslast aus Vorlage definieren“.
4. Folgen Sie den Anweisungen unterthe section called “Definieren eines Workloads anhand einer Vorlage”, um den Workload anhand Ihrer Bewertungsvorlage zu erstellen.

Sehen Sie sich einen Workload an in AWS Well-Architected Tool

Sie können die Details der Workloads, die Sie besitzen, und Workloads, die für Sie freigegeben wurden, anzeigen.

So zeigen Sie einen Workload an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie den Workload aus, um ihn auf ein der folgenden Arten anzuzeigen:
   - Wählen Sie den Namen des Workloads aus.
   - Wählen Sie den Workload und Details ansehen aus.

Die Detailseite des Workloads wird angezeigt.

> **Note**
>
> Das Pflichtfeld Review owner (Prüfeigentümer) wurde hinzugefügt, damit Sie die primäre Person oder Gruppe, die für den Überprüfungsprozess verantwortlich ist, leicht identifizieren können.
> Wenn Sie zum ersten Mal einen Workload anzeigen, der definiert wurde, bevor dieses Feld hinzugefügt wurde, werden Sie über diese Änderung benachrichtigt. Wählen Sie Edit (Bearbeiten), um das Feld Review owner (Prüfeigentümer) festzulegen. Es ist keine weitere Aktion erforderlich.
> Wählen Sie Acknowledge (Bestätigen), um das Festlegen des Feldes Review owner (Prüfeigentümer) aufzuschieben. In den kommenden 60 Tagen wird ein Banner angezeigt, um Sie daran zu erinnern, dass das Feld leer ist. Um das Banner zu entfernen, bearbeiten Sie Ihren Workload und geben Sie einen Review owner (Prüfeigentümer)an.
> Wenn Sie das Feld nicht bis zum angegebenen Datum festlegen, ist Ihr Zugriff auf den Workload eingeschränkt. Sie können den Workload weiterhin anzeigen und löschen, aber Sie können sie nicht bearbeiten, außer um das Feld Review owner (Prüfeigentümer) festzulegen.

Der freigegebene Zugriff auf den Workload wird nicht beeinträchtigt, während Ihr Zugriff eingeschränkt ist.

Bearbeiten Sie einen Workload in AWS Well-Architected Tool

Sie können die Details eines Workloads bearbeiten, den Sie besitzen.

So bearbeiten Sie einen Workload

1. Melden Sie sich bei an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie den Workload, den Sie bearbeiten möchten, aus und klicken Sie auf Edit (Bearbeiten).
4. Nehmen Sie Änderungen am Workload vor.

   Eine Beschreibung der einzelnen Felder finden Sie unter Einen Workload in AWS WA Tool definieren.

   > **Note**
   >
   > Wenn Sie einen vorhandenen Workload aktualisieren, können Sie Activate Trusted Advisor wählen. Dadurch wird automatisch die IAM Rolle für den Workload-Besitzer erstellt. Die Besitzer der zugehörigen Konten für Workloads mit Trusted Advisor aktiviertem Status müssen eine Rolle in IAM erstellen. Details hierzu finden Sie unter the section called “Trusted Advisor in IAM aktivieren”.

5. Wählen Sie Save (Speichern) aus, um Ihre Änderungen am Workload zu speichern.

   Wenn ein erforderliches Feld leer oder ein angegebener Wert nicht gültig ist, müssen Sie zuerst das Problem beheben, bevor Aktualisierungen am Workload gespeichert werden.

Teilen Sie sich einen Workload in AWS Well-Architected Tool

Sie können einen Workload, der Ihnen gehört AWS-Konten, mit anderen Benutzern, einer Organisation und Organisationseinheiten (OUs) in derselben Einheit teilen AWS-Region.

> **Note**
>
> Sie können Workloads nur innerhalb derselben AWS-Region Einheit teilen. Wenn der Empfänger ein Workload mit einem anderen teilt AWS-Konto, kann er die Einladung zum Teilen nicht annehmen, wenn er nicht über die `wellarchitected:UpdateShareInvitation` entsprechende Genehmigung verfügt. Beispiele the section called “Stellt Zugriff auf AWS WA Tool bereit.” für Berechtigungsrichtlinien finden Sie unter.

Um eine Arbeitslast mit anderen Benutzern AWS-Konten zu teilen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie einen Workload, den Sie besitzen, auf eine der folgenden Arten aus:
   - Wählen Sie den Namen des Workloads aus.
   - Wählen Sie den Workload und Details ansehen aus.
4. Wählen Sie Shares (Freigaben). Wählen Sie dann Create and Create and Create Shares to users or accounts, um eine Workload-Einladung zu erstellen.
5. Geben Sie die 12-stellige AWS-Konto ID oder die ARN des Benutzers ein, mit dem Sie den Workload teilen möchten.
6. Wählen Sie die Berechtigung aus, die Sie erteilen möchten.

   Read-Only (Schreibgeschützt)

   Bietet schreibgeschützten Zugriff auf den Workload.

   Beitragender

   Bietet Aktualisierungszugriff auf Antworten und ihre Notizen sowie schreibgeschützten Zugriff auf den restlichen Workload.
7. Wählen Sie Erstellen, um eine Workload-Einladung an den angegebenen Benutzer AWS-Konto oder zu senden.

Wenn die Workload-Einladung nicht innerhalb von sieben Tagen angenommen wird, ist die Einladung automatisch abgelaufen.

Wenn AWS-Konto sowohl ein Benutzer als auch die Benutzer Workload-Einladungen haben, wird die Workload-Einladung mit der höchsten Berechtigungsebene auf den Benutzer angewendet.

> **Important**
>
> Bevor Sie einen Workload mit einer Organisation oder Organisationseinheiten (OUs) teilen können, müssen Sie AWS Organizations den Zugriff aktivieren.

Um einen Workload mit Ihrer Organisation zu teilen oder OUs

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie einen Workload, den Sie besitzen, auf eine der folgenden Arten aus:
   - Wählen Sie den Namen des Workloads aus.
   - Wählen Sie den Workload und Details ansehen aus.
4. Wählen Sie Shares (Freigaben). Wählen Sie dann Create and Create Shares to Organizations.
5. Wählen Sie auf der Seite Workload-Sharing erstellen aus, ob Sie der gesamten Organisation oder einer oder mehreren Organisationen Berechtigungen gewähren möchtenOUs.
6. Wählen Sie die Berechtigung aus, die Sie erteilen möchten.

   Read-Only (Schreibgeschützt)

   Bietet schreibgeschützten Zugriff auf den Workload.

   Beitragender

   Bietet Aktualisierungszugriff auf Antworten und ihre Notizen sowie schreibgeschützten Zugriff auf den restlichen Workload.
7. Wählen Sie Erstellen, um den Workload gemeinsam zu nutzen.

Um zu sehen, wer einen gemeinsamen Zugriff auf einen Workload hat, wählen Sie Shares (Freigaben) auf der Seite Details zur Arbeitslast finden Sie unter AWS Well-Architected Tool.

Um zu verhindern, dass eine Entity Workloads löscht, fügen Sie eine Richtlinie an, die `wellarchitected:CreateWorkloadShare`-Aktionen verweigert.

Sie können benutzerdefinierte Objektive, die Sie besitzen AWS-Konten, auch mit anderen Benutzern, Ihrer Organisation und OUs innerhalb derselben teilen AWS-Region. Einzelheiten finden Sie unterFreigeben einer benutzerdefinierten Linse in AWS WA Tool.

Überlegungen bei der gemeinsamen Nutzung von AWS Well-Architected Tool Workloads

Ein Workload kann mit bis zu 20 verschiedenen AWS-Konten AND-Benutzern geteilt werden. Ein Workload kann nur mit Accounts und Benutzern geteilt werden, die sich im selben AWS-Region Workload befinden.

Um einen Workload in einer Region zu teilen, die nach dem 20. März 2019 eingeführt wurde, AWS-Konto müssen sowohl Sie als auch der gemeinsam genutzte Workload die Region in der aktivieren AWS Management Console. Weitere Informationen finden Sie unter AWS Globale Infrastruktur.

Sie können einen Workload mit einem AWS-Konto, einzelnen Benutzern in einem Konto oder mit beiden teilen. Wenn Sie einen Workload mit einem teilen AWS-Konto, erhalten alle Benutzer in diesem Konto Zugriff auf den Workload. Wenn nur bestimmte Benutzer in einem Konto Zugriff benötigen, befolgen Sie die bewährte Methode der Gewährung der geringsten Rechte und teilen Sie die Arbeitslast einzeln mit diesen Benutzern.

Wenn AWS-Konto sowohl ein Benutzer als auch ein Benutzer im Konto Workload-Einladungen haben, bestimmt die Workload-Einladung mit der höchsten Berechtigungsebene die Berechtigungen des Benutzers für den Workload. Wenn Sie die Workload-Einladung für den Benutzer löschen, wird der Zugriff des Benutzers durch die Workload-Einladung für bestimmt AWS-Konto. Löschen Sie beide Workload-Einladungen, um den Zugriff des Benutzers auf den Workload zu entfernen.

Bevor Sie einen Workload mit einer Organisation oder einer oder mehreren Organisationseinheiten (OUs) teilen können, müssen Sie AWS Organizations den Zugriff aktivieren.

Wenn Sie einen Workload sowohl mit einer Organisation als auch mit einer oder mehreren Organisationen teilenOUs, bestimmt die Workload-Einladung mit der höchsten Berechtigungsebene die Zugriffsrechte des Accounts für den Workload.

Um die AWS Organizations gemeinsame Nutzung zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.

3. Wählen Sie AWS Organizations Support aktivieren aus.
4. Wählen Sie Save settings (Einstellungen speichern).

Löschen Sie den gemeinsamen Zugriff in AWS Well-Architected Tool

Sie können eine Workload-Einladung löschen. Durch das Löschen einer Workload-Einladung der freigegebene Zugriff auf den Workload entfernt.

So löschen Sie den freigegebenen Zugriff auf einen Workload:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie den Workload auf eine der folgenden Arten aus:
   - Wählen Sie den Namen des Workloads aus.
   - Wählen Sie den Workload und Details ansehen aus.
4. Wählen Sie Shares (Freigaben).
5. Wählen Sie die zu löschende Workload-Einladung aus, und wählen Sie Delete (Löschen).
6. Wählen Sie zur Bestätigung Delete.

Wenn ein Benutzer und die des Benutzers Workload-Einladungen AWS-Konto haben, müssen Sie beide Workload-Einladungen löschen, um dem Benutzer die Berechtigung für den Workload zu entziehen.

Ändern Sie den gemeinsamen Zugriff in AWS Well-Architected Tool

Sie können eine ausstehende oder akzeptierte Workload-Einladung ändern.

So ändern Sie den freigegebenen Zugriff auf einen Workload:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie einen Workload, den Sie besitzen, auf eine der folgenden Arten aus:
   - Wählen Sie den Namen des Workloads aus.

- Wählen Sie den Workload und Details ansehen aus.

4. Wählen Sie Shares (Freigaben).
5. Wählen Sie die zu ändernde Workload-Einladung aus, und wählen Sie Edit (Bearbeiten).
6. Wählen Sie die neue Berechtigung aus, die Sie dem Benutzer AWS-Konto oder gewähren möchten.

   Read-Only (Schreibgeschützt)

   Bietet schreibgeschützten Zugriff auf den Workload.

   Beitragender

   Bietet Aktualisierungszugriff auf Antworten und ihre Notizen sowie schreibgeschützten Zugriff auf den restlichen Workload.
7. Wählen Sie Save (Speichern) aus.

Wenn die geänderte Workload-Einladung nicht innerhalb von sieben Tagen angenommen wird, ist sie automatisch abgelaufen.

Workload-Einladungen annehmen und ablehnen in AWS Well-Architected Tool

Eine Workload-Einladung ist eine Aufforderung, einen Workload gemeinsam zu nutzen, der einem anderen AWS-Konto gehört. Wenn Sie die Workload-Einladung akzeptieren, wird der Workload Ihren Workloads- und Dashboard-Seiten hinzugefügt. Wenn Sie die Workload-Einladung ablehnen, wird sie aus der Workload-Einladungsliste entfernt.

Sie haben sieben Tage Zeit, um eine Workload-Einladung anzunehmen. Wenn Sie die Einladung nicht innerhalb von sieben Tagen annehmen, wird sie automatisch abgelehnt.

> **Note**
>
> Workloads können nur innerhalb desselben AWS-Region Unternehmens gemeinsam genutzt werden.

So können Sie eine Workload-Einladung annehmen oder ablehnen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workload invitations (Workload-Einladungen).
3. Wählen Sie die Workload-Einladung aus, die angenommen oder abgelehnt werden soll.
   - Um die Workload-Einladung anzunehmen, wählen Sie Accept (Akzeptieren).

     Der Workload wird den Seiten Workloads und Dashboard hinzugefügt.
   - Um die Workload-Einladung abzulehnen, wählen Sie Reject (Ablehnen).

     Die Workload-Einladung wird aus der Liste entfernt.

Um den gemeinsamen Zugriff abzulehnen, nachdem eine Workload-Einladung angenommen wurde, wählen Sie auf der Details zur Arbeitslast finden Sie unter AWS Well-Architected Tool Seite für den Workload die Option Freigabe ablehnen aus.

Löschen Sie einen Workload in AWS Well-Architected Tool

Sie können einen Workload löschen, wenn er nicht mehr benötigt wird. Beim Löschen eines Workloads werden alle Daten, die mit dem Workload verknüpft sind, einschließlich Meilensteine und Einladungen für Workloadfreigaben, entfernt. Nur der Besitzer eines Workloads kann diesen löschen.

> **Warning**
>
> Das Löschen eines Workloads kann nicht rückgängig gemacht werden. Alle Daten, die dem Workload zuordnet sind, werden dauerhaft entfernt.

So löschen Sie einen Workload

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie den Workload aus, den Sie löschen möchten, und klicken Sie auf Delete (Löschen).

4. Wählen Sie im Fenster Delete (Löschen) die Option Delete (Löschen) aus, um das Löschen des Workloads und dessen Meilensteine zu bestätigen.

Um zu verhindern, dass eine Entity Workloads löscht, fügen Sie eine Richtlinie an, die `wellarchitected:DeleteWorkload`-Aktionen verweigert.

Generieren Sie einen Workload-Bericht in AWS Well-Architected Tool

Sie können einen Workload-Bericht für eine Linse erstellen. Der Bericht enthält Ihre Antworten auf die Workload-Fragen, Ihre Notizen und die Anzahl der erkannten hohen und mittleren Risiken. Wenn eine Frage ein oder mehrere Risiken identifiziert hat, listet der Verbesserungsplan für diese Frage Maßnahmen auf, die ergriffen werden können, um diese Risiken zu minimieren.

Wenn Ihrem Workload ein Profil zugeordnet ist, werden die Profilübersichtsinformationen und die priorisierten Risiken im Workload-Bericht angezeigt.

Über einen Bericht können Sie Details zu Ihrem Workload an andere Personen weitergeben, die keinen Zugriff auf AWS Well-Architected Tool haben.

So erstellen Sie einen Workload-Bericht

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie die Workload aus und klicken Sie auf View details (Details ansehen).
4. Wählen Sie die Linse aus, für die Sie einen Bericht erstellen möchten, und klicken Sie anschließend auf Generate report (Bericht erstellen).

   Der Bericht wird generiert und Sie können ihn anzeigen oder herunterladen.

Details zur Arbeitslast finden Sie unter AWS Well-Architected Tool

Die Seite „Workload-Details“ enthält Informationen über Ihren Workload, einschließlich der Meilensteine, des Verbesserungsplans und aller Workload-Freigaben. Verwenden Sie die Registerkarten oben auf der Seite, um zu den verschiedenen Detailabschnitten zu navigieren.

Um den Workload zu löschen, wählen Sie Delete workload (Workload löschen). Nur der Besitzer eines Workloads kann diesen löschen.

Um den Zugriff auf einen freigegebenen Workload zu entfernen, wählen Sie Reject share (Freigabe ablehnen).

Themen

Die Registerkarte „ AWS Well-Architected Tool Übersicht“

Wenn Sie einen Workload anfänglich anzeigen, ist die Registerkarte Overview (Übersicht) die erste Information, die angezeigt wird. Diese Registerkarte enthält den Gesamtstatus Ihres Workloads, gefolgt vom Status der einzelnen Linsen.

Wenn Sie nicht alle Fragen abgeschlossen haben, wird ein Banner angezeigt, das Sie daran erinnert, mit der Dokumentation Ihres Workloads zu beginnen oder fortzufahren.

Im Abschnitt Workload overview (Workload-Übersicht) werden der aktuelle Gesamtstatus des Workloads sowie alle eingegebenen Workload notes (Workload-Notizen) angezeigt. Wählen Sie Edit (Bearbeiten) aus, um den Status oder die Notizen zu aktualisieren.

Wählen Sie Save milestone (Meilenstein speichern) aus, um den aktuellen Status des Workloads zu erfassen. Meilensteine sind unveränderlich und können nicht geändert werden, nachdem sie gespeichert wurden.

Um mit der Dokumentation des Workload-Status fortzufahren, wählen Sie Start reviewing (Überprüfung starten) und wählen dann die gewünschte Linse aus.

Die Registerkarte „ AWS Well-Architected Tool Meilensteine“

Wählen Sie die Registerkarte Milestones (Meilensteine) aus, um die Meilensteine für die Workload anzuzeigen.

Nachdem Sie einen Meilenstein ausgewählt haben, klicken Sie auf Bericht erstellen, um den mit dem Meilenstein verknüpften Workload-Bericht zu erstellen. Der Bericht enthält die Antworten auf die

Workload-Fragen, Ihre Notizen und die Anzahl der hohen und mittleren Risiken in dem Workload zum Zeitpunkt der Speicherung des Meilensteins.

Sie können Details über den Status Ihres Workloads zum Zeitpunkt eines bestimmten Meilensteins anzeigen, indem Sie:

- Den Namen des Meilensteins auswählen.
- Den Meilenstein auswählen und auf View milestone (Meilenstein anzeigen) klicken.

Die Registerkarte „ AWS Well-Architected Tool Eigenschaften“

Wählen Sie die Registerkarte Properties (Eigenschaften) aus, um die Eigenschaften für die Workload anzuzeigen. Anfangs sind diese Eigenschaften die Werte, die beim Definieren des Workloads angegeben wurden. Sie können Edit (Bearbeiten) auswählen, um Änderungen vorzunehmen. Nur der Besitzer des Workloads kann Änderungen vornehmen.

Beschreibungen der Eigenschaften finden Sie unter Einen Workload in AWS WA Tool definieren.

Die Registerkarte „ AWS Well-Architected Tool Shares“

Um Ihre Workload-Einladungen anzuzeigen oder zu ändern, wählen Sie die Registerkarte Shares (Freigaben) . Diese Registerkarte wird nur für den Besitzer eines Workloads angezeigt.

Die folgenden Informationen werden für jeden AWS-Konto Benutzer angezeigt, der gemeinsamen Zugriff auf den Workload hat:

Auftraggeber

Die AWS-Konto ID oder der Benutzer ARN mit gemeinsamem Zugriff auf den Workload.

Status

Der Status der Workload-Einladung.

- Ausstehend

  Die Einladung wartet darauf, angenommen oder abgelehnt zu werden. Wenn eine Workload-Einladung nicht innerhalb von sieben Tagen angenommen wird, ist sie automatisch abgelaufen.

- Accepted (Akzeptiert)

  Die Einladung wurde angenommen.

- Rejected (Abgelehnt)

  Die Einladung wurde abgelehnt.
- Expired

  Die Einladung wurde nicht innerhalb von sieben Tagen angenommen oder abgelehnt.

Berechtigung

Die dem Benutzer AWS-Konto oder gewährte Berechtigung.

- Read-Only (Schreibgeschützt)

  Der Prinzipal hat schreibgeschützten Zugriff auf den Workload.
- Beitragender

  Der Prinzipal kann Antworten und ihre Notizen aktualisieren und hat schreibgeschützten Zugriff auf den restlichen Workload.

Berechtigungsdetails

Detaillierte Beschreibung der Berechtigung.

Um den Workload mit einem anderen Benutzer AWS-Konto oder demselben Benutzer zu teilen AWS-Region, wählen Sie Create aus. Ein Workload kann mit bis zu 20 verschiedenen AWS-Konten AND-Benutzern gemeinsam genutzt werden.

Um eine Workload-Einladung zu löschen, wählen Sie die Einladung aus, und wählen Sie Delete (Löschen).

Um eine Workload-Einladung zu ändern, wählen Sie die Einladung aus, und wählen Sie Edit (Bearbeiten).

Verwenden von Linsen in AWS WA Tool

In AWS Well-Architected Tool bieten Ihnen Linsen die Möglichkeit, Ihre Architekturen konsequent an bewährten Methoden zu messen und Verbesserungspotenzial zu identifizieren. Die AWSAWS Well-Architected Framework-Linse wird automatisch angewendet, wenn eine Workload definiert wird.

Bei einer Workload können eine oder mehrere Linsen eingesetzt werden. Jede Linse verfügt über einen eigenen Reihe von Fragen, bewährten Verfahren, Notizen und einen Verbesserungsplan.

Es gibt zwei Arten von Linsen , die für Ihre Workloads verwendet werden können: Linsen aus dem Lens-Katalog und benutzerdefinierte Linsen.

- Lens-Katalog: Offizielle Linsen, die von AWS erstellt und gewartet werden. Der Lens-Katalog steht allen Benutzern zur Verfügung und erfordert keine zusätzliche Installation.
- Benutzerdefinierte Linsen: Von Benutzern definierte Linden, bei denen es sich nicht um offizielle AWS-Inhalte handelt. Sie können benutzerdefinierte Linsen mit Ihren eigenen Säulen, Fragen, bewährten Methoden und Verbesserungsplänen erstellen und benutzerdefinierte Linsen mit anderen AWS-Konten teilen.

Einer Workload können jeweils fünf Linsen hinzugefügt werden, wobei maximal 20 Linsen auf eine Workload angewendet werden können.

Wenn eine Linse aus einer Workload entfernt wird, bleiben die mit der Linse verbundenen Daten erhalten. Die Daten werden wiederhergestellt, wenn Sie die Linse wieder zur Workload hinzufügen.

Hinzufügen einer Linse zu einer Workload in AWS WA Tool

Wenn Sie einer Workload eine Linse hinzufügen, können Sie die Stärken und Schwächen Ihrer Architektur besser verstehen, Verbesserungsmöglichkeiten erkennen und sicherstellen, dass Ihre Workloads den Best Practices entsprechen.

So fügen Sie einer Workload eine Linse hinzu

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.

3. Wählen Sie die Workload aus und klicken Sie auf View details (Details ansehen).
4. Wählen Sie die hinzuzufügende Linse aus, und klicken Sie auf Save (Speichern).

   Linsen können aus benutzerdefinierte Linsen, dem Lens-Katalog oder beidem ausgewählt werden.

Einer Workload können bis zu 20 Linsen hinzugefügt werden.

Weitere Informationen zum AWS-Lens-Katalog finden Sie unter AWSWell-Architected-Linsen. Beachten Sie, dass nicht jedes Whitepaper zu Linsen im Lens-Katalog als Linse angeboten wird.

> **Haftungsausschluss**
>
> Mit dem Zugriff auf und/oder der Anwendung von benutzerdefinierten Lenses, die von anderen AWS-Benutzern oder -Konten erstellt wurden, bestätigen Sie, dass benutzerdefinierte Lenses, die von anderen Benutzern erstellt und für Sie freigegeben wurden, Inhalte Dritter sind wie in der AWS-Kundenvereinbarung definiert.

Hinzufügen oder Entfernen einer Linse zu/von einer Workload in AWS WA Tool

Wenn eine Linse für Ihre Workload nicht mehr relevant ist, können Sie sie entfernen.

So entfernen Sie eine Linse aus einer Workload

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich die Option Workloads aus.
3. Wählen Sie die Workload aus und klicken Sie auf View details (Details ansehen).
4. Wählen Sie die Linse ab, die Sie entfernen möchten, und klicken Sie auf Save (Speichern).

   Die AWS Well-Architected Framework-Linse kann nicht aus einer Workload entfernt werden.

Die mit der Linse verbundenen Daten bleiben bestehen. Wenn die Linse wieder der Workload hinzugefügt wird, werden die Daten wiederhergestellt.

Anzeigen von Linsendetails für eine Workload in AWS WA Tool

Sie können Details zu Ihrer Linse in der AWS Well-Architected Tool-Konsole anzeigen. Um Details zu einer Linse anzuzeigen, wählen Sie die Linse aus.

Registerkarte Overview (Übersicht)

Die Registerkarte Übersicht enthält allgemeine Informationen zur Linse, z. B. die Anzahl der beantworteten Fragen. Auf dieser Registerkarte können Sie mit die Überprüfung eines Workloads fortsetzen, einen Bericht erstellen oder die Linsen-Notizen bearbeiten.

Registerkarte „Improvement Plan (Verbesserungsplan)“

Die Registerkarte Improvement Plan (Verbesserungsplan) enthält eine Liste empfohlener Maßnahmen zur Verbesserung Ihres Workloads. Sie können die Empfehlungen basierend auf Risiko und Säule filtern.

Registerkarte „Shares (Freigaben)“

Bei einer benutzerdefinierten Linse finden Sie auf der Registerkarte Shares (Freigaben) eine Liste der IAM-Prinzipale, für die die Linse freigegeben wurde.

Benutzerdefinierte Linsen für Workloads in AWS WA Tool

Sie können benutzerdefinierte Linsen mit Ihren eigenen Säulen, Fragen, bewährten Methoden und Verbesserungsplänen erstellen. Sie wenden benutzerdefinierte Linsen auf dieselbe Weise auf eine Workload an, wie Sie von AWS bereitgestellte Linsen anwenden. Sie können auch benutzerdefinierte Linsen, die Sie erstellen, für andere AWS-Konten freigeben, und benutzerdefinierte Linsen, die anderen gehören, können für Sie freigegeben werden.

Sie können die Fragen in einer benutzerdefinierten Linse auf eine bestimmte Technologie zuschneiden, dafür sorgen, dass sie Ihnen helfen, die Governance-Anforderungen in Ihrem Unternehmen zu erfüllen, oder die durch das Well-Architected Framework und die AWS-Linsen bereitgestellte Anleitung erweitern. Wie bei den vorhandenen Linsen können Sie den Fortschritt im Laufe der Zeit verfolgen, indem Sie Meilensteine erstellen und anhand von Berichten regelmäßig den Status angeben.

Themen

- Erstellen einer benutzerdefinierten Linse für eine Workload in AWS WA Tool
- Vorschau einer benutzerdefinierten Linse für eine Workload in AWS WA Tool
- Erstmaliges Veröffentlichen einer benutzerdefinierten Linse in AWS WA Tool
- Veröffentlichen eines Updates für eine benutzerdefinierte Linse in AWS WA Tool
- Freigeben einer benutzerdefinierten Linse in AWS WA Tool
- Hinzufügen von Tags zu einer benutzerdefinierten Linse in AWS WA Tool
- Löschen einer benutzerdefinierten Linse in AWS WA Tool
- Spezifikation des Linsenformats in AWS WA Tool

Anzeige benutzerdefinierter Linsen in AWS WA Tool

Sie können die Details benutzerdefinierter Linsen, die Sie besitzen, und solcher, die für Sie freigegebenen wurden, anzeigen.

Anzeigen einer Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.

   > **Note**
   >
   > Der Abschnitt Benutzerdefinierte Linsen ist leer, wenn Sie keine benutzerdefinierte Linse erstellt haben oder keine benutzerdefinierte Linse für Sie freigegeben wurde.

3. Wählen die benutzerdefinierten Linsen aus, die Sie anzeigen möchten.
   - Owned by me (Gehört mir) – Zeigt benutzerdefinierte Linsen an, die Sie erstellt haben.
   - Shared with me (Für mich freigegeben) – Zeigt benutzerdefinierte Linsen an, die für Sie freigegeben wurden.
4. Wählen Sie die anzuzeigende benutzerdefinierte Linse auf eine der folgenden weisen aus:
   - Wählen Sie den Namen der Linse aus.
   - Wählen Sie die Linse aus, und klicken Sie auf View details (Details anzeigen).

Die Seite Anzeigen von Linsendetails für eine Workload in AWS WA Tool wird angezeigt.

Die Seite Custom lenses (Benutzerdefinierte Linsen) enthält die folgenden Felder:

Name

Der Name der Linse.

Eigentümer

Die AWS-Konto-ID, der die benutzerdefinierte Linsev gehört.

Status

Der Status PUBLISHED (VERÖFFENTLICHT) bedeutet, dass die benutzerdefinierte Linse veröffentlicht wurde und auf Workloads angewendet oder für andere AWS-Konten freigegeben werden kann.

Der Status DRAFT (ENTWURF) bedeutet, dass die benutzerdefinierte Linse erstellt, jedoch noch nicht veröffentlicht wurde. Eine benutzerdefinierte Linse muss veröffentlicht werden, bevor sie auf Workloads angewendet freigegeben werden kann.

Version

Der Name der Version der benutzerdefinierten Linse.

Letzte Aktualisierung

Datum und Uhrzeit, zu dem/der die benutzerdefinierte Linse zuletzt aktualisiert wurde.

Erstellen einer benutzerdefinierten Linse für eine Workload in AWS WA Tool

Erstellen einer benutzerdefinierten Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Wählen Sie Create custom lens (Benutzerdefinierte Linse erstellen).
4. Wählen Sie zum Herunterladen der JSON-Vorlagendatei Download file (Datei herunterladen) aus.
5. Öffnen Sie die JSON-Vorlagendatei mit Ihrem bevorzugten Texteditor, und fügen Sie die Daten für Ihre benutzerdefinierte Linse hinzu. Zu diesen Daten gehören Ihre Säulen, Fragen, bewährten Verfahren und Links zu Verbesserungsplänen.

Weitere Einzelheiten finden Sie unter Spezifikation des Linsenformats in AWS WA Tool. Eine benutzerdefinierte Linse darf eine Größe von 500 KB nicht überschreiten.

6. Wählen Sie Choose file (Datei auswählen), um Ihre JSON-Datei auszuwählen.
7. (Optional) Fügen Sie im Abschnitt Tags alle Tags hinzu, die Sie der benutzerdefinierten Linse zuordnen möchten.
8. Wählen Sie Submit & Preview (Senden und Vorschau), um eine Vorschau der benutzerdefinierten Linse anzuzeigen, oder Submit (Senden), um die benutzerdefinierte Linse ohne Vorschau zu senden.

   Wenn Sie für Ihre benutzerdefinierte Linse Submit & Preview (Senden und Vorschau) wählen, können Sie auf Next (Weiter) klicken, um durch die Linsen-Vorschau zu navigieren, oder auf Exit preview (Vorschau beenden) klicken, um zu den benutzerdefinierten Linsen zurückzukehren.

Wenn die Überprüfung fehlschlägt, bearbeiten Sie Ihre JSON-Datei, und versuchen Sie erneut, die benutzerdefinierte Linse zu erstellen.

Nach der Validierung Ihrer JSON-Datei durch AWS WA Tool wird Ihre benutzerdefinierte Linse unter Benutzerdefinierte Linsen angezeigt.

Nachdem eine benutzerdefinierte Linse erstellt wurde, befindet sie sich im Status DRAFT (ENTWURF). Sie müssen die Linse veröffentlichen, bevor sie auf Workloads angewendet oder für andere AWS-Konten freigegeben werden kann.

Sie können bis zu 15 benutzerdefinierte Linsen in einem AWS-Konto erstellen.

> **Haftungsausschluss**
>
> Geben oder erfassen Sie keine personenbezogenen Daten (PII) von Endbenutzern oder anderen identifizierbaren Personen in oder über Ihre benutzerdefinierten Linsen. Wenn Ihre benutzerdefinierte Linse oder die für Sie freigegebenen geteilten und in Ihrem Konto verwendeten Linsen personenbezogene Daten enthalten oder erfassen, sind Sie dafür verantwortlich, sicherzustellen, dass die enthaltenen personenbezogenen Daten gemäß geltendem Recht verarbeitet werden, angemessene Datenschutzhinweise bereitzustellen und die erforderlichen Einwilligungen für die Verarbeitung dieser Daten einzuholen.

Vorschau einer benutzerdefinierten Linse für eine Workload in AWS WA Tool

Vorschau einer benutzerdefinierten Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Nur Linsen mit dem Status DRAFT (ENTWURF) können in der Vorschau angezeigt werden. Wählen Sie die gewünschte benutzerdefinierte DRAFT-Linse aus, und wählen Sie Preview experience (Vorschau).
4. Wählen Sie Next (Weiter), um durch die Linsenvorschau zu navigieren.
5. (Optional) Sie können Ihren Verbesserungsplan überprüfen, indem Sie für jede Frage in der Vorschau Best Practices auswählen und Update based on answers (Auf Grundlage der Antworten aktualisieren) auswählen, um Ihre Risikologik zu testen. Wenn Änderungen erforderlich sind, können Sie die Risikoregeln in Ihrer JSON-Vorlage vor der Veröffentlichung aktualisieren.
6. Wählen Sie Exit preview (Vorschau beenden)“, um zur benutzerdefinierten Linse zurückzukehren.

> **Note**
>
> Sie können auch eine Vorschau einer benutzerdefinierten Linse anzeigen, indem Sie beim Erstellen einer benutzerdefinierten Linse die Option Submit & Preview (Senden und Vorschau) auswählen.

Erstmaliges Veröffentlichen einer benutzerdefinierten Linse in AWS WA Tool

Veröffentlichen einer benutzerdefinierten Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.

3. Wählen Sie die gewünschte benutzerdefinierte Linse aus, und wählen Sie Publish lens (Linse veröffentlichen).
4. Geben Sie im Feld Version name (Versionsname) eine eindeutige Kennung für die Versionsänderung ein. Dieser Wert kann bis zu 32 Zeichen lang sein und darf nur alphanumerische Zeichen und Punkte („.“) enthalten.
5. Wählen Sie Publish custom lens (Benutzerdefinierte Linse veröffentlichen).

   Nachdem eine benutzerdefinierte Linse veröffentlicht wurde, befindet sie sich im Status PUBLISHED (VERÖFFENTLICHT).

Die benutzerdefinierte Linse kann jetzt auf Workloads angewendet oder für andere AWS-Konten-Benutzer freigegeben werden.

Veröffentlichen eines Updates für eine benutzerdefinierte Linse in AWS WA Tool

Veröffentlichen eines Updates für eine vorhandene benutzerdefinierte Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Wählen Sie die gewünschte benutzerdefinierte Linse aus, und klicken Sie auf Edit (Bearbeiten).
4. Wenn Sie keine aktualisierte JSON-Datei zur Hand haben, wählen Sie Download file (Datei herunterladen), um eine Kopie der aktuellen benutzerdefinierten Linse herunterzuladen. Bearbeiten Sie die heruntergeladene JSON-Datei mit einem Texteditor Ihrer Wahl, und nehmen Sie die gewünschten Änderungen vor.
5. Wählen Sie Choose file (Datei auswählen), um Ihre aktualisierte JSON-Datei auszuwählen, und wählen Sie Submit & Preview (Senden und Vorschau), um eine Vorschau der benutzerdefinierten Linse anzuzeigen, oder Submit (Senden), um die benutzerdefinierte Linse ohne Vorschau einzureichen.

   Eine benutzerdefinierte Linse darf eine Größe von 500 KB nicht überschreiten.

   Nach der Validierung Ihrer JSON-Datei durch AWS WA Tool wird Ihre benutzerdefinierte Linse unter Custom lenses (Benutzerdefinierte Linsen) im Status DRAFT (ENTWURF) angezeigt.

6. Wählen Sie erneut die benutzerdefinierte Linse aus, und wählen Sie Publish lens (Linse veröffentlichen).
7. Wählen Sie Review changes before publishing (Änderungen vor der Veröffentlichung überprüfen), um zu überprüfen, ob die an Ihrer benutzerdefinierten Linse vorgenommenen Änderungen korrekt sind. Dies beinhaltet die Überprüfung folgender Elemente:

   - Der Name der benutzerdefinierten Linse
   - Die Namen der Säulen
   - Die neuen, aktualisierten und gelöschten Fragen

   Wählen Sie Next (Weiter) aus.
8. Geben Sie Art der Versionsänderung an.

   Hauptversion

   Zeigt an, dass an der Linse substanzielle Änderungen vorgenommen wurden. Wird für Änderungen verwendet, die sich auf die Bedeutung der benutzerdefinierten Linse auswirken.

   Bei Workloads, bei denen die Linse angewendet wurde, wird eine Benachrichtigung darüber angezeigt, dass eine neue Version der benutzerdefinierten Linse verfügbar ist.

   Größere Versionsänderungen werden nicht automatisch auf Workloads angewendet, bei denen die Linse verwendet wird.

   Unterversion

   Zeigt an, dass geringfügigere Änderungen an der Linse vorgenommen wurden. Wird für kleinere Änderungen verwendet, z. B. Textänderungen oder Aktualisierungen der URL-Links.

   Kleinere Versionsänderungen werden automatisch auf Workloads angewendet, die die benutzerdefinierte Linse verwenden.

   Wählen Sie Next (Weiter) aus.
9. Geben Sie im Feld Version name (Versionsname) eine eindeutige Kennung für die Versionsänderung ein. Dieser Wert kann bis zu 32 Zeichen lang sein und darf nur alphanumerische Zeichen und Punkte („.“) enthalten.
10. Wählen Sie Publish custom lens (Benutzerdefinierte Linse veröffentlichen).

Nachdem eine benutzerdefinierte Linse veröffentlicht wurde, befindet sie sich im Status PUBLISHED (VERÖFFENTLICHT).

Die aktualisierte benutzerdefinierte Linse kann jetzt auf Workloads angewendet oder für andere AWS-Konten-Benutzer freigegeben werden.

Wenn es sich bei dem Update um eine größere Versionsänderung handelt, werden alle Workloads, auf die die vorherige Version der Linse angewendet wurde, darüber informiert, dass eine neue Version verfügbar ist, und es wird die Option zum Upgrade angeboten.

Kleinere Versionsaktualisierungen werden automatisch und ohne Benachrichtigung angewendet.

Sie können bis zu 100 Versionen einer benutzerdefinierten Linse erstellen.

Freigeben einer benutzerdefinierten Linse in AWS WA Tool

Sie können eine benutzerdefinierte Linse für andere AWS-Konten, Benutzer, AWS Organizations und Organisationseinheiten (OUs) freigeben.

Freigeben einer benutzerdefinierten Linse für andere AWS-Konten und Benutzer

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Wählen Sie die freizugebende Linse aus, und klicken Sie auf View details (Details anzeigen).
4. Wählen Sie auf der Anzeigen von Linsendetails für eine Workload in AWS WA Tool-Seite die Option Shares (Freigaben). Wählen Sie dann Create (Erstellen) und Create Shares to Users oder Accounts (Freigaben für Benutzer oder Konten erstellen) aus, um eine Einladung zur gemeinsamen Nutzung von Linsen zu erstellen.
5. Geben Sie die 12-stellige AWS-Konto-ID oder den ARN des Benutzers ein, für den Sie die benutzerdefinierte Linse freigeben möchten.
6. Wählen Sie Create (Erstellen), um dem angegebenen AWS-Konto Benutzer eine Einladung zur gemeinsamen Nutzung einer benutzerdefinierten Linse zu senden.

Sie können benutzerdefinierte Linsen für bis zu 300 AWS-Konten oder Benutzer freigeben.

Wenn die Einladung zur gemeinsamen Nutzung der Linse nicht innerhalb von sieben Tagen angenommen wird, ist die Einladung automatisch abgelaufen.

> **Important**
>
> Bevor Sie eine benutzerdefinierte Linse für eine Organisation oder Organisationseinheiten (OUs) freigeben können, müssen Sie den AWS Organizations-Zugriff aktivieren.

Freigeben einer benutzerdefinierten Linse für Ihre Organisation oder Organisationseinheiten

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Wählen Sie die benutzerdefinierte Linse aus, die freigegeben werden soll.
4. Wählen Sie auf der Anzeigen von Linsendetails für eine Workload in AWS WA Tool-Seite die Option Shares (Freigaben). Wählen Sie dann Create (Erstellen) und Create Shares to Organizations (Freigaben für Organisationen erstellen) aus.
5. Wählen Sie auf der Seite Create custom lens share (Freigabe einer benutzerdefinierten Linse erstellen) aus, ob Sie der gesamten Organisation oder einer oder mehreren Organisationseinheiten Berechtigungen gewähren möchten.
6. Wählen Sie Create (Erstellen), um die benutzerdefinierte Linse freizugeben.

Um zu sehen, wer über freigegebenen Zugriff auf eine Workload verfügt, wählen Sie Shares (Freigaben) auf der Seite Anzeigen von Linsendetails für eine Workload in AWS WA Tool.

> **Haftungsausschluss**
>
> Indem Sie Ihre benutzerdefinierten Linsen für andere AWS-Konten freigeben, erklären Sie sich damit einverstanden, dass AWS Ihre benutzerdefinierten Linsen diesen anderen Konten zur Verfügung stellt. Diese anderen Konten können weiterhin auf Ihre freigegebenen benutzerdefinierten Linsen zugreifen und diese verwenden, auch wenn Sie die benutzerdefinierten Linsen aus Ihren eigenen AWS-Konto löschen oder Ihre AWS-Konto beenden.

Hinzufügen von Tags zu einer benutzerdefinierten Linse in AWS WA Tool

Hinzufügen von Tags zu einer benutzerdefinierten Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Wählen Sie die benutzerdefinierte Linse aus, die Sie aktualisieren möchten.
4. Wählen Sie im Abschnitt Tags die Option Manage tags (Tags verwalten).
5. Wählen Sie für jeden Tag, den Sie hinzufügen möchten, Add new tag (Neuen Tag hinzufügen), und geben Sie den Schlüssel und den Wert des Tags ein.
6. Wählen Sie Save (Speichern).

Zum Entfernen eines vorhandenen Tags wählen Sie neben dem zu entfernenden Tag Remove (Entfernen) aus.

Löschen einer benutzerdefinierten Linse in AWS WA Tool

Löschen einer benutzerdefinierten Linse

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie AWS Well-Architected Tool-Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie im linken Navigationsbereich Custom lenses (Benutzerdefinierte Linsen) aus.
3. Wählen Sie die zu löschende benutzerdefinierte Linse aus, und klicken Sie auf Delete (Löschen).
4. Wählen Sie Löschen aus.

   Bestehende Workloads, bei denen die Linse angewendet wurde, werden darüber informiert, dass die benutzerdefinierte Linse gelöscht wurde, können sie aber weiterhin verwenden. Die benutzerdefinierte Linse kann nicht mehr auf neue Workloads angewendet werden.

> **Haftungsausschluss**
>
> Indem Sie Ihre benutzerdefinierten Linsen für andere AWS-Konten freigeben, erklären Sie sich damit einverstanden, dass AWS Ihre benutzerdefinierten Linsen diesen anderen Konten zur Verfügung stellt. Diese anderen Konten können weiterhin auf Ihre

freigegebenen benutzerdefinierten Linsen zugreifen und diese verwenden, auch wenn Sie die benutzerdefinierten Linsen aus Ihren eigenen AWS-Konto löschen oder Ihre AWS-Konto beenden.

Spezifikation des Linsenformats in AWS WA Tool

Linsen werden mithilfe eines bestimmten JSON-Formats definiert. Wenn Sie mit der Erstellung einer benutzerdefinierten Linse beginnen, haben Sie die Möglichkeit, eine JSON-Vorlagendatei herunterzuladen. Sie können diese Datei als Grundlage für Ihre benutzerdefinierten Linsen verwenden, da sie die Grundstruktur für die Säulen, Fragen, bewährten Methoden und den Verbesserungsplan definiert.

Abschnitt „Lens (Linse)“

In diesem Abschnitt werden die Attribute für die benutzerdefinierte Linse selbst definiert. Dies sind ihr Name und ihre Beschreibung.

- `schemaVersion`: Die Version des benutzerdefinierten Linsenschemas, das verwendet werden soll. Von der Vorlage festgelegt, nicht ändern.
- `name`: Name der Linse Der Name kann eine Länge von bis zu 128 Zeichen haben.
- `description`: Textbeschreibung der Linse. Dieser Text wird angezeigt, wenn Sie Linsen auswählen, die während der Workload-Erstellung hinzugefügt werden sollen, oder wenn Sie eine Linse auswählen, die später auf eine vorhandene Workload angewendet werden soll. Die Beschreibung kann bis zu 2048 Zeichen lang sein.

```
   "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.",
```

Abschnitt „Pillars (Säulen)“

In diesem Abschnitt werden die Säulen definiert, die der benutzerdefinierten Linse zugeordnet sind. Sie können Ihre Fragen den Säulen des AWS Well-Architected Framework zuordnen, Ihre eigenen Säulen definieren oder beides.

Sie können bis zu zehn Säulen in einer benutzerdefinierten Linse erstellen.

- `id`: ID für die Säule. Die ID kann zwischen 3 und 128 Zeichen lang sein und darf nur alphanumerische Zeichen, Bindestriche („-“) und/oder Unterstriche („_“) enthalten. Die in einer Säule verwendete ID muss eindeutig sein.

  Verwenden Sie die folgenden IDs, wenn Sie Ihre Fragen den Säulen des Frameworks zuordnen:

  - `operationalExcellence`
  - `security`
  - `reliability`
  - `performance`
  - `costOptimization`
  - `sustainability`
- `name`: Name der Säule. Der Name kann eine Länge von bis zu 128 Zeichen haben.

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

Abschnitt „Questions (Frage)“

In diesem Abschnitt werden die Fragen definiert, die zu einer Säule gehören.

Sie können bis zu 20 Fragen in einer Säule in einer benutzerdefinierten Linse definieren.

- `id`: ID für die Frage. Die ID kann zwischen 3 und 128 Zeichen lang sein und darf nur alphanumerische Zeichen und Unterstriche („_“) enthalten. Die in einer Frage verwendeten IDs müssen eindeutig sein.
- `title`: Titel der Frage. Der Titel kann eine Länge von bis zu 128 Zeichen haben.
- `description`: Beschreibt die Frage ausführlicher. Die Beschreibung kann bis zu 2048 Zeichen lang sein.
- `helpfulResource displayText`: Optional. Text, der hilfreiche Informationen zu der Frage enthält. Der Text kann eine Länge von bis zu 2048 Zeichen haben. Muss angegeben werden, wenn `helpfulResource url` angegeben ist.
- `helpfulResource url`: Optional. Eine URL-Ressource, die die Frage ausführlicher erläutert. Die URL muss mit `http://` oder `https://` beginnen.

> **Note**
>
> Beim Synchronisieren eines benutzerdefinierten Lens-Workloads mit Jira werden bei Fragen sowohl die „ID“ als auch der „Titel“ der Frage angezeigt.
> Das in Jira-Tickets verwendete Format ist `[ 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"
        },
        .
        .
        .
    }
]
```

Abschnitt „Choices (Auswahlmöglichkeiten)“

In diesem Abschnitt werden die Wahlmöglichkeiten definiert, die mit einer Frage verknüpft sind.

Sie können bis zu 15 Auswahlmöglichkeiten für eine Frage in einer benutzerdefinierten Linse erstellen.

- `id`: ID für die Auswahlmöglichkeit. Die ID kann zwischen 3 und 128 Zeichen lang sein und darf nur alphanumerische Zeichen und Unterstriche („_“) enthalten. Für jede Auswahlmöglichkeit in einer Frage muss eine eindeutige ID angegeben werden. Das Hinzufügen einer Auswahlmöglichkeit mit dem Suffix von _no fungiert als `None of these`-Auswahl für die Frage.
- `title`: Titel der Auswahlmöglichkeit Der Titel kann eine Länge von bis zu 128 Zeichen haben.
- `helpfulResource displayText`: Optional. Text, der hilfreiche Informationen zu einer Auswahlmöglichkeit enthält. Der Text kann eine Länge von bis zu 2048 Zeichen haben. Muss enthalten sein, falls `helpfulResource url` angegeben ist.
- `helpfulResource url`: Optional. Eine URL-Ressource, die die Auswahlmöglichkeit detaillierter erklärt. Die URL muss mit `http://` oder `https://` beginnen.
- `improvementPlan displayText`: Text, der beschreibt, wie eine Auswahlmöglichkeit verbessert werden kann. Der Text kann eine Länge von bis zu 2048 Zeichen haben. Ein `improvementPlan` ist für jede Auswahlmöglichkeit erforderlich, außer für `None of these`.
- `improvementPlan url`: Optional. Eine URL-Ressource, die bei der Verbesserung helfen kann. Die URL muss mit `http://` oder `https://` beginnen.
- `additionalResources type`: Optional. Die Art der zusätzlichen Ressourcen. Der Wert kann entweder `HELPFUL_RESOURCE` oder `IMPROVEMENT_PLAN` sein.
- `additionalResources content`: Optional. Gibt die `displayText`- und `url`-Werte für die zusätzliche Ressource an. Für eine Auswahlmöglichkeit können bis zu fünf zusätzliche nützliche Ressourcen und bis zu fünf zusätzliche Verbesserungsplanelemente angegeben werden.

- `displayText`: Optional. Text, der die nützliche Ressource oder den Verbesserungsplan beschreibt. Der Text kann eine Länge von bis zu 2048 Zeichen haben. Muss enthalten sein, falls `url` angegeben ist.
- `url`: Optional. Eine URL-Ressource für die nützliche Ressource oder den Verbesserungsplan. Die URL muss mit `http://` oder `https://` beginnen.

> **Note**
>
> Wenn eine benutzerdefinierte Lens-Workload mit Jira synchronisiert wird, werden in den Auswahlmöglichkeiten die „ID“ der Frage und der Auswahlmöglichkeit sowie der „Titel“ der Auswahlmöglichkeit angezeigt.
> Das verwendete Format ist `[ 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"
          }

        }
```

Abschnitt „Risk Rules (Risikoregeln)“

In diesem Abschnitt wird definiert, wie die ausgewählten Optionen das Risikoniveau bestimmen.

Sie können maximal drei Risikoregeln pro Frage definieren, eine für jede Risikostufe.

- `condition`: Ein boolescher Ausdruck für die Auswahlmöglichkeiten, der einer Risikostufe für die Frage zugeordnet wird, oder `default`.

  Für jede Frage muss eine `default`-Risikoregel vorhanden sein.
- `risk`: Gibt das mit der Bedingung verbundene Risiko an. Gültige Werte sind `HIGH_RISK`, `MEDIUM_RISK` und `NO_RISK`.

Die Reihenfolge Ihrer Risikoregeln ist bedeutsam. Die erste `condition`, die als `true` bewertet wird, legt das Risiko für die Frage fest. Ein gängiges Muster für die Implementierung von Risikoregeln besteht darin, mit den am wenigsten riskanten (und in der Regel detailliertesten) Regeln zu beginnen und sich dann bis zu den riskantesten (und unspezifischsten) Regeln vorzuarbeiten.

Zum Beispiel:

```
"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"
      }
]
```

Wenn für die Frage drei Auswahlmöglichkeiten (`choice_1`, `choice_2` und `choice_3`) zur Verfügung stehen, führen diese Risikoregeln zu folgendem Verhalten:

- Wenn alle drei Optionen ausgewählt sind, besteht kein Risiko.
- Wenn entweder `choice_1` oder `choice_2` ausgewählt und `choice_3` ausgewählt ist, besteht ein mittleres Risiko.
- Wenn `choice_1` nicht ausgewählt, aber `choice_3` ausgewählt ist, besteht ebenfalls ein mittleres Risiko.
- Wenn keine dieser Bedingungen zutrifft, besteht ein hohes Risiko.

Linsen-Upgrades in AWS WA Tool

Die Linse des AWS Well-Architected Framework oder andere von AWS bereitgestellte Linsen werden mit der Einführung neuer Services aktualisiert, vorhandene bewährte Methoden für cloud-basierte Systeme werden optimiert, und neue bewährte Methoden werden hinzugefügt. Wenn eine neue Version einer Linse zur Verfügung gestellt wird, wird für AWS WA Tool ein Upgrade mit den neuesten bewährten Methoden durchgeführt. Alle neu definierten Workloads verwenden die neue Version der Linse.

Ein Linsen-Upgrade findet auch statt, wenn für eine benutzerdefinierte Linse, die Sie auf eine Workload oder eine Review-Vorlage angewendet haben, eine neue Hauptversion veröffentlicht wurde.

Ein Linsen-Upgrade besteht aus einer beliebigen Kombination folgender Aktionen:

- Hinzufügen neuer Fragen oder bewährter Methoden
- Entfernen alter Fragen oder Methoden, die nicht mehr empfohlen werden
- Aktualisieren vorhandener Fragen oder bewährter Methoden
- Hinzufügen oder Entfernen von Säulen

Ihre Antworten auf bestehende Fragen werden beibehalten.

> **Note**
>
> Sie können ein Linsen-Upgrade nicht rückgängig machen. Nachdem eine Workload auf die neueste Linsenversion aktualisiert wurde, können Sie nicht zur vorherigen Version der Linse zurückkehren.

Festlegen, für welche Linse in AWS WA Tool ein Upgrade durchgeführt werden soll

Auf der Seite Notifications (Benachrichtigungen) können Sie herausfinden, welche Workloads nicht die aktuelle Version der Linse verwenden.

Für jede Workload werden auf der Seite Notifications (Benachrichtigungen) die folgenden Informationen angezeigt:

Ressource

Der Name der Workload oder der Review-Vorlage.

Ressourcentyp

Der Typ der Ressource. Dabei kann es sich entweder um eine Workload oder eine Review-Vorlage handeln.

Zugehörige Ressource

Der Name der Linse.

Benachrichtigungstyp

Der Typ der Upgrade-Benachrichtigung.

- Nicht aktuell – Die Workload verwendet eine Version der Linse, die nicht mehr aktuell ist. Führen Sie ein Upgrade auf die aktuelle Linsen-Version durch, um bessere Tipps zu erhalten.
- Veraltet – Die Workload verwendet eine Version der Linse, die nicht mehr die bewährten Methoden widerspiegelt. Aktualisieren auf die aktuelle Linsen-Version.
- Gelöscht – Die Workload verwendet eine Linse, die von ihrem Eigentümer gelöscht wurde.

Verwendete Version

Die derzeit für die Workload verwendete Linsen-Version.

Aktuell verfügbare Version

Die Version der Linse, die aktualisiert werden kann, oder None (Keine), wenn die Linse gelöscht wurde.

Zum Durchführen eines Upgrades für die Linse, die einer Workload zugeordnet ist, wählen Sie die Workload und Upgrade lens version (Upgrade für Linsen-Version durchführen).

Aktualisieren einer Linse in AWS WA Tool

Linsen können für Workloads und Review-Vorlagen aktualisiert werden.

> **Note**
>
> Sie können das Upgrade einer Linse nicht rückgängig machen. Nachdem eine Workload oder oder eine Review-Vorlage auf die neueste Version der Linse aktualisiert wurde, können Sie nicht mehr zur vorherigen Version der Linse zurückkehren.

Aktualisieren einer Linse für eine Workload

1. Wählen Sie auf der Seite Notifications (Benachrichtigungen) eine Workload aus, die aktualisiert werden soll, und wählen Sie dann Upgrade lens version (Linsenversion aktualisieren) aus. In den einzelnen Säulen werden Informationen darüber angezeigt, was sich geändert hat.

   > **Note**
   >
   > Sie können auch auf der Registerkarte Overview (Übersicht) der Workload die Option View available upgrades (Verfügbare Upgrades anzeigen) auswählen.

2. Bevor Sie ein Upgrade der Linse durchführen, wird ein Meilenstein erstellt, um den Zustand Ihrer vorhandenen Workload für eine spätere Verwendung zu speichern. Geben Sie einen eindeutigen Namen für den Meilenstein im Feld Milestone (Meilenstein) ein.
3. Markieren Sie das Feld Confirmation (Bestätigung) neben I understand and accept these changes (Ich verstehe und akzeptiere diese Änderungen), und wählen Sie Save (Speichern).

Sobald die Linse aktualisiert wurde, können Sie die vorherige Version der Linse auf der Registerkarte Milestones (Meilensteine) anzeigen.

Aktualisieren einer Linse für eine Review-Vorlage

1. Um die Linse für eine Review-Vorlage zu aktualisieren, wählen Sie
2. Wählen Sie auf der Seite Notifications (Benachrichtigungen) eine Review-Vorlage aus, die Sie aktualisieren möchten, und wählen Sie dann Upgrade lens version (Linsenversion aktualisieren). Informationen dazu, was sich in den einzelnen Säulen geändert hat, werden angezeigt.

   > **Note**
   >
   > Sie können auch auf der Registerkarte Overview (Übersicht) der Review-Vorlage die Option View available upgrades (Verfügbare Upgrades anzeigen) auswählen.

3. Markieren Sie das Feld Confirmation (Bestätigung) neben I understand and accept these changes (Ich verstehe und akzeptiere diese Änderungen), und wählen Sie Update and edit template answers (Aktualisieren und Vorlagenantworten bearbeiten), um die Antworten auf bewährte Verfahren für Ihre Review-Vorlage anzupassen, oder Upgrade (Aktualisieren), um die Linse zu aktualisieren, ohne Ihre Vorlagenantworten zu ändern.

Lens-Katalog für AWS WA Tool

Der Lens-Katalog ist eine Sammlung offizieller AWS-Linsen, die speziell für AWS Well-Architected Tool entwickelt wurden und aktuelle Technologien und branchenspezifische Best Practices bieten. Diese Linsen stehen allen Benutzern zur Verfügung und erfordern keine zusätzliche Installation.

In der folgenden Tabelle werden alle offiziellen AWS-Linsen beschrieben, die derzeit im Lens-Katalog verfügbar sind.

Name der Linse	Beschreibung
AWS Well-Architected Framework	Wird standardmäßig auf alle Workloads angewendet. Sammlung bewährter Architekturverfahren für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme in der Cloud.
Vernetzte Mobilität	Bewährte Verfahren zur Integration von Technologie in Verkehrssysteme und zur

Name der Linse	Beschreibung
	Verbesserung des allgemeinen Mobilität skomforts.
Container Build	Bietet bewährte Verfahren für den Entwurfs- und Build-Prozess von Containern.
Datenanalytik	Enthält Erkenntnisse aus realen Fallstudien von AWS und hilft Ihnen dabei, die wichtigsten Designelemente von Well Architected-Analyt ics-Workloads sowie Verbesserungsempfe hlungen kennenzulernen.
DevOps	Beschreibt einen strukturierten Ansatz, den Unternehmen jeder Größe verfolgen können, um eine geschwindigkeits- und sicherhei tsorientierte Kultur zu entwickeln, die mit modernen Technologien und DevOps-Best-Practices erheblichen Geschäftswert bietet.
Finanzdienstleistungsbranche	Bewährte Methoden für die Gestaltung Ihrer Workloads in der Finanzdienstleistungsbranche auf AWS.
Generative KI	Bewährte Methoden für die Architektur Ihrer generativen KI-Workloads auf AWS.
Behörden	Bewährte Methoden für das Entwerfen und die Verwendung von Behördenservices auf AWS.
Gesundheitsbranche	Bewährte Methoden und Anleitungen für die Gestaltung, Bereitstellung und Verwaltung Ihrer Workloads im Gesundheitswesen in der AWS Cloud.
IoT	Bewährte Methoden für das Management Ihrer IoT- (Internet of Things) Workloads in AWS.

Name der Linse	Beschreibung
Fusionen und Übernahmen	Bewährte Methoden für die Integration von Workloads und die Migration in die Cloud bei Fusionen und Übernahmen.
Machine Learning	Bewährte Methoden für das Management von Machine Learning-Ressourcen und -Workloads in .
Migration	Bewährte Methoden für die Migration zur AWS Cloud.
SaaS	Konzentriert sich auf den Entwurf, die Bereitstellung und die Architektur Ihrer Software-as-a-Service (SaaS)-Workloads in der AWS Cloud.
SAP	Entwurfsprinzipien und bewährte Methoden für SAP-Workloads in der AWS Cloud.
Serverless-Anwendungen	Bewährte Methoden für die Erstellung von Serverless-Workloads auf AWS. Behandelt Szenarien wie RESTful-Microservices, mobile App-Backends, die Stream-Verarbeitung und Webanwendungen.

Vorlagen überprüfen in AWS WA Tool

Sie können Bewertungsvorlagen erstellen AWS WA Tool , die vorausgefüllte Antworten auf Well-Architected Framework und Best-Practice-Fragen für benutzerdefinierte Objektive enthalten. Mit Vorlagen für Well-Architected-Bewertungen müssen Sie bei der Durchführung einer Well-Architected-Überprüfung nicht dieselben Antworten für Best Practices manuell eingeben, die bei der Durchführung einer Well-Architected-Überprüfung üblich sind, und tragen dazu bei, die Konsistenz und Standardisierung von Best Practices für Teams und Workloads zu fördern.

Sie können eine Bewertungsvorlage erstellen, um häufig gestellte Fragen zu bewährten Verfahren zu beantworten oder Notizen zu erstellen, die dann mit einem anderen IAM Benutzer oder Konto oder einer Organisation oder Organisationseinheit derselben Person geteilt werden können. AWS-Region Sie können einen Workload anhand einer Bewertungsvorlage definieren, was Ihnen hilft, gängige bewährte Verfahren zu skalieren und Redundanzen zwischen Ihren Workloads zu reduzieren.

Erstellen Sie eine Bewertungsvorlage in AWS WA Tool

Um eine Bewertungsvorlage zu erstellen

1. Wählen Sie im linken Navigationsbereich Vorlagen überprüfen aus.
2. Wählen Sie Create template (Vorlage erstellen) aus.
3. Geben Sie auf der Seite „Vorlagendetails angeben“ einen Namen und eine Beschreibung für Ihre Bewertungsvorlage ein.
4. (Optional) Fügen Sie in den Abschnitten „Anmerkungen zur Vorlage“ und „Schlagworte“ alle Anmerkungen oder Tags zur Vorlage hinzu, die Sie mit der Bewertungsvorlage verknüpfen möchten. Alle hinzugefügten Notizen werden auf alle Workloads angewendet, die die Bewertungsvorlage verwenden, wohingegen Tags nur für die Bewertungsvorlage gelten.

   Weitere Informationen zu Stichwörtern finden Sie unterMarkieren Ihrer AWS WA Tool-Ressourcen.
5. Wählen Sie Weiter.
6. Wählen Sie auf der Seite Kontaktlinsen anwenden die Kontaktlinsen aus, die Sie auf die Bewertungsvorlage anwenden möchten. Die maximale Anzahl von Kontaktlinsen, die aufgetragen werden können, ist 20.

Objektive können aus dem Bereich Benutzerdefinierte Objektive, aus dem Objektivkatalog oder aus beiden ausgewählt werden.

> **Note**
>
> Objektive, die mit Ihnen geteilt wurden, können nicht auf die Bewertungsvorlage angewendet werden.

7. Wählen Sie Create template (Vorlage erstellen) aus.

Um mit der Beantwortung von Fragen zu der Bewertungsvorlage zu beginnen, die Sie gerade erstellt haben

1. Wählen Sie auf der Registerkarte „Übersicht“ der Vorlage in der Informationsmeldung mit der Beantwortung von Fragen beginnen die Linse in der Dropdownliste „Fragen beantworten“ aus.

> **Note**
>
> Sie können auch zum Bereich Objektive gehen, das Objektiv auswählen und dann „Fragen beantworten“ auswählen.

2. Beantworten Sie für jedes Objektiv, das Sie auf Ihre Bewertungsvorlage angewendet haben, die entsprechenden Fragen und wählen Sie Speichern und beenden, wenn Sie fertig sind.

Sobald Ihre Bewertungsvorlage erstellt wurde, können Sie daraus einen neuen Workload definieren.

Auf der Registerkarte „Übersicht“ der Bewertungsvorlage sollte die Gesamtzahl der im Abschnitt „Vorlagendetails“ beantworteten Fragen und im Abschnitt „Objektive“ die für jede Linse beantworteten Fragen angezeigt werden.

Bearbeitung einer Bewertungsvorlage in AWS WA Tool

Um eine Bewertungsvorlage zu bearbeiten

1. Wählen Sie im linken Navigationsbereich Vorlagen überprüfen aus.
2. Wählen Sie den Namen der Bewertungsvorlage aus, die Sie bearbeiten möchten.

3. Um den Namen, die Beschreibung oder die Vorlagennotizen für die Bewertungsvorlage zu aktualisieren, wählen Sie auf der Registerkarte „Übersicht“ im Abschnitt „Vorlagendetails“ die Option „Bearbeiten“.
   a. Nehmen Sie Ihre Änderungen an den Anmerkungen zu Name, Beschreibung oder Vorlage vor.
   b. Wählen Sie Vorlage speichern, um die Bewertungsvorlage mit Ihren Änderungen zu aktualisieren.
4. Um zu aktualisieren, welche Brillengläser auf die Bewertungsvorlage angewendet wurden, wählen Sie auf dem Tab „Übersicht“ im Bereich „Objektive“ die Option „Verwendete Brillengläser bearbeiten“.
   a. Aktivieren oder deaktivieren Sie die Kontrollkästchen der Brillengläser, die Sie hinzufügen oder entfernen möchten.

      Objektive können im Bereich Benutzerdefinierte Objektive, im Objektivkatalog oder in beiden Bereichen ausgewählt oder abgewählt werden.
   b. Wählen Sie Vorlage speichern, um Ihre Änderungen zu speichern.
5. Um die Antworten auf Fragen zu bewährten Verfahren zum Objektiv zu aktualisieren, wählen Sie auf der Registerkarte Übersicht im Bereich Objektive den Namen des Objektivs aus.
   a. Wählen Sie im Bereich Objektiv-Übersicht die Option Fragen beantworten aus.

      > **Note**
      >
      > Optional können Sie im linken Navigationsbereich in der Dropdownliste Vorlagen überprüfen den Namen des Objektivs auswählen, um zum Bereich Objektivübersicht zu gelangen.

   b. Aktivieren oder deaktivieren Sie die Kontrollkästchen neben den Best-Practice-Antworten, die Sie ändern möchten.
   c. Wählen Sie Speichern und beenden, um Ihre Änderungen zu speichern.

Teilen einer Bewertungsvorlage in AWS WA Tool

Bewertungsvorlagen können für Benutzer oder Konten oder für eine gesamte Organisation oder Organisationseinheit freigegeben werden.

Um eine Bewertungsvorlage zu teilen

1. Wählen Sie im linken Navigationsbereich Vorlagen überprüfen aus.
2. Wählen Sie den Namen der Bewertungsvorlage aus, die Sie teilen möchten.
3. Wählen Sie den Tab „Shares“.
4. Um etwas für einen Benutzer oder ein Konto freizugeben, wählen Sie Erstellen und dann Mit IAM Benutzern oder Konten teilen aus. Geben Sie im Feld Einladungen senden den Benutzer oder das Konto IDs an und wählen Sie Erstellen aus.
5. Um Inhalte für eine Organisation oder Organisationseinheit freizugeben, wählen Sie Erstellen und anschließend Mit Organizations teilen aus. Um die Daten für die gesamte Organisation freizugeben, wählen Sie Berechtigungen für die gesamte Organisation gewähren aus. Um die Daten für eine Organisationseinheit freizugeben, wählen Sie Berechtigungen für einzelne Organisationseinheiten erteilen aus, geben Sie die Organisationseinheit im Feld an und wählen Sie Erstellen aus.

> **Important**
>
> Bevor Sie ein Profil mit einer Organisation oder Organisationseinheit (OU) teilen können, müssen Sie AWS Organizations den Zugriff aktivieren.

Definieren Sie einen Workload anhand einer Vorlage in AWS WA Tool

Sie können einen Workload anhand einer Bewertungsvorlage definieren, die Sie erstellt haben, oder anhand einer Bewertungsvorlage, die mit Ihnen geteilt wurde. Sie können keinen neuen Workload anhand einer gelöschten Bewertungsvorlage definieren. Wenn die Bewertungsvorlage eine veraltete Version einer Linse enthält, müssen Sie die Bewertungsvorlage aktualisieren, bevor Sie daraus einen neuen Workload definieren können. Informationen zum Aktualisieren einer Bewertungsvorlage finden Sie unterthe section called “Aktualisieren einer Linse”.

> **Note**
>
> Um einen Workload anhand einer Bewertungsvorlage zu definieren, müssen Sie die IAM Berechtigungen zum Erstellen eines

Workloads aktiviert haben:`wellarchitected:CreateWorkload`,
sowie die folgenden Berechtigungen für Bewertungsvorlagen:
`wellarchitected:GetReviewTemplatewellarchitected:GetReviewTemplateAnswer`,`wel`
und`wellarchitected:GetReviewTemplateLensReview`. Weitere Informationen zu IAM Berechtigungen finden Sie im AWS Identity and Access Management Benutzerhandbuch.

Um einen Workload anhand einer Bewertungsvorlage zu definieren

1. Wählen Sie im linken Navigationsbereich Vorlagen überprüfen aus.
2. Wählen Sie den Namen der Bewertungsvorlage aus, aus der Sie einen Workload definieren möchten.
3. Wählen Sie „Arbeitslast aus Vorlage definieren“.

   > **Note**
   >
   > Sie können auf der Seite „Workloads“ auch in der Dropdownliste „Workload definieren“ die Option „Aus Bewertungsvorlage definieren“ auswählen.

4. Wählen Sie im Schritt Bewertungsvorlage auswählen die Karte mit der Bewertungsvorlage aus und klicken Sie auf Weiter.
5. Füllen Sie im Schritt Eigenschaften angeben die erforderlichen Felder für die Workload-Eigenschaften aus und wählen Sie Weiter aus. Weitere Details erhalten Sie unter the section called “Einen Workload definieren”.
6. (Optional) Ordnen Sie im Schritt Profil anwenden dem Workload ein Profil zu, indem Sie ein vorhandenes Profil auswählen, nach dem Profilnamen suchen oder Profil erstellen auswählen, um ein Profil zu erstellen. Wählen Sie Weiter.

   Well-Architected Profile und Bewertungsvorlagen können zusammen verwendet werden. Die Fragen, die in Ihrer Bewertungsvorlage vorab ausgefüllt sind, bleiben im Workload beantwortet, und die Fragen werden anhand Ihres Profils priorisiert.
7. (Optional) Im Schritt Brillengläser anwenden können Sie wählen, ob Sie zusätzliche Brillengläser aus dem Katalog für benutzerdefinierte Brillengläser oder Brillengläser verwenden möchten, die noch nicht auf die Bewertungsvorlage angewendet wurden.
8. Wählen Sie Define workload (Workload definieren) aus.

Löschen einer Bewertungsvorlage in AWS WA Tool

Um eine Bewertungsvorlage zu löschen

1. Wählen Sie im linken Navigationsbereich Vorlagen überprüfen aus.
2. Wählen Sie im Abschnitt Bewertungsvorlagen die Bewertungsvorlage aus, die Sie löschen möchten, und wählen Sie im Drop-down-Menü Aktionen die Option Löschen aus.

   > **Note**
   >
   > Sie können auch den Namen der Vorlage auswählen und auf der Registerkarte Übersicht der Bewertungsvorlage die Option Löschen auswählen.

3. Geben Sie im Dialogfeld Bewertungsvorlage löschen den Namen der Bewertungsvorlage in das Feld ein, um das Löschen zu bestätigen.
4. Wählen Sie Löschen.

Sie können aus einer gelöschten Bewertungsvorlage keinen neuen Workload erstellen. Wenn Sie eine Bewertungsvorlage, die Sie gelöscht haben, mit anderen IAM Benutzern, Konten oder Organisationen geteilt haben, können diese keine Workloads daraus erstellen.

Verwenden von Profilen in AWS WA Tool

Sie können Profile erstellen, um Ihren Geschäftskontext anzugeben und Ziele zu identifizieren, die Sie bei der Durchführung eines Well-Architected-Reviews erreichen möchten. AWS Well-Architected Tool verwendet die in Ihrem Profil gesammelten Informationen, damit Sie sich bei der Überprüfung der Arbeitslast auf eine priorisierte Liste von Fragen konzentrieren können, die für Ihr Unternehmen relevant sind. Wenn Sie Ihrem Workload ein Profil beifügen, können Sie auch sehen, welche Risiken priorisiert sind, damit Sie sich mit Ihrem Verbesserungsplan befassen können.

Sie können auf der Seite „Profile“ ein Profil erstellen und es einer neuen Arbeitslast zuordnen, oder Sie können einer vorhandenen Arbeitslast ein Profil hinzufügen.

Erstellen eines -Profils

So erstellen Sie ein Profil

1. Wählen Sie im linken Navigationsbereich Profile aus.
2. Wählen Sie Create profile (Profil erstellen) aus.
3. Geben Sie im Abschnitt Profileigenschaften einen Namen und eine Beschreibung für Ihr Profil ein.
4. Um die Informationen zu verfeinern, die für Ihr Unternehmen im Plan zur Überprüfung und Verbesserung der Arbeitslast priorisiert wurden, wählen Sie im Abschnitt Profilfragen die Antworten aus, die für Ihr Unternehmen am relevantesten sind.
5. (Optional) Fügen Sie im Abschnitt Stichwörter alle Tags hinzu, die Sie dem Profil zuordnen möchten.

   Weitere Informationen zu Stichwörtern finden Sie unterMarkieren Ihrer AWS WA Tool-Ressourcen.
6. Wählen Sie Save (Speichern) aus. Eine Erfolgsmeldung wird angezeigt, wenn das Profil erfolgreich erstellt wurde.

Wenn ein Profil erstellt wird, wird die Profilübersicht angezeigt. In der Übersicht werden die mit dem Profil verknüpften Daten angezeigt, einschließlich Name, BeschreibungARN, Erstellungs- und Aktualisierungsdatum sowie Antworten auf die Profilfragen. Auf der Profilübersichtsseite können Sie Ihr Profil bearbeiten, löschen oder teilen.

Bearbeiten eines Profils in AWS WA Tool

So bearbeiten Sie ein Profil

1. Wählen Sie im linken Navigationsbereich Profile aus, oder wählen Sie im Abschnitt Profile des Workloads die Option Profil anzeigen aus.
2. Wählen Sie den Namen des Profils aus, das Sie aktualisieren möchten.
3. Wählen Sie auf der Profilübersichtsseite Bearbeiten aus.
4. Nehmen Sie alle erforderlichen Aktualisierungen an den Profilfragen vor.
5. Wählen Sie Save (Speichern) aus.

Ein Profil teilen in AWS WA Tool

Profile können für Benutzer oder Konten oder für eine gesamte Organisation oder Organisationseinheit freigegeben werden.

Um ein Profil zu teilen

1. Wählen Sie im linken Navigationsbereich Profile aus.
2. Wählen Sie den Namen des Profils aus, das Sie teilen möchten.
3. Wählen Sie den Tab Shares.
4. Um Inhalte für einen Benutzer oder ein Konto freizugeben, wählen Sie Erstellen und anschließend Shares für IAM Benutzer oder Konten erstellen aus. Geben Sie im Feld Einladungen senden den Benutzer oder das Konto IDs an und wählen Sie Erstellen aus.
5. Um Inhalte für eine Organisation oder Organisationseinheit freizugeben, wählen Sie Erstellen und anschließend Freigaben für Organizations erstellen aus. Um sie für eine gesamte Organisation freizugeben, wählen Sie Berechtigungen für die gesamte Organisation gewähren aus. Um die Daten für eine Organisationseinheit freizugeben, wählen Sie Berechtigungen für einzelne Organisationseinheiten erteilen aus, geben Sie die Organisationseinheit im Feld an und wählen Sie Erstellen aus.

> **Important**
>
> Bevor Sie ein Profil mit einer Organisation oder Organisationseinheit (OU) teilen können, müssen Sie AWS Organizations den Zugriff aktivieren.

Hinzufügen eines Profils zu einem Workload in AWS WA Tool

Sie können einem vorhandenen Workload oder bei der Definition eines Workloads ein Profil hinzufügen, um den Workload-Überprüfungsprozess zu beschleunigen. AWS WA Tool verwendet die in Ihrem Profil gesammelten Informationen, um Fragen in der Workload-Überprüfung zu priorisieren, die für Ihr Unternehmen relevant sind.

Weitere Informationen zum Hinzufügen eines Profils bei der Definition eines Workloads finden Sie unterthe section called “Einen Workload definieren”.

So fügen Sie einem vorhandenen Workload ein Profil hinzu

1. Wählen Sie im linken Navigationsbereich Workloads aus und wählen Sie den Namen des Workloads aus, den Sie einem Profil zuordnen möchten.

   > **Note**
   >
   > Einem Workload kann nur ein Profil zugeordnet werden.

2. Wählen Sie im Abschnitt Profil die Option Profil hinzufügen aus.
3. Wählen Sie das Profil, das Sie auf den Workload anwenden möchten, aus der Liste der verfügbaren Profile aus, oder wählen Sie Profil erstellen. Weitere Informationen finden Sie unter the section called “Erstellen eines -Profils”.
4. Wählen Sie Save (Speichern) aus.

In der Workload-Übersicht wird die Anzahl der beantworteten priorisierten Fragen und der priorisierten Risiken angezeigt, die auf den Informationen im zugehörigen Profil basieren. Wählen Sie „Überprüfung fortsetzen“, um die priorisierten Fragen in der Workload-Überprüfung zu beantworten. Weitere Informationen finden Sie unter the section called “Einen Workload dokumentieren”.

Im Abschnitt Profil werden der Name, die BeschreibungARN, die Version und das Datum der letzten Aktualisierung für das mit dem Workload verknüpfte Profil angezeigt.

Entfernen eines Profils aus einem Workload in AWS WA Tool

Durch das Entfernen eines Profils aus dem Workload wird der Workload auf die Version zurückgesetzt, vor der das Profil dem Workload zugeordnet wurde, und Fragen und Risiken bei der Überprüfung des Workloads werden nicht mehr priorisiert.

Um ein Profil aus einem Workload zu entfernen

1. Wählen Sie im Abschnitt Profile des Workloads die Option Entfernen aus.
2. Um das Entfernen zu bestätigen, geben Sie den Namen des Profils in das Texteingabefeld ein.
3. Wählen Sie Remove (Entfernen) aus.

Es wird eine Benachrichtigung angezeigt, dass das Profil erfolgreich aus dem Workload entfernt wurde. Durch das Entfernen eines Profils wird die Arbeitslast auf die Version zurückgesetzt, vor der das Profil dem Profil zugeordnet wurde, und Fragen und Risiken bei der Überprüfung der Arbeitslast werden nicht mehr priorisiert.

Löschen eines Profils von AWS WA Tool

Wenn Sie ein Profil erstellt haben, können Sie das Profil aus der Liste der verfügbaren Profile in löschen AWS WA Tool.

Durch das Löschen eines Profils von der Profilseite wird das Profil nicht aus den zugehörigen Workloads entfernt. Sie können weiterhin Profile verwenden, die vor dem Löschen gemeinsam genutzt und einem Workload zugeordnet wurden. Einem gelöschten Profil können jedoch keine neuen Workloads zugeordnet werden. the section called “Benachrichtigungen über das Profil”werden mithilfe gelöschter Profile an Workload-Besitzer gesendet.

> **Haftungsausschluss**
>
> Indem Sie Ihre Profile mit anderen teilen AWS-Konten, erklären Sie sich damit einverstanden, dass AWS Ihre Profile diesen anderen Konten zur Verfügung stehen. Diese anderen Konten können weiterhin auf Ihre geteilten Profile zugreifen und diese nutzen, auch wenn Sie das Profil aus Ihrem eigenen löschen AWS-Konto oder Ihr Profil kündigen AWS-Konto.

Um ein Profil aus Ihrer Profilliste zu löschen

1. Wählen Sie im linken Navigationsbereich Profile aus.
2. Wählen Sie den Namen des Profils aus, das Sie entfernen möchten.
3. Wählen Sie Löschen.
4. Um das Entfernen zu bestätigen, geben Sie den Profilnamen in das Texteingabefeld ein.
5. Wählen Sie Löschen.

Wenn Sie ein Profil in Ihrer Profilliste behalten, es aber aus einem Workload entfernen möchten, finden Sie weitere Informationen unterthe section called “Ein Profil aus einem Workload entfernen”.

AWS Well-Architected Tool Konnektor für Jira

Sie können den AWS Well-Architected Tool Connector für Jira verwenden, um Ihr Jira-Konto mit Ihren Workloads zu verknüpfen AWS Well-Architected Tool und Verbesserungselemente aus Ihren Workloads mit Jira-Projekten zu synchronisieren, sodass Sie einen geschlossenen Mechanismus für die Implementierung von Verbesserungen einrichten können.

Der Konnektor ermöglicht sowohl automatische als auch manuelle Synchronisation. Weitere Informationen finden Sie unter Konfiguration des Connectors.

Der Connector kann auf Konto- und Workload-Ebene eingerichtet werden, wobei Sie die Option haben, Ihre Einstellungen auf Kontoebene pro Workload zu überschreiben. Auf Workload-Ebene können Sie sich auch dafür entscheiden, einen Workload vollständig von der Synchronisierung auszuschließen.

Sie können wählen, ob Verbesserungselemente mit dem WA Jira-Standardprojekt synchronisiert werden sollen, oder Sie können einen vorhandenen Projektschlüssel angeben, mit dem synchronisiert werden soll. Auf Workload-Ebene können Sie bei Bedarf jeden Workload mit einem eindeutigen Jira-Projekt synchronisieren.

> **Note**
>
> Der Connector unterstützt nur Scrum- und Kanban-Projekte in Jira.

Wenn Verbesserungselemente mit Jira synchronisiert werden, sind sie wie folgt organisiert:

- Projekt: WA (oder vorhandenes Projekt, das Sie angeben)
- Episch: Arbeitsaufwand
- Aufgabe: Frage
- Unteraufgabe: Bewährte Verfahren
- Kennzeichnung: Säule

Nachdem Sie die Synchronisierung Ihres Jira-Kontos auf der Seite Einstellungen eingerichtet haben, können Sie den Jira-Connector konfigurieren und Verbesserungselemente mit Ihrem Jira-Konto synchronisieren.

Den Connector einrichten

Um den Connector zu installieren

> **Note**
>
> Alle folgenden Schritte werden in Ihrem Jira-Konto ausgeführt, nicht in Ihrem AWS-Konto.

1. Loggen Sie sich in Ihr Jira-Konto ein.
2. Wähle in der oberen Navigationsleiste Apps und dann Weitere Apps entdecken aus.
3. Geben AWS Sie auf der Seite Apps und Integrationen für Jira entdecken Well-Architected ein. Wählen Sie dann den Connector für Jira aus.AWS Well-Architected Tool
4. Wählen Sie auf der App-Seite die Option App abrufen aus.
5. Wählen Sie im Bereich Zu Jira hinzufügen die Option Jetzt herunterladen aus.
6. Wählen Sie nach der Installation der App „Konfigurieren“, um die Einrichtung abzuschließen.
7. Wählen Sie auf der AWS Well-Architected Tool Konfigurationsseite Connect a new aus AWS-Konto.
8. Geben Sie Ihre AccessKeyID und Ihren geheimen Schlüssel ein. Optional: Geben Sie Ihr Sitzungstoken ein. Wählen Sie dann Connect.

   > **Note**
   >
   > Vergewissern Sie sich, dass Ihr Konto über die entsprechende Genehmigung verfügt`wellarchitected:ConfigureIntegration`. Diese Berechtigungen sind für das Hinzufügen AWS-Konten zu Jira erforderlich.
   > Es AWS-Konten können mehrere verbunden werden. AWS WA Tool

   > **Note**
   >
   > Aus Sicherheitsgründen wird dringend empfohlen, kurzfristige IAM-Anmeldeinformationen zu verwenden. Einzelheiten zur Erstellung einer AccessKeyID und eines geheimen Schlüssels für Sie AWS-Konto finden Sie unter Verwaltung von

Zugriffsschlüsseln (Konsole). Weitere Informationen zur Verwendung kurzfristiger Anmeldeinformationen finden Sie unter Temporäre Anmeldeinformationen anfordern.

9. Wählen Sie unter Regionen die aus, zu denen AWS-Regionen Sie eine Verbindung herstellen möchten. Wählen Sie dann Connect.

Einrichtung des Jira-Projekts

Wenn Sie benutzerdefinierte Projekte verwenden, stellen Sie sicher, dass Sie die folgenden Problemtypen in Ihrem Projekt-Setup haben:

- Scrum: Epic, Story, Subtask
- Kanban: Episch, Aufgabe, Unteraufgabe

Einzelheiten zur Verwaltung von Vorgangstypen findest du unter Atlassian Support | Einen Vorgangstyp hinzufügen, bearbeiten und löschen.

So überprüfst du den Status des Connectors in AWS Well-Architected Tool

1. Melden Sie sich bei Ihrem an AWS-Konto und navigieren Sie zu AWS Well-Architected Tool.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie im Bereich Jira-Kontosynchronisierung unter Verbindungsstatus der Jira-App nach dem Status Konfiguriert.

Der Connector ist jetzt eingerichtet und kann konfiguriert werden. Informationen zur Konfiguration der Jira-Sync-Einstellungen auf Konto- und Workload-Ebene finden Sie unter Konfiguration des Connectors.

Konfigurieren des Connectors

Mit dem AWS Well-Architected Tool Connector für Jira können Sie die Jira-Synchronisierung auf Kontoebene, Workload-Ebene oder auf beiden Ebenen konfigurieren. Sie können Jira-Einstellungen auf Workload-Ebene unabhängig von den Einstellungen auf Kontoebene konfigurieren oder Ihre Einstellungen auf Kontoebene für einen bestimmten Workload überschreiben, um das Synchronisierungsverhalten des Workloads festzulegen. Sie können Jira-Einstellungen auch konfigurieren, wenn Sie einen Workload definieren.

Der Connector bietet zwei Synchronisierungsmethoden: Automatische und manuelle Synchronisierung. Bei beiden Synchronisierungsmethoden werden Änderungen, die in vorgenommen wurden, in AWS WA Tool Ihrem Jira-Projekt widergespiegelt, und in Jira vorgenommene Änderungen werden wieder synchronisiert. AWS WA Tool

> **Important**
>
> Durch die automatische Synchronisierung erklären Sie sich damit einverstanden, Ihren Workload als Reaktion auf Änderungen in Jira zu AWS WA Tool ändern.
> Wenn Sie vertrauliche Informationen haben, die Sie nicht mit Jira synchronisieren möchten, geben Sie diese Informationen nicht in das Feld Notizen in Ihren Workloads ein.

- Automatische Synchronisierung: Der Connector aktualisiert Ihr Jira-Projekt und Ihren Workload automatisch bei jeder Aktualisierung einer Frage. Dazu gehört auch das Auswählen oder Abwählen einer bewährten Methode und das Ausfüllen einer Frage.
- Manuelle Synchronisierung: Sie müssen im Workload-Dashboard die Option Mit Jira synchronisieren auswählen, wenn Sie Verbesserungselemente zwischen Jira und dem synchronisieren möchten. AWS WA Tool Sie können auch auswählen, welche spezifischen Säulen und Fragen Sie synchronisieren möchten. Weitere Informationen finden Sie unter Synchronisieren eines Workloads.

Um den Connector auf Kontoebene zu konfigurieren

1. Wählen Sie im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie im Bereich für die Synchronisierung von Jira-Konten die Option Bearbeiten aus.
3. Wählen Sie als Synchronisierungstyp eine der folgenden Optionen aus:
    a. Um Workloads automatisch zu synchronisieren, wenn Änderungen vorgenommen werden, wählen Sie Automatisch aus.
    b. Um manuell auszuwählen, wann Workloads synchronisiert werden sollen, wählen Sie Manuell.
4. Standardmäßig erstellt der Konnektor ein WA Jira-Projekt. Gehen Sie wie folgt vor, um Ihren eigenen Jira-Projektschlüssel anzugeben:
    a. Wählen Sie Standard-Jira-Projektschlüssel überschreiben aus.
    b. Geben Sie Ihren Jira-Projektschlüssel ein.

> **Note**
>
> Der angegebene Jira-Projektschlüssel wird für alle Workloads verwendet, sofern Sie das Projekt nicht auf Workload-Ebene ändern.

5. Wählen Sie Save settings (Einstellungen speichern).

Um den Connector auf Workload-Ebene zu konfigurieren

1. Wählen Sie im linken Navigationsbereich Workloads und dann den Namen des Workloads aus, den Sie konfigurieren möchten.
2. Wählen Sie Properties (Eigenschaften).
3. Wählen Sie im Jira-Bereich Bearbeiten aus.
4. Um die Jira-Einstellungen des Workloads zu konfigurieren, wählen Sie Einstellungen auf Kontoebene überschreiben aus.

> **Note**
>
> Einstellungen auf Kontoebene überschreiben muss ausgewählt werden, um workload-spezifische Einstellungen anzuwenden.

5. Wählen Sie für Sync Override eine der folgenden Optionen aus:
   a. Um den Workload von Jira Sync auszuschließen, wähle Workload nicht synchronisieren aus.
   b. Um manuell auszuwählen, wann der Workload synchronisiert werden soll, wähle Workload synchronisieren — Manuell.
   c. Um Workload-Änderungen automatisch zu synchronisieren, wählen Sie Workload synchronisieren — Automatisch aus.
6. (Optional) Geben Sie unter Jira-Projektschlüssel den Projektschlüssel ein, mit dem der Workload synchronisiert werden soll. Dieser Projektschlüssel kann sich von Ihrem Projektschlüssel auf Kontoebene unterscheiden.

   Wenn Sie keinen Projektschlüssel angeben, erstellt der Connector ein WA Jira-Projekt.
7. Wählen Sie Speichern.

Einzelheiten zur Durchführung einer manuellen Synchronisierung finden Sie unter Synchronisieren eines Workloads.

Einen Workload synchronisieren

Bei der automatischen Synchronisierung synchronisiert der Connector automatisch Verbesserungselemente, wenn Sie einen Workload aktualisieren (z. B. wenn Sie eine Frage beantworten oder eine neue bewährte Methode auswählen).

Sowohl bei der manuellen als auch bei der automatischen Synchronisierung werden alle in Jira vorgenommenen Änderungen (wie das Ausfüllen einer Frage oder bewährte Verfahren) wieder synchronisiert. AWS Well-Architected Tool

Um einen Workload manuell zu synchronisieren

1. Wenn Sie bereit sind, Ihren Workload mit Jira zu synchronisieren, wählen Sie im linken Navigationsbereich Workloads aus. Wählen Sie dann den Workload aus, den Sie synchronisieren möchten.
2. Wählen Sie in der Workload-Übersicht die Option Mit Jira synchronisieren aus.
3. Wählen Sie das Objektiv aus, das Sie synchronisieren möchten.
4. Wählen Sie für Fragen, die mit Jira synchronisiert werden sollen, die Fragen oder ganze Säulen aus, die Sie mit dem Jira-Projekt synchronisieren möchten.
    - Wählen Sie für alle Fragen, die Sie entfernen möchten, das X-Symbol neben dem Titel der Frage aus.
5. Wählen Sie Synchronisieren.

Den Connector deinstallieren

Um den AWS Well-Architected Tool Connector für Jira vollständig zu deinstallieren, führen Sie die folgenden Aufgaben aus:

- Deaktivieren Sie Jira Sync in allen Workloads, die die Synchronisierungseinstellungen auf Kontoebene außer Kraft setzen
- Deaktiviere Jira Sync auf Kontoebene
- Trennen Sie Ihre Verknüpfung mit Jira AWS-Konto

- Deinstalliere den Connector von deinem Jira-Konto

Um den Connector auf Kontoebene auszuschalten

> **Note**
>
> Die folgenden Schritte werden in Ihrem ausgeführt AWS-Konto.

1. Wählen Sie im linken Navigationsbereich Einstellungen aus.
2. Wähle im Bereich Synchronisieren von Jira-Konten die Option Bearbeiten aus.
3. Deaktivieren Sie die Option Synchronisation mit Jira-Konten aktivieren.
4. Wählen Sie Save settings (Einstellungen speichern).

Um die Verknüpfung zu einem aufzuheben AWS-Konto

> **Note**
>
> Alle folgenden Schritte werden in Ihrem Jira-Konto ausgeführt, nicht in Ihrem. AWS-Konto

1. Loggen Sie sich in Ihr Jira-Konto ein.
2. Wähle in der oberen Navigationsleiste Apps und dann Apps verwalten aus.
3. Wählen Sie den Dropdown-Pfeil neben AWS Well-Architected Tool Connector for Jira und wählen Sie dann Konfigurieren aus.
4. Wählen Sie im AWS Well-Architected Tool Konfigurationsbereich unter Aktionen die Option X aus AWS-Konto, um die Verknüpfung mit einem aufzuheben.

Um den Connector zu deinstallieren

> **Note**
>
> Alle folgenden Schritte werden in Ihrem Jira-Konto ausgeführt, nicht in Ihrem AWS-Konto. Wir empfehlen, in der Konfiguration des Connectors zu überprüfen, ob alle Verbindungen getrennt AWS-Konten sind, bevor Sie den Connector deinstallieren.

1. Loggen Sie sich in Ihr Jira-Konto ein.
2. Wähle in der oberen Navigationsleiste Apps und dann Apps verwalten aus.
3. Wählen Sie den Dropdown-Pfeil neben AWS Well-Architected Tool Connector for Jira aus.
4. Wählen Sie Deinstallieren und dann App deinstallieren.

Meilensteine

Ein Meilenstein zeichnet den Status eines Workloads zu einem bestimmten Zeitpunkt auf.

Speichern Sie einen Meilenstein, nachdem Sie zunächst alle Fragen im Zusammenhang mit einem Workload abgeschlossen haben. Wenn Sie Ihren Workload basierend auf Elementen in Ihrem Verbesserungsplan ändern, können Sie zusätzliche Meilensteine speichern, um den Fortschritt zu messen.

Eine bewährte Methode besteht darin, bei jeder Verbesserung eines Workloads einen Meilenstein zu speichern.

Speichern eines Meilensteins

Ein Meilenstein erfasst den aktuellen Status eines Workloads. Der Besitzer eines Workloads kann jederzeit einen Meilenstein speichern.

So speichern Sie einen Meilenstein

1. Wählen Sie auf der Detailseite des Workloads Save milestone (Meilenstein speichern) aus.
2. Geben Sie im Feld Milestone name (Name des Meilensteins) einen Namen für den Meilenstein ein.

   > **Note**
   >
   > Der Name muss zwischen 3 und 100 Zeichen lang sein. Mindestens drei Zeichen dürfen keine Leerzeichen sein. Einem Workload zugeordnete Meilensteinnamen müssen eindeutig sein. Leerzeichen und Groß-/Kleinschreibung werden ignoriert, wenn auf Eindeutigkeit geprüft wird.

3. Wählen Sie Save (Speichern) aus, um den Meilenstein zu speichern.

Nachdem ein Meilenstein gespeichert wurde, können Sie die Daten des Workloads, die erfasst wurden, nicht mehr ändern. Wenn Sie einen Workload löschen, werden die zugehörigen Meilensteine ebenfalls gelöscht.

Anzeigen von Meilensteinen

Sie können Meilensteine für einen Workload wie folgt anzeigen:

- Wählen Sie auf der Detailseite des Workloads Milestones (Meilensteine) und anschließend den Meilenstein aus, den Sie anzeigen möchten.
- Wählen Sie auf der Seite Dashboard den Workload aus und wählen Sie im Abschnitt Milestones (Meilensteine) den Meilenstein aus, den Sie anzeigen möchten.

Erstellen eines Meilensteinberichts

Sie können einen Meilensteinbericht erstellen. Der Bericht enthält die Antworten auf die Workload-Fragen, Ihre Notizen und alle hohen und mittleren Risiken, die beim Speichern des Meilensteins vorhanden waren.

Über einen Bericht können Sie Details zu den Meilenstein an andere Personen weitergeben, die keinen Zugriff auf das AWS Well-Architected Tool haben.

So erstellen Sie einen Meilensteinbericht

1. Wählen Sie den Meilenstein auf eine der folgenden Arten aus.
   - Wählen Sie auf der Detailseite des Workloads Milestones (Meilensteine) und anschließend den Meilenstein aus.
   - Wählen Sie auf der Seite Dashboard den Workload mit dem Meilenstein aus, über den Sie berichten möchten. Wählen Sie im Abschnitt Milestones (Meilensteine) den Meilenstein aus.
2. Wählen Sie Bericht erstellen aus, um einen Bericht zu erstellen.

   Die PDF-Datei wird generiert und Sie können sie anzeigen oder herunterladen.

Einladungen teilen

Eine Einladung zum Teilen ist eine Anfrage zur gemeinsamen Nutzung eines Workloads, einer benutzerdefinierten Linse oder einer Bewertungsvorlage, die einem anderen AWS Konto gehört. Ein Workload oder eine Linse kann mit allen Benutzern einer GruppeAWS-Konto, einzelnen Benutzern oder beiden gemeinsam genutzt werden.

- Wenn Sie eine Workload-Einladung annehmen, wird der Workload zu Ihren Workloads - und Dashboard-Seiten hinzugefügt.
- Wenn Sie eine Einladung zu einer benutzerdefinierten Linse annehmen, wird die Linse zu Ihrer Seite „Benutzerdefinierte Objektive“ hinzugefügt.
- Wenn Sie eine Profileinladung annehmen, wird das Profil zu Ihrer Profilseite hinzugefügt.
- Wenn Sie eine Einladung zur Bewertungsvorlage annehmen, wird die Vorlage zu Ihrer Seite mit Bewertungsvorlagen hinzugefügt.

Wenn Sie die Einladung ablehnen, wird sie aus der Liste entfernt.

> **Note**
>
> Workloads, benutzerdefinierte Objektive, Profile und Bewertungsvorlagen können nur innerhalb derselben AWS-Region Website gemeinsam genutzt werden.

Der Besitzer des Workloads oder der benutzerdefinierten Linse legt fest, wer gemeinsamen Zugriff hat.

Die Seite „Einladungen teilen“, die im linken Navigationsbereich verfügbar ist, enthält Informationen zu Ihren ausstehenden Workloads und zu benutzerdefinierten Lens-Einladungen.

Für jeden Workload werden die folgenden Informationen angezeigt:

Name

Der Name des Workloads, der benutzerdefinierten Linse oder der Bewertungsvorlage, die geteilt werden soll.

Ressourcentyp

Die Art der Einladung, entweder Workload, Benutzerdefiniertes Objektiv, Profile oder Bewertungsvorlage.

Eigentümer

Die AWS-Konto ID, der der Workload gehört.

Berechtigung

Die Berechtigung, die Ihnen für den Workload erteilt wird.

- Read-Only (Schreibgeschützt)

  Bietet schreibgeschützten Zugriff auf den Workload, die benutzerdefinierte Linse, die Profile oder die Bewertungsvorlage.

- Beitragender

  Bietet Aktualisierungszugriff auf Antworten und ihre Notizen sowie schreibgeschützten Zugriff auf den restlichen Workload. Diese Berechtigung ist nur für Workloads verfügbar.

Berechtigungsdetails

Detaillierte Beschreibung der Berechtigung.

Annahme einer Einladung zum Teilen

Um eine Einladung zum Teilen anzunehmen

1. Wählen Sie die Einladung zum Teilen aus, die Sie annehmen möchten.
2. Wählen Sie Accept (Akzeptieren) aus.

Bei Workload-Einladungen wird der Workload zu den Seiten Workloads und Dashboard hinzugefügt. Bei Einladungen mit benutzerdefinierten Objektiven wird die benutzerdefinierte Linse der Seite Benutzerdefinierte Objektive hinzugefügt. Bei Profileinladungen wird das Profil der Profilseite hinzugefügt. Für Einladungen zu Bewertungsvorlagen wird die Vorlage der Seite Vorlagen überprüfen hinzugefügt.

Sie haben sieben Tage Zeit, um eine Einladung anzunehmen. Wenn Sie die Einladung nicht innerhalb von sieben Tagen annehmen, wird sie automatisch abgelehnt.

Wenn ein Benutzer und AWS-Konto beide Benutzer Workload-Einladungen angenommen haben, bestimmt die Workload-Einladung für den Benutzer die Berechtigungen des Benutzers.

Eine Einladung zum Teilen ablehnen

Um eine Einladung zum Teilen abzulehnen

1. Wählen Sie die Einladung zum Workload oder zur benutzerdefinierten Linse aus, die Sie ablehnen möchten.
2. Wählen Sie Reject (Ablehnen).

Die Einladung wird aus der Liste entfernt.

Benachrichtigungen

Auf der Seite „Benachrichtigungen“ werden Versionsunterschiede für Workloads und Testvorlagen angezeigt, denen Objektive und Profile zugeordnet sind. Sie können auf der Seite „Benachrichtigungen“ ein Upgrade auf die neueste Version einer Linse oder eines Profils für einen Workload durchführen.

Benachrichtigungen für Objektive

Wenn eine neue Version eines Objektivs verfügbar ist, erscheint oben auf der Seite „Workloads“ oder „Vorlagen überprüfen“ ein Banner, das Sie darüber informiert. Wenn Sie eine bestimmte Workload- oder Review-Vorlage mit einer veralteten Linse betrachten, wird Ihnen auch ein Banner angezeigt, das darauf hinweist, dass eine neue Lens-Version verfügbar ist.

Wählen Sie Verfügbare Upgrades anzeigen, um eine Liste der Workloads oder Bewertungsvorlagen zu erhalten, die aktualisiert werden können.

Anweisungen the section called “Aktualisieren einer Linse” zur Aktualisierung eines Objektivs für einen Workload oder eine Bewertungsvorlage finden Sie unter.

Wenn der Besitzer einer gemeinsam genutzten Linse diese löscht und Sie mit der gelöschten Linse eine Arbeitslast verknüpft haben, erhalten Sie eine Benachrichtigung, dass Sie die Linse weiterhin in Ihrem bestehenden Workload verwenden können, aber Sie können sie nicht zu neuen Workloads hinzufügen.

Benachrichtigungen über das Profil

Es gibt zwei Arten von Profilbenachrichtigungen:

- Profil-Upgrade
- Löschen von Profilen

Wenn ein mit einem Workload verknüpftes Profil bearbeitet wurde (weitere Informationen finden Sie unterthe section called “Ein Profil bearbeiten”), wird unter Profilbenachrichtigungen eine Benachrichtigung angezeigt, dass es eine neue Version des Profils gibt.

Wenn der Besitzer eines geteilten Profils das Profil löscht und dem gelöschten Profil ein Workload zugeordnet ist, erhalten Sie eine Benachrichtigung, dass Sie das Profil weiterhin in Ihrem

vorhandenen Workload verwenden können, aber Sie können es nicht zu neuen Workloads hinzufügen.

Um eine Profilversion zu aktualisieren

1. Wählen Sie im linken Navigationsbereich Benachrichtigungen aus.
2. Wählen Sie den Namen des Workloads aus der Liste auf der Registerkarte Profilbenachrichtigungen aus, oder verwenden Sie die Suchleiste, um nach dem Workload-Namen zu suchen.
3. Wählen Sie die Upgrade-Profilversion aus.
4. Wählen Sie im Bereich Bestätigung das Bestätigungsfeld für Ich verstehe und akzeptiere diese Änderungen.
5. (Optional) Wenn Sie einen Meilenstein speichern möchten, aktivieren Sie das Feld Meilenstein speichern und geben Sie einen Meilensteinnamen ein.
6. Wählen Sie Save.

Sobald das Profil aktualisiert wurde, werden die neueste Versionsnummer und das Aktualisierungsdatum im Abschnitt Profil des Workloads angezeigt.

Weitere Informationen finden Sie unter Profile.

Dashboard

Das Dashboard, das im linken Navigationsbereich verfügbar ist, bietet Ihnen Zugriff auf Ihre Workloads und die damit verbundenen Probleme mit mittlerem und hohem Risiko. Sie können auch Workloads auf, die für Sie freigegeben wurden. Das Dashboard besteht aus vier Abschnitten.

- Zusammenfassung — Zeigt die Gesamtzahl der Workloads, die Anzahl der Workloads mit hohem und mittlerem Risiko sowie die Gesamtzahl der Probleme mit hohem und mittlerem Risiko für alle Workloads.
- Well-Architected Framework-Probleme pro Säule — Zeigt eine grafische Darstellung der Probleme mit hohem und mittlerem Risiko nach Säulen für all Ihre Workloads.
- Well-Architected Framework-Probleme pro Workload — Zeigt die Probleme mit hohem und mittlerem Risiko nach Säulen für jeden Ihrer Workloads an.
- Well-Architected Framework-Probleme nach Verbesserungsplanelementen — Zeigt die Elemente des Verbesserungsplans für all Ihre Workloads an.

Übersicht

Dieser Abschnitt zeigt die Gesamtzahl der Workloads und die Anzahl der Workloads mit Problemen mit hohem und mittlerem Risiko für die Well-Architected Framework-Linse und alle anderen Objektive. Die Gesamtzahl der Probleme mit hohem und mittlerem Risiko für alle Workloads, die entweder Ihnen gehören oder mit Ihnen geteilt wurdenAWS-Konto, wird angezeigt.

Wählen Sie „Für mich geteilte Workloads einbeziehen“, damit die zusammenfassenden Statistiken, der konsolidierte Bericht und die anderen Dashboard-Abschnitte sowohl Ihre Workloads als auch die Workloads, die mit Ihnen geteilt wurden, widerspiegeln.

Wählen Sie Bericht erstellen, um einen konsolidierten Bericht als PDF-Datei für Sie erstellen zu lassen.

Der Berichtsname hat die Form von:`wellarchitected_consolidatedreport_`*`account-ID`*`.pdf`.

Well-Architected Framework-Probleme pro Säule

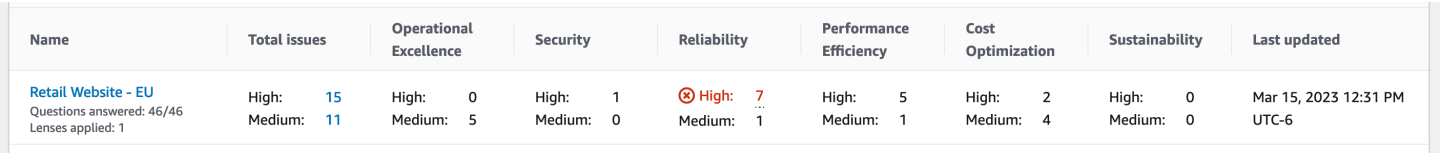
Der Abschnitt Well-Architected Framework-Probleme pro Säule zeigt eine grafische Darstellung der Anzahl der Probleme mit hohem und mittlerem Risiko pro Säule für alle Workloads.

Verwenden Sie die verbleibenden Abschnitte des Dashboards, um von einer Detailebene zur nächsten zu gelangen.

> **Note**
>
> In diesem Abschnitt sind nur Probleme aus der Well-Architected Framework-Linse enthalten.

Well-Architected Framework-Probleme pro Workload

Im Abschnitt Well-Architected Framework-Probleme pro Workload werden Informationen für jeden Workload angezeigt.



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

Für jede Workload werden die folgenden Informationen angezeigt:

Name

Name der Workload. Die Anzahl der beantworteten Fragen und die Anzahl der Objektive, die auf die Arbeitslast angewendet wurden, werden ebenfalls angezeigt.

Wählen Sie den Workload-Namen, um die Seite mit den Workload-Details aufzurufen und Meilensteine, Verbesserungspläne und Beteiligungen einzusehen.

Gesamtzahl der Probleme

Die Gesamtzahl der von der Well-Architected Framework-Linse identifizierten Probleme für den Workload.

Wählen Sie die Anzahl der Probleme mit hohem oder mittlerem Risiko aus, um die empfohlenen Verbesserungspläne für diese Probleme einzusehen.

Operative Exzellenz

Die Anzahl der Probleme mit hohem Risiko (HRIs) und mit mittlerem Risiko (MRIs), die im Rahmen des Workloads für den Pfeiler Operational Excellence identifiziert wurden.

Sicherheit

Die Anzahl der für den Pfeiler Sicherheit identifizierten HRIs und MRIs.

Zuverlässigkeit

Die Anzahl der HRI und MRT, die für den Pfeiler Zuverlässigkeit identifiziert wurden.

Leistungseffizienz

Die Anzahl der HRIs und MRIs, die für den Pfeiler Leistungseffizienz identifiziert wurden.

Kostenoptimierung

Die Anzahl der HRIs und MRIs, die für den Pfeiler Kostenoptimierung identifiziert wurden.

Nachhaltigkeit

Die Anzahl der HRIs und MRIs, die für die Säule Nachhaltigkeit identifiziert wurden.

Letzte Aktualisierung

Datum und die Uhrzeit, zu dem/der der Workload zuletzt aktualisiert wurde.

Für jeden Workload wird die Säule mit der höchsten Anzahl von Hochrisikoproblemen (HRIs) hervorgehoben.

> **Note**
>
> In diesem Abschnitt sind nur Probleme aus der Well-Architected Framework-Linse enthalten.

Well-Architected Framework-Probleme nach Elementen des Verbesserungsplans

Im Abschnitt Well-Architected Framework-Probleme nach Verbesserungsplanelementen werden die Elemente des Verbesserungsplans für all Ihre Workloads angezeigt. Sie können die Elemente nach Säule und Schweregrad filtern.

Die folgenden Informationen werden für jeden mit dem Verbesserungsplan werden für jeden freigeben, der für den Verbesserungsplan wurde

Verbesserungsobjekt

Der Name des Elements des Verbesserungsplans.

Wählen Sie den Namen, um die bewährte Methode anzuzeigen, die dem Element des Verbesserungsplans zugeordnet ist.

Säule

Die Säule, die dem Verbesserungsobjekt zugeordnet ist.

Risk

Gibt an, ob das damit verbundene Problem ein hohes oder mittleres Risiko darstellt.

Anwendbare Workloads werden

Die Anzahl der Workloads, für die dieser Verbesserungsplan gilt.

Wählen Sie ein Element des Verbesserungsplans aus, um die entsprechenden Workloads zu sehen.

> **Note**
>
> In diesem Abschnitt sind nur Elemente des Verbesserungsplans aus der Well-Architected Framework-Linse enthalten.

Sicherheit im AWS Well-Architected Tool

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und als Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für AWS Well-Architected Tool gelten, finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von AWS WA Tool einsetzen können. Die folgenden Themen veranschaulichen, wie Sie AWS WA Tool zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre AWS WA Tool-Ressourcen zu überwachen und zu schützen.

Themen

- Serviceübergreifende Confused-Deputy-Prävention

Datenschutz in AWS Well-Architected Tool

Das Modell der geteilten Verantwortung von AWS gilt für den Datenschutz in AWS Well-Architected Tool. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein. Informationen zur Verwendung von CloudTrail-Trails zur Erfassung von AWS-Aktivitäten finden Sie unter Arbeiten mit CloudTrail-Trails im AWS CloudTrail-Benutzerhandbuch.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der

AWS WA Tool oder anderen AWS-Services über die Konsole, API, AWS CLI oder AWS-SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Alle von AWS WA Tool gespeicherten Daten sind im Ruhezustand verschlüsselt.

Verschlüsselung während der Übertragung

Alle Daten, die an und von AWS WA Tool gesendet werden, werden während der Übertragung verschlüsselt.

So verwendet AWS Ihre Daten

Das AWS Well-Architected-Team sammelt aggregierte Daten aus AWS Well-Architected Tool, um den AWS WA Tool-Service für Kunden bereitzustellen und zu verbessern. Einzelne Kundendaten können für AWS-Konto-Teams freigegeben werden, um die Bemühungen unserer Kunden zur Verbesserung ihrer Workloads und ihrer Architektur zu unterstützen. Das AWS Well-Architected-Team kann nur auf Workload-Eigenschaften und ausgewählte Optionen für jede Frage zugreifen. AWS gibt keine Daten aus dem AWS WA Tool außerhalb von AWS frei.

Das AWS Well-Architected-Team hat unter anderem Zugriff auf folgende Workload-Eigenschaften:

- Name des Workloads
- Eigentümer überprüfen
- Umgebung
- Regionen
- Konto-IDs
- Industrietyp

Das AWS Well-Architected-Team hat keinen Zugriff auf:

- Beschreibung des Workloads
- Architektur-Design

- Notizen, die Sie eingegeben haben

Identity and Access Management für AWS Well-Architected Tool

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, um AWS WA Tool Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS WA Tool.

Service-Benutzer: Wenn Sie den AWS WA Tool-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere AWS WA Tool-Features ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung für AWS Well-Architected Tool-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS WA Tool haben.

Service-Administrator: Wenn Sie in Ihrem Unternehmen für AWS WA Tool-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf AWS WA Tool. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS WA Tool-Features und Ressourcen Ihre Service-Benutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die

Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit AWS WA Tool verwenden kann, finden Sie unter Funktionsweise von AWS Well-Architected Tool mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS WA Tool verfassen können. Beispiele für identitätsbasierte AWS WA Tool-Richtlinien, die Sie in IAM verwenden können, finden Sie unter AWS Well-Architected ToolBeispiele für identitätsbasierte -Richtlinien.

Authentifizierung mit Identitäten

Sie melden sich über eine Authentifizierung mit Ihren Anmeldeinformationen bei AWS an. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuerten Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS empfiehlt beispielsweise die Verwendung der Multi-Faktor-Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges

Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der AWS Management Console zu übernehmen, können Sie von einem Benutzer zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI- oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil,

das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter

Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen und SCPs finden Sie unter Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) – RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbare Zahl von Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource in Ihrem Besitz angefügt sind. Die RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organisationen und RCPs, einschließlich einer Liste von AWS-Services, die RCPs unterstützen, finden Sie unter Ressourcenkontrollrichtlinien (RCPs) im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Funktionsweise von AWS Well-Architected Tool mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf AWS WA Tool verwenden, erfahren Sie, welche IAM-Funktionen Sie mit AWS WA Tool verwenden können.

IAM-Funktionen, die Sie mit AWS Well-Architected Tool verwenden können

IAM-Feature	AWS WA Tool-Support
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen Überblick über das Zusammenwirken von AWS WA Tool und anderen AWS-Services mit den meisten IAM-Funktionen finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte AWS WA Tool-Richtlinien

Unterstützt Richtlinienaktionen: Ja

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Ressourcenbasierte Richtlinien in AWS WA Tool

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto

auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS WA Tool

Unterstützt Richtlinienaktionen: Ja

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in AWS WA Tool verwenden das folgende Präfix vor der Aktion: `wellarchitected:`. Wenn eine Entity z. B. eine Workload definieren soll, muss ein Administrator eine Richtlinie anfügen, die `wellarchitected:CreateWorkload`-Aktionen zulässt. Um zu verhindern, dass eine Entity Workloads löscht, kann ein Administrator dementsprechend eine Richtlinie anfügen, die `wellarchitected:DeleteWorkload`-Aktionen verweigert. Richtlinienanweisungen müssen ein `Action`- oder `NotAction`-Element enthalten. AWS WA Tool definiert seinen eigenen Satz an Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Eine Liste der AWS WA Tool-Aktionen finden Sie unter Von AWS Well-Architected Tool definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienressourcen

Unterstützt Richtlinienressourcen: Ja

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS WA Tool-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Well-Architected Tool definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Well-Architected Tool definierte Aktionen.

Die AWS WA Tool-Workload-Ressource verfügt über den folgenden ARN:

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

Weitere Informationen zum Format von ARNs finden Sie unter Amazon-Ressourcennamen (ARNs) und AWS-Service-Namespaces.

Der ARN befindet sich auf der Seite Workload properties (Workload-Eigenschaften) für eine Workload. So geben Sie beispielsweise eine bestimmte Workload an:

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

Um alle Workloads anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

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

Einige AWS WA Tool-Aktionen, z. B. zum Erstellen und Auflisten von Workloads, können auf bestimmten Ressourcen nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

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

Eine Liste der AWS WA Tool-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Well-Architected Tool definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Well-Architected Tool definierte Aktionen.

Richtlinien-Bedingungsschlüssel für AWS WA Tool

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

AWS WA Tool stellt einen einzelnen servicespezifischen Bedingungsschlüssel bereit (`wellarchitected:JiraProjectKey`), unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel in der Service-Authorization-Referenz.

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

ACLs in AWS WA Tool

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Autorisierung auf der Basis von AWS WA Tool-Tags

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS WA Tool

Unterstützt temporäre Anmeldeinformationen: Ja

Einige AWS-Services funktionieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche AWS-Services mit temporären Anmeldeinformationen funktionieren, finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipal-Berechtigungen für AWS WA Tool

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS WA Tool

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Serviceverknüpfte Rollen für AWS WA Tool

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der

Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

AWS Well-Architected ToolBeispiele für identitätsbasierte -Richtlinien

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS WA Tool-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben ausführen, die die AWS Management Console-, – AWS CLIoder AWS-API benutzen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS WA Tool-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Erteilen von vollem Zugriff auf Workloads
- Erteilen von Lesezugriff auf Workloads
- Zugreifen auf einen einzelnen Workload
- Verwenden eines servicespezifischen Bedingungsschlüssels für den AWS Well-Architected Tool-Konnektor für Jira

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS WA Tool-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine

Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS WA Tool-Konsole

Um auf die AWS Well-Architected Tool-Konsole zuzugreifen, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen Ihnen das Auflisten und Anzeigen von Details zu den AWS WA Tool-Ressourcen in Ihrem AWS-Konto gestatten. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten die AWS WA Tool-Konsole weiterhin verwenden können, weisen Sie den Entitäten auch die folgende AWS-verwaltete Richtlinie zu:

```
WellArchitectedConsoleReadOnlyAccess
```

Um das Erstellen, Ändern und Löschen von Workloads zuzulassen, weisen Sie den Entitäten die folgende AWS-verwaltete Richtlinie zu:

```
WellArchitectedConsoleFullAccess
```

Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

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

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Erteilen von vollem Zugriff auf Workloads

In diesem Beispiel möchten Sie einem Benutzer in Ihrem AWS-Konto vollen Zugriff auf Ihre Workloads erteilen. Der Vollzugriff ermöglicht es dem Benutzer, alle Aktionen in AWS WA Tool auszuführen. Dieser Zugriff ist erforderlich, um Workloads zu definieren, Workloads zu löschen, Workloads anzuzeigen und Workloads zu aktualisieren.

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

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

Erteilen von Lesezugriff auf Workloads

In diesem Beispiel möchten Sie einem Benutzer in Ihrem AWS-Konto Lesezugriff auf Ihre Workloads erteilen. Der schreibgeschützte Zugriff ermöglicht es dem Benutzer nur, Workloads in AWS WA Tool anzuzeigen.

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

Zugreifen auf einen einzelnen Workload

In diesem Beispiel möchten Sie einem Benutzer in Ihrem AWS-Konto Lesezugriff auf einen Ihrer Workloads (99999999999955555555555566666666) in der Region `us-west-2` erteilen. Ihre Konto-ID ist 777788889999.

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555566666666"
```

```
      }
    ]
}
```

Verwenden eines servicespezifischen Bedingungsschlüssels für den AWS Well-Architected Tool-Konnektor für Jira

Dieses Beispiel zeigt, wie Sie mithilfe des servicespezifischen Bedingungsschlüssels `wellarchitected:JiraProjectKey` festlegen, welche Jira-Projekte mit Workloads in Ihrem Konto verknüpft werden können.

Im Folgenden werden relevante Verwendungen für den Bedingungsschlüssel beschrieben:

- **`CreateWorkload`:** Wenn Sie `wellarchitected:JiraProjectKey` auf `CreateWorkload` anwenden, können Sie definieren, welche benutzerdefinierten Jira-Projekte mit einem vom Benutzer erstellten Workload verknüpft werden können. Wenn ein Benutzer beispielsweise versucht, einen neuen Workload mit dem Projekt ABC zu erstellen, die Richtlinie aber das Projekt PQR spezifiziert, wird die Aktion abgelehnt.
- **`UpdateWorkload`:** Wenn Sie `wellarchitected:JiraProjectKey` auf `UpdateWorkload` anwenden, können Sie definieren, welche benutzerdefinierten Jira-Projekte mit diesem oder einem beliebigen Workload verknüpft werden können. Wenn ein Benutzer beispielsweise versucht, einen vorhandenen Workload mit dem Projekt ABC zu erstellen, die Richtlinie aber das Projekt PQR spezifiziert, wird die Aktion abgelehnt. Wenn der Benutzer einen Workload erstellt hat, der mit dem Projekt PQR verknüpft ist, und versucht, den Workload so zu aktualisieren, dass er mit dem Projekt ABC verknüpft wird, wird die Aktion abgelehnt.
- **`UpdateGlobalSettings`:** Wenn Sie `wellarchitected:JiraProjectKey` auf `UpdateGlobalSettings` anwenden, können Sie definieren, welche benutzerdefinierten Jira-Projekte mit dem AWS-Konto verknüpft werden können. Die Einstellung auf Kontoebene schützt Workloads in Ihrem Konto, die die Jira-Einstellungen auf Kontoebene nicht überschreiben. Wenn ein Benutzer beispielsweise Zugriff auf `UpdateGlobalSettings` hat, kann er Workloads in Ihrem Konto nicht mit Projekten verknüpfen, die in der Richtlinie nicht angegeben werden.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
```

```
    "Action": [
     "wellarchitected:UpdateGlobalSettings",
     "wellarchitected:CreateWorkload"
    ],
    "Resource": "*",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   },
   {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
     "wellarchitected:UpdateWorkload"
    ],
    "Resource": "WORKLOAD_ARN",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   }
  ]
}
```

Von AWS verwaltete Richtlinien für AWS Well-Architected Tool

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass von AWS verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS-Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus,

denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS-verwaltete Richtlinie: WellArchitectedConsoleFullAccess

Sie können die `WellArchitectedConsoleFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt vollen Zugriff auf AWS Well-Architected Tool.

Details zu Berechtigungen

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

AWS-verwaltete Richtlinie: WellArchitectedConsoleReadOnlyAccess

Sie können die `WellArchitectedConsoleReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie erteilt AWS Well-Architected Tool Lesezugriff.

Details zu Berechtigungen

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

```
      "Effect" : "Allow",
      "Action" : [
           "wellarchitected:Get*",
           "wellarchitected:List*"
           "wellarchitected:ExportLens"
      ],
      "Resource": "*"
      }
   ]
}
```

AWS-verwaltete Richtlinie: AWSWellArchitectedOrganizationsServiceRolePolicy

Sie können die `AWSWellArchitectedOrganizationsServiceRolePolicy`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie erteilt Administratorberechtigungen in AWS Organizations, die zur Unterstützung der AWS Well-Architected Tool-Integration mit Organizations erforderlich sind. Diese Berechtigungen ermöglichen dem Organisationsverwaltungskonto die Aktivierung der Ressourcenfreigabe für AWS WA Tool.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations:ListAWSServiceAccessForOrganization` – Ermöglicht Prinzipalen die Überprüfung, ob der AWS-Servicezugriff für AWS WA Tool aktiviert ist.
- `organizations:DescribeAccount` – Ermöglicht Prinzipalen den Abruf von Informationen über ein Konto in der Organisation.
- `organizations:DescribeOrganization` – Ermöglicht Prinzipalen den Abruf von Informationen über die Konfiguration der Organisation.
- `organizations:ListAccounts` – Ermöglicht Prinzipalen den Abruf der Liste der Konten, die zu einer Organisation gehören.
- `organizations:ListAccountsForParent` – Ermöglicht Prinzipalen den Abruf der Liste der Konten, die zu einer Organisation gehören, von einem angegebenen Stammknoten in der Organisation.
- `organizations:ListChildren` – Ermöglicht Prinzipalen den Abruf der Liste der Konten und Organisationseinheiten, die zu einer Organisation gehören, von einem angegebenen Stammknoten in der Organisation.

- `organizations:ListParents` – Ermöglicht Prinzipalen den Abruf der Liste der unmittelbaren übergeordneten Elemente, die von der Organisationseinheit oder einem Konto innerhalb einer Organisation angegeben werden.
- `organizations:ListRoots` – Ermöglicht Prinzipalen den Abruf der Liste aller Stammknoten innerhalb einer Organisation.

```
{
    "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-verwaltete Richtlinie: AWSWellArchitectedDiscoveryServiceRolePolicy

Sie können die `AWSWellArchitectedDiscoveryServiceRolePolicy`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie ermöglicht AWS Well-Architected Tool den Zugriff auf AWS-Services und -Ressourcen im Zusammenhang mit AWS WA Tool-Ressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `trustedadvisor:DescribeChecks` – Listet die verfügbaren Trusted Advisor-Überprüfungen auf.

- `trustedadvisor:DescribeCheckItems` – Ruft Trusted Advisor-Überprüfungsdaten ab, einschließlich Status und Ressourcen, die von Trusted Advisor markiert wurden.
- `servicecatalog:GetApplication` – Ruft Details einer AppRegistry-Anwendung ab.
- `servicecatalog:ListAssociatedResources` – Listet Ressourcen auf, die einer AppRegistry-Anwendung zugeordnet sind.
- `cloudformation:DescribeStacks` – Ruft Details zu AWS CloudFormation-Stacks ab.
- `cloudformation:ListStackResources` – Listet die den AWS CloudFormation-Stacks zugeordneten Ressourcen auf.
- `resource-groups:ListGroupResources` – Listet Ressourcen aus einer ResourceGroup auf.
- `tag:GetResources` – Erforderlich für ListGroupResources.
- `servicecatalog:CreateAttributeGroup` – Erstellt eine serviceverwaltete Attributgruppe, wenn erforderlich.
- `servicecatalog:AssociateAttributeGroup` – Ordnet einer AppRegistry-Anwendung eine serviceverwaltete Attributgruppe zu.
- `servicecatalog:UpdateAttributeGroup` – Aktualisiert eine serviceverwaltete Attributgruppe.
- `servicecatalog:DisassociateAttributeGroup` – Trennt eine serviceverwaltete Attributgruppe von einer AppRegistry-Anwendung.
- `servicecatalog:DeleteAttributeGroup` – Löscht eine serviceverwaltete Attributgruppe, wenn erforderlich.

```
{
 "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-Aktualisierungen für AWS-verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für AWS WA Tool, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS WA Tool-Dokumentverlauf.

Änderung	Beschreibung	Datum
Änderung für AWS WA Tool-verwaltete Richtlinien	Hinzufügung von `"wellarchitected:Export*"` zu `WellArchitectedConsoleReadOnlyAccess` .	22. Juni 2023
Hinzufügung einer AWS WA Tool-Richtlinie für Servicerollen	Hinzufügung von `AWSWellArchitectedDiscoveryServiceRolePolicy` , um AWS Well-Architected Tool den Zugriff auf AWS-Services und -Ressourcen zu erteilen, die im Zusammenhang mit AWS WA Tool-Ressourcen stehen.	3. Mai 2023
Hinzufügung von AWS WA Tool-Berechtigungen	Hinzufügung einer neuen Aktion, um `ListAWSServiceAccessForOrganization` die Berechtigung zu erteilen, AWS WA Tool die Überprüfung zu gestatten, ob der AWS-Servicezugriff für AWS WA Tool aktiviert ist.	22. Juli 2022
AWS WA Tool hat die Änderungsverfolgung gestartet	AWS WA Tool hat mit der Verfolgung von Änderungen für seine AWS-verwalteten Richtlinien begonnen.	22. Juli 2022

Fehlerbehebung für AWS Well-Architected Tool-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit AWS WA Tool und IAM auftreten könnten.

Themen

- Ich bin nicht autorisiert, eine Aktion in AWS WA Tool auszuführen

Ich bin nicht autorisiert, eine Aktion in AWS WA Tool auszuführen

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Fehler tritt beispielsweise auf, wenn der Benutzer *mateojackson* versucht, die Konsole zur Ausführung der Aktion `DeleteWorkloadDeleteWorkload` zu verwenden, jedoch keine Berechtigungen hierfür besitzt.

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

Bitten Sie in diesem Beispiel Ihren Administrator, Ihre Richtlinien zu aktualisieren, damit Sie über die Aktion `wellarchitected:DeleteWorkload` auf die Ressource `11112222333344445555666677778888` zugreifen können.

Vorfallreaktion in AWS Well-Architected Tool

Die Reaktion auf Vorfälle für die AWS Well-Architected Tool liegt in der Verantwortung von AWS. AWS verfügt über eine formelle, dokumentierte Richtlinie und ein Programm, die/das die Reaktion auf Vorfälle regelt.

Operative AWS-Probleme mit weitreichenden Auswirkungen werden auf dem AWS Service Health Dashboard gepostet.

Operative Probleme werden über AWS Health Dashboard auch in den einzelnen Konten veröffentlicht. Weitere Informationen zur Verwendung von AWS Health Dashboard finden Sie im AWS Health-Benutzerhandbuch.

Compliance-Validierung für AWS Well-Architected Tool

Informationen dazu, ob ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services im Geltungsbereich nach Compliance-Programm. Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-berechtigt.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS-Compliance-Leitfäden für Kunden – Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Auswertung von Ressourcen mit Regeln im AWS Config-Entwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Verfahren, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub: Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty – Dieser AWS-Service erkennt potenzielle Bedrohungen für Ihre AWS-Konten, Workloads, Container und Daten, indem er Ihre Umgebung auf verdächtige und böswillige

Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedenen Compliance-Anforderungen wie PCI DSS nachzukommen, indem es die Anforderungen zur Erkennung von Eindringlingen erfüllt, die in bestimmten Compliance-Frameworks vorgeschrieben sind.

- AWS Audit Manager – Dies AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Ausfallsicherheit in AWS Well-Architected Tool

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Sicherheit der Infrastruktur in AWS Well-Architected Tool

Als verwalteter Service ist AWS Well-Architected Tool durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter AWS-Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf AWS WA Tool zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Konfigurations- und Schwachstellenanalyse in AWS Well-Architected Tool

Konfiguration und IT-Steuerelemente unterliegen der übergreifenden Verantwortlichkeit von AWS und Ihnen, unserem Kunden. Weitere Informationen finden Sie unter AWSModell der übergreifenden Verantwortlichkeit.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine Entität mit größeren Rechten zwingen kann, die Aktion auszuführen. In AWS kann der serviceübergreifende Identitätswechsel zu Confused-Deputy-Problem führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die AWS Well-Architected Tool einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (`*`) für die unbekannten Teile des ARN. Beispiel, `arn:aws:wellarchitected:*:123456789012:*`.

Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken.

Der Wert von `aws:SourceArn` muss ein Workload oder eine Lens sein.

Das folgende Beispiel zeigt, wie Sie die globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in AWS WA Tool verwenden können, um das Problem des verwirrten Stellvertreters zu vermeiden.

```
{
  "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"
      }
    }
  }
}
```

Teilen Sie Ihre AWS WA Tool Ressourcen

Gehen Sie wie folgt vor, um eine Ressource, die Sie besitzen, mit anderen zu teilen:

- Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations (optional)
- Teilen Sie sich einen Workload
- Teilen Sie ein benutzerdefiniertes Objektiv
- Teilen Sie ein Profil
- Teilen Sie eine Bewertungsvorlage

Hinweise

- Wenn Sie eine Ressource gemeinsam nutzen, steht sie auch anderen Benutzern zur VerfügungAWS-Konto, die die Ressource erstellt haben. Durch das Teilen werden keine Berechtigungen geändert, die für die Ressource in dem Konto gelten, mit dem sie erstellt wurde.
- AWS WA Toolist ein regionaler Dienst. Die Prinzipale, für die Sie die gemeinsame Nutzung verwenden, können nur auf die Ressourcenfreigaben zugreifen, AWS-Regionen in der sie erstellt wurden.
- Um Ressourcen in einer Region gemeinsam zu nutzen, die nach dem 20. März 2019 eingeführt wurde, AWS-Konto müssen sowohl Sie als auch die gemeinsam genutzte Region die Region in der AWS Management Console aktivieren. Weitere Informationen finden Sie unter AWSGlobale Infrastruktur.

Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations

Wenn Ihr Konto von verwaltet wirdAWS Organizations, können Sie dies nutzen, um Ressourcen einfacher gemeinsam zu nutzen. Mit oder ohne Organizations kann ein Benutzer Inhalte mit einzelnen Konten teilen. Wenn sich Ihr Konto jedoch in einer Organisation befindet, können Sie Inhalte für einzelne Konten oder für alle Konten in der Organisation oder in einer Organisationseinheit freigeben, ohne jedes Konto aufzählen zu müssen.

Um Ressourcen innerhalb einer Organisation gemeinsam zu nutzen, müssen Sie zuerst die AWS WA Tool Konsole verwenden oder AWS Command Line Interface (AWS CLI), um das Teilen mit zu aktivieren. AWS Organizations Wenn Sie Ressourcen in Ihrer Organisation gemeinsam nutzen, sendet AWS WA Tool keine Einladungen an Schulleiter. Principals in Ihrer Organisation erhalten Zugriff auf gemeinsam genutzte Ressourcen, ohne Einladungen austauschen zu müssen.

Wenn Sie die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation aktivieren, AWS WA Tool wird eine dienstbezogene Rolle mit dem Namen erstellt. `AWSServiceRoleForWellArchitected` Diese Rolle kann nur vom AWS WA Tool Dienst übernommen werden und gewährt die AWS WA Tool Berechtigung, mithilfe der AWS verwalteten Richtlinie `AWSWellArchitectedOrganizationsServiceRolePolicy` Informationen über die Organisation abzurufen, der er angehört.

Wenn Sie Ressourcen nicht mehr für Ihre gesamte Organisation oder Organisationseinheiten gemeinsam nutzen müssen, können Sie die gemeinsame Nutzung von Ressourcen deaktivieren.

Voraussetzungen

- Sie können diese Schritte nur ausführen, wenn Sie als Principal im Verwaltungskonto der Organisation angemeldet sind.
- In der Organisation müssen alle Funktionen aktiviert sein. Weitere Informationen finden Sie im AWS OrganizationsBenutzerhandbuch unter Alle Funktionen in Ihrer Organisation aktivieren.

> **Important**
>
> Sie müssen das Teilen mit AWS Organizations über die AWS WA Tool Konsole aktivieren. Dadurch wird sichergestellt, dass die `AWSServiceRoleForWellArchitected`-serviceverknüpfte Rolle erstellt wird. Wenn Sie den vertrauenswürdigen Zugriff mit AWS Organizations mithilfe der AWS Organizations Konsole oder des enable-aws-service-accessAWS CLIBefehls aktivieren, wird die `AWSServiceRoleForWellArchitected` dienstbezogene Rolle nicht erstellt, und Sie können Ressourcen innerhalb Ihrer Organisation nicht gemeinsam nutzen.

Um die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.

Sie müssen sich als Principal im Verwaltungskonto der Organisation anmelden.

2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Wählen Sie AWS OrganizationsSupport aktivieren aus.
4. Wählen Sie Save settings (Einstellungen speichern).

Um die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation zu deaktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.

   Sie müssen sich als Principal im Verwaltungskonto der Organisation anmelden.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Deaktivieren Sie die Option AWS OrganizationsSupport aktivieren.
4. Wählen Sie Save settings (Einstellungen speichern).

Markieren Ihrer AWS WA Tool-Ressourcen

Um Sie bei der Verwaltung Ihrer AWS WA Tool-Ressourcen zu unterstützen, können Sie jeder Ressource eigene Metadaten in Form von Tags zuweisen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

Inhalt

Grundlagen zu Tags (Markierungen)

Ein Tag (Markierung) ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen.

Mit Tags können Sie Ihre AWS-Ressourcen kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Wenn Sie viele Ressourcen desselben Typs haben, können Sie bestimmte Ressourcen basierend auf den zugewiesenen Tags schnell bestimmen. Sie können beispielsweise eine Reihe von Tags für Ihre AWS WA Tool-Cluster definieren. Diese helfen Ihnen, den Besitzer und die Stack-Ebene jedes einzelnen Clusters nachzuverfolgen. Sie sollten für jeden Ressourcentyp einen konsistenten Satz von Tag-Schlüsseln entwickeln.

Tags werden nicht automatisch Ihren Ressourcen zugewiesen. Nachdem Sie ein Tag hinzugefügt haben, können Sie jederzeit Tag-Schlüssel und -Werte bearbeiten oder Tags aus einer Ressource entfernen. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Tags haben keine semantische Bedeutung für AWS WA Tool und werden ausschließlich als Zeichenfolgen interpretiert. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht Null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben.

Sie können mit der AWS Management Console, AWS CLI und AWS WA Tool-API mit Tags arbeiten.

Wenn Sie AWS Identity and Access Management (IAM) verwenden, können Sie steuern, welche Benutzer in Ihrem Umfeld die Berechtigung AWS-Konto haben, Tags zu erstellen, zu bearbeiten oder zu löschen.

Markieren Ihrer -Ressourcen

Sie können neue oder bestehende AWS WA Tool Ressourcen taggen.

Wenn Sie die AWS WA Tool Konsole verwenden, können Sie Tags auf neue Ressourcen anwenden, wenn diese erstellt werden, oder auf vorhandene Ressourcen jederzeit. Für bestehende Workloads können Sie Tags über die Registerkarte Eigenschaften anwenden. Für bestehende benutzerdefinierte Objektive, Profile und Bewertungsvorlagen können Sie über den Tab „Übersicht“ Tags hinzufügen.

Wenn Sie die AWS WA Tool-API, die AWS CLI oder ein AWS-SDK verwenden, können Sie Tags mithilfe des Parameters `tags` auf neue Ressourcen oder mithilfe der API-Aktion `TagResource` auf vorhandene Ressourcen anwenden. Weitere Informationen finden Sie unter TagResource.

Bei einigen Aktionen zur Ressourcenerstellung können Sie Tags für eine Ressource angeben, wenn die Ressource erstellt wird. Wenn Tags während der Ressourcenerstellung nicht angewendet werden können, schlägt die Ressourcenerstellung fehl. Auf diese Weise wird sichergestellt, dass Ressourcen, die Sie bei der Erstellung markieren möchten, entweder mit angegebenen Tags oder gar nicht erstellt werden. Wenn Sie Ressourcen zum Zeitpunkt der Erstellung markieren, müssen Sie nach der Ressourcenerstellung keine benutzerdefinierten Tagging-Skripts ausführen.

In der folgenden Tabelle werden die markierbaren AWS WA Tool-Ressourcen und die bei Erstellung markierbaren Ressourcen beschrieben.

Markierungsunterstützung für AWS WA Tool-Ressourcen

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Tag-Propagierung	Unterstützt das Markieren bei Erstellung (AWS WA Tool-API, AWS CLI, AWS-SDK)
AWS WA ToolArbeitslasten	Ja	Nein	Ja

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Tag-Propagierung	Unterstützt das Markieren bei Erstellung (AWS WA Tool-API, AWS CLI, AWS-SDK)
AWS WA Toolkundenspezifische Objektive	Ja	Nein	Ja
AWS WA ToolProfile	Ja	Nein	Ja
AWS WA ToolVorlagen überprüfen	Ja	Nein	Ja

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 256 Unicode-Zeichen in UTF-8
- Wenn Ihr Markierungsschema für mehrere AWS-Services und -Ressourcen verwendet wird, denken Sie daran, dass andere Services möglicherweise Einschränkungen für zulässige Zeichen haben. Allgemein erlaubte Zeichen sind Buchstaben, Zahlen, Leerzeichen, die in UTF-8 darstellbar sind, sowie die folgenden Zeichen: + - = . _ : / @.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Verwenden Sie weder `aws:` noch `AWS:` oder Kombinationen aus Groß- und Kleinbuchstaben von diesen als Präfix für Schlüssel oder Werte, da sie für die AWS-Verwendung reserviert sind. Sie können keine Tag-Schlüssel oder -Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht auf Ihr tags-per-resource Limit angerechnet.

Arbeiten mit Tags über die Konsole

Mithilfe der AWS WA Tool Konsole können Sie die Tags verwalten, die neuen oder vorhandenen Ressourcen zugeordnet sind.

Hinzufügen von Tags zu einer einzelnen Ressource bei der Erstellung

Sie können AWS WA Tool Ressourcen bei der Erstellung Tags hinzufügen.

Hinzufügen und Löschen von Tags für einzelne Ressourcen

AWS WA Toolermöglicht es Ihnen, mit Ihren Ressourcen verknüpfte Tags direkt von der Registerkarte Eigenschaften für einen Workload und von der Registerkarte Übersicht für benutzerdefinierte Objektive, Profile und Bewertungsvorlagen aus hinzuzufügen oder zu löschen.

Um ein Tag zu einem Workload hinzuzufügen oder zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie in der Navigationsleiste die Region aus, die Sie verwenden möchten.
3. Wählen Sie im Navigationsbereich Workloads aus.
4. Wählen Sie den zu ändernden Workload aus und klicken Sie auf Eigenschaften.
5. Wählen Sie im Abschnitt Tags (Markierungen) die Option Manage tags (Tags (Markierungen) verwalten).
6. Fügen Sie Ihre Tags nach Bedarf hinzu oder löschen Sie sie.
   - Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und füllen Sie die Felder Schlüssel und Wert aus.
   - Zum Entfernen eines Tags wählen Sie Remove (Entfernen).
7. Wiederholen Sie diesen Vorgang für jedes Tag, das Sie hinzufügen, ändern oder löschen möchten. Wählen Sie Save (Speichern), um Ihre Änderungen zu speichern.

Um eine Markierung auf einer benutzerdefinierten Linse hinzuzufügen oder zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie in der Navigationsleiste die Region aus, die Sie verwenden möchten.

3. Wählen Sie im Navigationsbereich die Option Benutzerdefinierte Objektive aus.
4. Wählen Sie den Namen der benutzerdefinierten Linse aus, die Sie ändern möchten.
5. Wählen Sie auf der Registerkarte „Übersicht“ im Abschnitt „Tags“ die Option „Tags verwalten“.
6. Fügen Sie nach Bedarf Ihre Tags hinzu oder löschen Sie sie.
   - Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und füllen Sie die Felder Schlüssel und Wert aus.
   - Zum Entfernen eines Tags wählen Sie Remove (Entfernen).
7. Wiederholen Sie diesen Vorgang für jedes Tag, das Sie hinzufügen, ändern oder löschen möchten. Wählen Sie Save (Speichern), um Ihre Änderungen zu speichern.

Um ein Tag zu einem Profil hinzuzufügen oder zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie in der Navigationsleiste die Region aus, die Sie verwenden möchten.
3. Wählen Sie im Navigationsbereich Profile aus.
4. Wählen Sie den Namen des zu ändernden Profils aus.
5. Wählen Sie auf der Registerkarte „Übersicht“ im Abschnitt „Tags“ die Option „Tags verwalten“ aus.
6. Fügen Sie nach Bedarf Ihre Tags hinzu oder löschen Sie sie.
   - Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und füllen Sie die Felder Schlüssel und Wert aus.
   - Zum Entfernen eines Tags wählen Sie Remove (Entfernen).
7. Wiederholen Sie diesen Vorgang für jedes Tag, das Sie hinzufügen, ändern oder löschen möchten. Wählen Sie Save (Speichern), um Ihre Änderungen zu speichern.

Um ein Schlagwort zu einer Bewertungsvorlage hinzuzufügen oder zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Well-Architected Tool Konsole unter https://console.aws.amazon.com/wellarchitected/.
2. Wählen Sie in der Navigationsleiste die Region aus, die Sie verwenden möchten.
3. Wählen Sie im Navigationsbereich die Option Vorlagen überprüfen aus.

4. Wählen Sie den Namen der zu ändernden Bewertungsvorlage aus.
5. Wählen Sie auf der Registerkarte „Übersicht“ im Abschnitt „Tags“ die Option „Schlagworte verwalten“ aus.
6. Fügen Sie nach Bedarf Ihre Tags hinzu oder löschen Sie sie.
   - Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und füllen Sie die Felder Schlüssel und Wert aus.
   - Zum Entfernen eines Tags wählen Sie Remove (Entfernen).
7. Wiederholen Sie diesen Vorgang für jedes Tag, das Sie hinzufügen, ändern oder löschen möchten. Wählen Sie Save (Speichern), um Ihre Änderungen zu speichern.

Arbeiten mit Tags mithilfe der API

Verwenden Sie die folgenden AWS WA Tool API-Operationen, um die Tags für Ihre Ressourcen hinzuzufügen, zu aktualisieren, aufzulisten und zu löschen.

Markierungsunterstützung für AWS WA Tool-Ressourcen

Aufgabe	API-Aktion
Fügen Sie einen oder mehrere Tags hinzu oder überschreiben Sie sie.	TagResource
Löschen Sie ein oder mehrere Tags.	UntagResource
Listet Tags für eine Ressource auf	ListTagsForResource

Mit einigen Aktionen zur Ressourcenerstellung können Sie Tags beim Erstellen der Ressource angeben. Die folgenden Aktionen unterstützen das Markieren bei der Erstellung.

Aufgabe	API-Aktion
Erstellen Sie einen Workload	CreateWorkload
Importiere ein neues Objektiv	ImportLens
Erstellen eines -Profils	CreateProfile

Aufgabe	API-Aktion
Erstellen Sie eine Bewertungsvorlage	CreateReviewTemplate

Protokollierung von AWS WA Tool-API-Aufrufen mit AWS CloudTrail

AWS Well-Architected Tool ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in AWS WA Tool protokolliert. CloudTrail erfasst alle API-Aufrufe für AWS WA Tool als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS WA Tool-Konsole und Code-Aufrufe der AWS WA Tool-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket, einschließlich Ereignisse für AWS WA Tool aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail erfassten Informationen können Sie die an AWS WA Tool gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

AWS WA Tool-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Konto für Sie aktiviert. Die in AWS WA Tool auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS WA Tool, erstellen Sie einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Aktionen von AWS WA Tool werden von CloudTrail protokolliert und unter Von AWS Well-Architected Tool definierte Aktionen dokumentiert. Zum Beispiel generieren Aufrufe der Aktionen `CreateWorkload`, `DeleteWorkload` und `CreateWorkloadShare` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Benutzers oder des Root-Benutzers gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter dem CloudTrail userIdentity-Objekt.

Grundlagen zu AWS WA Tool-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Aktion `CreateWorkload` demonstriert.

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
```

```
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
```

```
        "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
        "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

EventBridge

AWS Well-Architected Tool sendet Ereignisse an Amazon EventBridge, wenn Aktionen für Well-Architected-Ressourcen durchgeführt werden. Sie können EventBridge und diese Ereignisse verwenden, um Regeln zu schreiben, die Aktionen ausführen. Beispielsweise können Sie benachrichtigt werden, wenn eine Änderung an einer Ressource übernommen wird. Weitere Informationen finden Sie unter Was ist Amazon EventBridge?

> **Note**
>
> Ereignisse werden auf einer Best-Effort-Basis bereitgestellt.

Die folgenden Aktionen führen zu EventBridge-Ereignissen:

- In Bezug auf Workloads
  - Erstellen oder Löschen eines Workloads
  - Erstellen eines Meilensteins
  - Aktualisieren der Eigenschaften eines Workloads
  - Freigeben eines Workloads bzw. Aufheben der Freigabe
  - Aktualisieren des Status einer Freigabeeinladung
  - Hinzufügen und Entfernen von Tags
  - Aktualisieren einer Antwort
  - Aktualisieren von Überprüfungsnotizen
  - Hinzufügen oder Entfernen eines Fokusbereichs aus einem Workload
- In Bezug auf Fokusbereiche
  - Importieren oder Exportieren eines benutzerdefinierten Fokusbereichs
  - Veröffentlichen eines benutzerdefinierten Fokusbereichs
  - Löschen eines benutzerdefinierten Fokusbereichs
  - Freigeben eines benutzerdefinierten Fokusbereichs bzw. Aufheben der Freigabe
  - Aktualisieren des Status einer Freigabeeinladung
  - Hinzufügen oder Entfernen eines Fokusbereichs aus einem Workload

Beispielereignisse aus AWS WA Tool

Dieser Abschnitt enthält Beispielereignisse aus AWS Well-Architected Tool.

Aktualisieren einer Antwort in einem Workload


```
{
  "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"
   }
}
```

Veröffentlichen eines benutzerdefinierten Fokusbereichs

```
{
   "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"
   }
}
```

Dokumentverlauf

Die folgende Tabelle beschreibt die Dokumentation zu dieser Version der AWS Well-Architected Tool.

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 17. April 2025

Änderung	Beschreibung	Datum
Neue Linse	In dieser Version wurde dem Lens-Katalog eine neue Linse hinzugefügt.	17. April 2025
Neue und aktualisierte Linsen	In dieser Version wurde dem Lens-Katalog eine neue Linse hinzugefügt, und eine weitere Linse wurde aktualisiert.	27. Juni 2024
Jira	In dieser Version wurde der AWS Well-Architected Tool-Connector für Jira hinzugefügt.	16. April 2024
Neue Linsen	In dieser Version wurden dem Lens-Katalog neue Linsen hinzugefügt.	26. März 2024
Aktualisierte Funktionalität	In dieser Version wurde AWS WA Tool die Funktion Lens-Katalog hinzugefügt.	26. November 2023
Aktualisierte Funktionalität	In dieser Version wurde AWS WA Tool die Funktion Vorlagen überprüfen hinzugefügt.	3. Oktober 2023

Aktualisierung der verwalteten Richtlinie WellArchitectedConsoleReadOnlyAccess	Hinzufügung von `"wellarchitected:ExportLens"` zu `WellArchitectedConsoleReadOnlyAccess` .	22. Juni 2023
Aktualisierte Funktionalität	In dieser Version wurde AWS WA Tool die Funktion Profile hinzugefügt.	13. Juni 2023
Aktualisierte Funktionalität	In dieser Version wurde die AWS Trusted Advisor- und AWS Service Catalog AppRegistry-Integration verbessert und `AWSWellArchitectedDiscoveryServiceRolePolicy` zu von AWS verwalteten Richtlinien hinzugefügt.	3. Mai 2023
Inhaltsaktualisierung	Die Dashboard-Seite wurde aktualisiert und enthält jetzt detaillierte Informationen zum Risiko- und Verbesserungsplan. Dazu wurde die Möglichkeit, einen konsolidierten Workload-Bericht zu erstellen, hinzugefügt.	30. März 2023
Inhaltsaktualisierung	Der Name der WellArchitectedConsoleReadOnlyAccess-Richtlinie wurde korrigiert.	19. Januar 2023

Die IAM-Anleitung für AWS WA Tool wurde aktualisiert	Aktualisierung des Leitfadens zur Ausrichtung an bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	4. Januar 2023
Aktualisierte Funktionalität	In dieser Version wurde die FTR-Linse aus dem Tool entfernt.	14. Dezember 2022
Aktualisierte Funktionalität	In dieser Version wurde die AWS Trusted Advisor- und AWS Service Catalog AppRegistry-Integration hinzugefügt.	7. November 2022
Inhaltsaktualisierung	Ein Problem im JSON-Beispiel für benutzerdefinierte Linsen für `choices` wurde behoben.	29. September 2022
Inhaltsaktualisierung	Der `choices`-Abschnitt der JSON-Spezifikation für benutzerdefinierte Linsen wurde aktualisiert.	02.August 2022
Aktualisierte Funktionalität	In dieser Version wurde die Nachverfolgung von Änderungen für AWS-verwaltete Richtlinien hinzugefügt. Außerdem wurde eine neue Aktion hinzugefügt, um der `AWSWellArchitectedOrganizationsServiceRolePolicy` die Berechtigung `ListAWSServiceAccessForOrganization` zu erteilen.	22. Juli 2022

Die gemeinsame Nutzung von Organisationen wurde hinzugefügt	In dieser Version wurde die Möglichkeit, Workloads und benutzerdefinierte Linsen mit einer Organisation und Organisationseinheiten (OUs) gemeinsam zu nutzen, hinzugefügt.	30. Juni 2022
Aktualisierte Funktionalität	In dieser Version wurde die Möglichkeit hinzugefügt, zusätzliche Ressourcen für Auswahlmöglichkeiten in einer benutzerdefinierten Linse anzugeben, eine Vorschau einer benutzerdefinierten Linse anzuzeigen, bevor sie veröffentlicht wird, und benutzerdefinierten Linsen Tags hinzuzufügen.	21. Juni 2022
Aktualisierte Funktionalität	In dieser Version wurde die Möglichkeit hinzugefügt, auf AWS re:Post auf die AWS Well-Architected-Community zuzugreifen.	31. Mai 2022
Aktualisierte Funktionalität	In dieser Version wurden dem Tutorial die Säule Nachhaltigkeit und kleinere Updates hinzugefügt.	31. März 2022
Unterstützung für EventBridge hinzugefügt	AWS WA Tool sendet nun ein Ereignis an Amazon EventBridge, wenn eine Änderung an einer Well-Architected-Ressource vorgenommen wird.	3. März 2022

Aktualisierte Funktionalität	Einzelne Best Practices können jetzt als nicht anwendbar markiert werden.	14. Juli 2021
Ressourcen-Tagging verfügbar	In dieser Version wurde die Möglichkeit, Workloads Tags hinzuzufügen, hinzugefügt.	3. März 2021
API jetzt verfügbar	In dieser Version wurde die AWS WA Tool-API hinzugefügt. AWS CloudTrail-Protokollierungsinformationen wurden hinzugefügt.	16. Dezember 2020
Aktualisierte Funktionalität	In dieser Version wurden dem Tool die Linsen FTR und SaaS hinzugefügt.	3. Dezember 2020
Aktualisierung des Datenschutzes	Die Informationen zum Datenschutz wurden aktualisiert.	5. November 2020
Inhaltsaktualisierung	Es wurde klargestellt, dass Sie nach dem Upgrade eines Workloads zur Verwendung einer neuen Linse nicht zur vorherigen Version zurückkehren können.	8. Juli 2020
Inhaltsaktualisierung	Es wurde klargestellt, dass das Freigeben von Inhalten in AWS-Regionen nach dem 20. März 2019 eingeführt wurde.	24. Juni 2020

Aktualisierte Funktionalität	Der Zugriff auf eine Workload-Freigabe wird sofort entfernt, wenn eine Einladung zur Workload-Freigabe abgelehnt wird. Der gemeinsame Zugriff wird gewährt, wenn die Freigabe akzeptiert wird.	17. Juni 2020
Inhaltsaktualisierung	Definitionen für Probleme mit hohem Risiko (HRI) und Probleme mit mittlerem Risiko (MRIs) wurden hinzugefügt.	12. Juni 2020
Inhaltsaktualisierung	Es wurde ein Abschnitt zur Verwendung Ihrer Daten durch AWS hinzugefügt.	21. Mai 2020
Aktualisierte Funktionalität	In dieser Version wird dem Workload ein Prüfeigentümer hinzugefügt.	01. April 2020
Aktualisierte Funktionalität	Diese Version fügt der Workload einen Architekt urdiagramm-Link hinzu.	10. März 2020
Inhaltsaktualisierung	Es wurde klargestellt, dass Workload-Freigaben AWS-Region-spezifisch sind.	10. Januar 2020
Aktualisierte Funktionalität	Diese Version fügt die Workload-Freigabe hinzu.	9. Januar 2020
Inhaltsaktualisierung	Sicherheitsbereich mit aktueller Anleitung aktualisiert.	6. Dezember 2019
Aktualisierte Funktionalität	Diese Version macht die Branchenfelder beim Definiere n eines Workloads optional.	19. August 2019

Aktualisierte Funktionalität	Diese Version fügt Verbesserungsplanelemente in den Workload-Bericht ein.	29. Juli 2019
Aktualisierte Funktionalität	Die Version fügt der Richtlinie die Aktion DeleteWorkload hinzu.	18. Juli 2019
Inhaltsaktualisierung	Der Inhalt in diesem Handbuch wurde aktualisiert und enthält jetzt kleinere Fehlerbehebungen.	19. Juni 2019
Inhaltsaktualisierung	Der Inhalt in diesem Handbuch wurde aktualisiert und enthält jetzt kleinere Fehlerbehebungen.	30. Mai 2019
Aktualisierte Funktionalität	Diese Version unterstützt ein Upgrade der Version des Frameworks, das für eine Workloadüberprüfung verwendet wird.	1. Mai 2019
Aktualisierte Funktionalität	In dieser Version wurde die Möglichkeit hinzugefügt, beim Definieren eines Workloads Nicht-AWS-Regionen anzugeben.	14. Februar 2019
Allgemeine Verfügbarkeit von AWS Well-Architected Tool	Mit dieser Version wird das AWS Well-Architected Tool eingeführt.	29. November 2018

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.