User Guide

AWS Well-Architected Tool

AWS Well-Architected Tool: User Guide

Table of Contents

Sie können den AWS Well-Architected Tool Connector für Jira verwenden, um Ihr Jira-Konto mit AWS Well-Architected Tool Ihren Workloads und Jira-Projekten zu verknüpfen und Verbesserungselemente zwischen Ihren Workloads und Jira-Projekten zu synchronisieren.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

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 Toolunterstützt Sie während des gesamten Produktlebenszyklus durch:

- 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.

Integrationen mit AWS Trusted Advisorund AWS Service Catalog AppRegistryhelfen Ihnen dabei, leichter die Informationen zu finden, die Sie zur Beantwortung von Fragen zur Well-Architected-Bewertung benötigen.

Dieser Service richtet sich an Personen, die an der technischen Produktentwicklung beteiligt sind, wie z. B. Chief Technology Officers (CTOs), Architekten, Entwickler und Mitglieder des Betriebsteams. AWSKunden 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

- Das AWS Well-Architected Framework

Das AWS Well-Architected Framework

Das AWSWell-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 AWSWell-Architected-Website.

Definitionen

In AWS WA Tool und im AWS Well-Architected Framework:

- 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 (HRI) handelt es sich um architektonische und betriebliche Entscheidungen, bei denen festgestellt AWS wurde, dass sie erhebliche negative Auswirkungen auf ein Unternehmen haben können. Diese HRI können sich auf organisatorische Vorgänge, Vermögenswerte und Einzelpersonen auswirken.
- Bei Problemen mit mittlerem Risiko (MRI) handelt es sich um architektonische und betriebliche Entscheidungen, bei denen festgestellt AWS wurde, dass sie sich negativ auf das Geschäft auswirken können, jedoch in geringerem Maße als HRI.

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

Erste Schritte mit AWS Well-Architected Tool

In diesem Abschnitt wird beschrieben, wie Sie mit beginnen können AWS WA Tool.

Themen

Benutzern, Gruppen oder Rollen Zugriff auf gewähren AWS WA Tool

In diesem Schritt gewähren Sie Zugriff auf AWS WA Tool.

Gewähren Sie Zugriff auf AWS WA Tool

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 Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
   - IAM-Benutzer:
     - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer 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 WellArchitectedConsoleFullAccessverwaltete Richtlinie auf den Berechtigungssatz oder die Rolle an.

   Vollzugriff ermöglicht es dem Principal, alle Aktionen in durchzuführen AWS WA Tool. Dieser Zugriff ist erforderlich, um Workloads zu definieren, Workloads zu löschen, Workloads anzuzeigen, Workloads zu aktualisieren, Workloads gemeinsam zu nutzen, benutzerdefinierte Objektive zu erstellen und benutzerdefinierte Objektive gemeinsam zu nutzen.
3. Um nur Lesezugriff zu gewähren, wenden Sie die WellArchitectedConsoleReadOnlyAccessverwaltete Richtlinie auf den Berechtigungssatz oder die Rolle an. Principals mit dieser Rolle können nur Ressourcen anzeigen.

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

Unterstützung für andere AWS Dienste aktivieren

Wenn Sie den AWS WA Tool Organisationszugriff aktivieren, können Sie Informationen über die Struktur Ihrer Organisation sammeln, um Ressourcen einfacher gemeinsam nutzen zu können (the section called “Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations”weitere Informationen finden Sie unter). Durch die Aktivierung des Discovery-Supports werden Informationen aus AWS Trusted AdvisorAWS Service Catalog AppRegistry, und verwandten Ressourcen (z. B. AWS CloudFormation Stapeln in AppRegistry Ressourcensammlungen) gesammelt, sodass Sie leichter die Informationen finden können, die Sie zur Beantwortung von Well-Architected-Überprüfungsfragen benötigen, und die Trusted Advisor Prüfungen auf einen bestimmten Workload zuschneiden können.

Wenn Sie den Support für oder den Discovery-Support aktivieren AWS Organizations, wird automatisch eine dienstbezogene Rolle für Ihr Konto erstellt.

Um den Support für andere Dienste zu aktivieren, mit denen Sie interagieren AWS WA Tool können, navigieren Sie zu Einstellungen.

1. Um Informationen von zu sammeln AWS Organizations, aktiviere die Option AWS Organizations Support aktivieren.
2. Aktivieren Sie die Option Activate Discovery-Support, um Informationen von anderen AWS Diensten und Ressourcen zu sammeln.

3. Wählen Sie Rollenberechtigungen anzeigen aus, um die mit dem Dienst verknüpften Rollenberechtigungen oder die Richtlinien für Vertrauensbeziehungen anzuzeigen.
4. Wählen Sie Einstellungen speichern aus.

AppRegistry Für einen Workload aktivieren

AppRegistry Die Verwendung ist optional und AWS Business- und Enterprise Support-Kunden können sie pro Workload aktivieren.

Immer wenn der Discovery-Support aktiviert AppRegistry ist und einem neuen oder vorhandenen Workload zugeordnet ist, wird eine vom Service verwaltete Attributgruppe AWS WA Tool erstellt. Die Attributgruppe Metadaten 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 oder die Anwendung aus dem Workload entfernt wird, werden die Workload-Informationen aus entfernt AWS Service Catalog.

Wenn Sie möchten, dass eine AppRegistry Anwendung die abgerufenen Daten steuert Trusted Advisor, legen Sie Ihre Workload-Ressourcendefinition auf AppRegistryoder Alle fest. Erstellen Sie Rollen für alle Konten, die Ressourcen in Ihrer Anwendung besitzen. Folgen Sie dabei den Richtlinien unterthe section called “Aktivierung Trusted Advisor in IAM”.

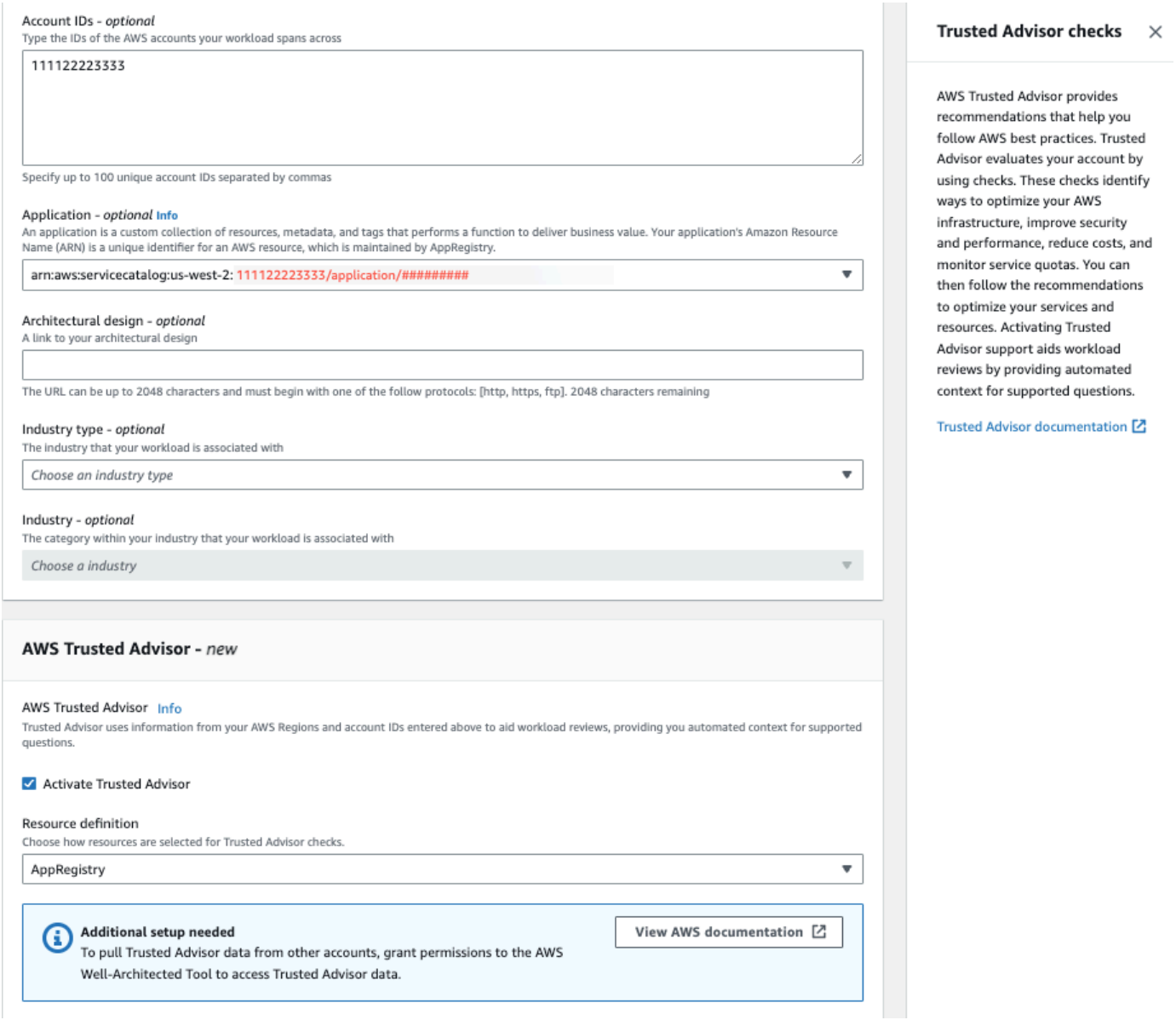
Aktivierung AWS Trusted Advisor für einen Workload

Die Integration mit AWS Trusted Advisor ist optional und kann für AWS Business- und Enterprise Support-Kunden pro Workload aktiviert werden. Die Integration Trusted Advisor ist kostenlos AWS WA Tool, Trusted Advisor Preisdetails finden Sie jedoch unter AWS Supportpläne.

So aktivieren Sie Trusted Advisor für einen Workload

1. Zur Aktivierung Trusted Advisor können Workload-Besitzer AWS WA Tool damit einen vorhandenen Workload aktualisieren oder einen neuen Workload erstellen, indem sie Workload definieren wählen.
2. Geben Sie Trusted Advisor im Feld Konto-IDs eine Konto-ID ein, die von verwendet wird, wählen Sie im Feld Anwendung einen Anwendungs-ARN aus, oder wählen Sie beide aus, um sie zu aktivieren Trusted Advisor.

3. Wählen Sie in dem AWS Trusted AdvisorAbschnitt Aktivieren aus Trusted Advisor.



4. Bei der ersten Aktivierung für einen Workload wird eine Benachrichtigung angezeigt, dass die IAM-Servicerolle erstellt Trusted Advisor wird. Wenn Sie Berechtigungen anzeigen wählen, 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 die Aktivierung Trusted Advisornachfolgender Workloads nur die Meldung „Zusätzliche Einrichtung erforderlich“ angezeigt.
5. In der Dropdownliste Ressourcendefinition können Sie Workload-Metadaten oder Alle AppRegistryauswählen. Die Auswahl der Ressourcendefinition definiert, von welchen Daten AWS WA Tool abgerufen werden, Trusted Advisor um die Statuschecks in der Workload-Überprüfung bereitzustellen, die den Best Practices von Well-Architected entsprechen.

Workload-Metadaten — Der Workload wird durch Konto-IDs definiert und im Workload AWS-Regionen spezifiziert.

AppRegistry— Der Workload wird durch Ressourcen (wie AWS CloudFormation Stacks) definiert, die in der mit dem Workload verknüpften AppRegistry Anwendung vorhanden sind.

Alle — Die Arbeitslast wird sowohl durch die Workload-Metadaten als auch durch AppRegistry Ressourcen definiert.

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

Der ruft AWS WA Tool regelmäßig Daten Trusted Advisor mithilfe der in IAM erstellten Rollen ab. Die IAM-Rolle wird automatisch für den Workload-Besitzer erstellt. Um Trusted Advisor Informationen einzusehen, müssen die Besitzer aller zugehörigen Konten auf dem Workload jedoch zu IAM gehen und dort eine Rolle erstellen. ??? Weitere Informationen finden Sie unter. Wenn diese Rolle nicht existiert, AWS WA Tool kann sie keine Trusted Advisor Informationen für dieses Konto abrufen und es wird eine Fehlermeldung angezeigt.

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

Aktivierung Trusted Advisor für einen Workload in IAM

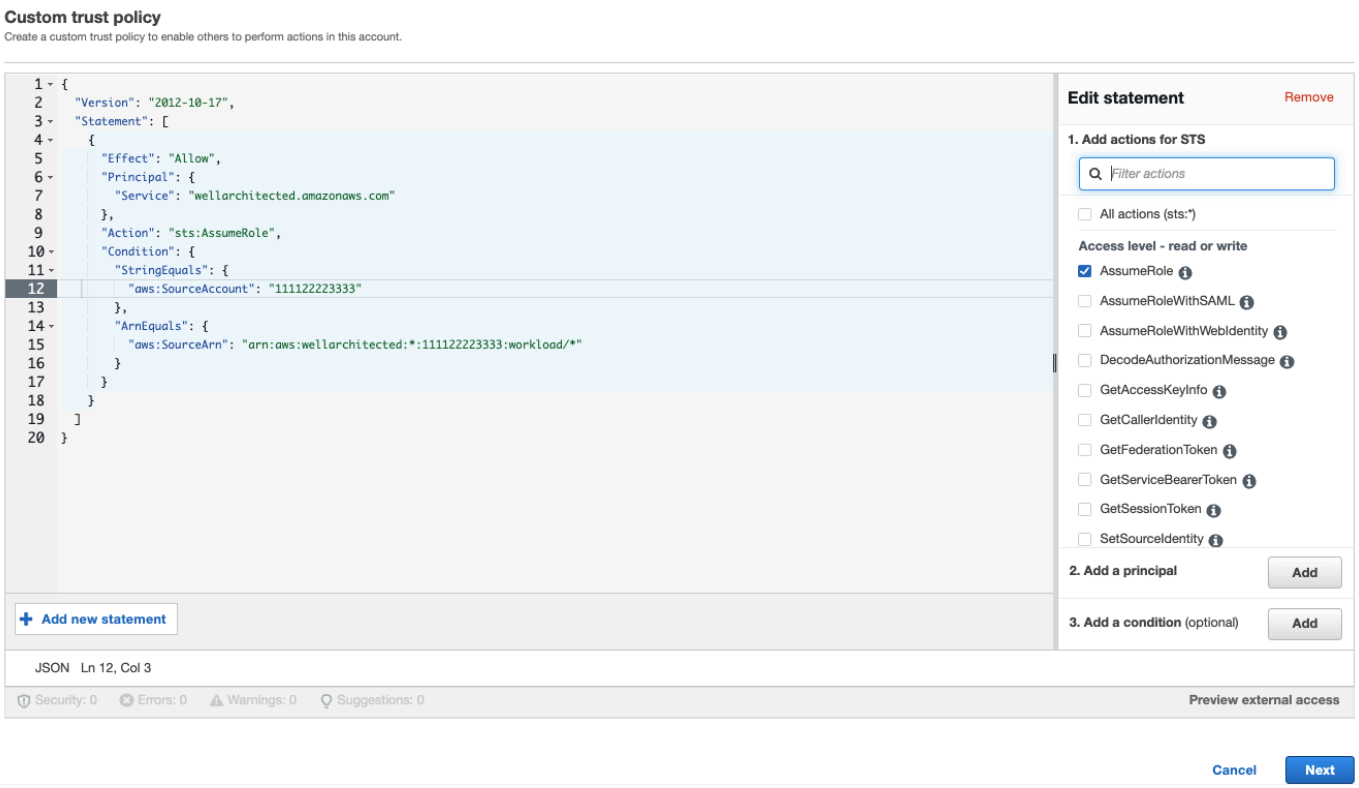
> **Note**
>
> Workload-Besitzer sollten die Discovery-Unterstützung für ihr Konto aktivieren, bevor sie einen Trusted Advisor Workload erstellen. Wenn Sie Discovery-Support aktivieren wählen, wird die Rolle erstellt, die für den Workload-Besitzer erforderlich ist. Führen Sie die folgenden Schritte für alle anderen verknüpften Konten aus.

Die Besitzer verknüpfter Konten für Workloads, die aktiviert wurden, Trusted Advisor müssen eine Rolle in IAM erstellen, um Trusted Advisor Informationen zu erhalten. AWS WA Tool

Um eine Rolle in IAM zu erstellen, von der Informationen abgerufen AWS WA Tool werden sollen Trusted Advisor

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

```
{
  "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 Block `aws:sourceArn` im Bedingungsblock der vorhergehenden benutzerdefinierten Vertrauensrichtlinie ist. Dabei handelt es sich um eine allgemeine Bedingung`"arn:aws:wellarchitected:*:`*WORKLOAD_OWNER_ACCOUNT_ID*`:workload/*"`, die besagt, dass diese Rolle AWS WA Tool für alle Workloads des Workload-Besitzers verwendet werden kann. Der Zugriff kann jedoch auf einen bestimmten Workload-ARN oder eine Reihe von Workload-ARNs beschränkt werden. Informationen zur Angabe mehrerer ARNs finden Sie im folgenden Beispiel für eine Vertrauensrichtlinie.

```
{
    "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“ für Berechtigungsrichtlinien die Option Richtlinie erstellen aus Trusted Advisor, um AWS WA Tool Zugriff auf Lesedaten zu gewähren. Wenn Sie Richtlinie erstellen auswählen, wird ein neues Fenster geöffnet.

> **Note**
>
> Darüber hinaus haben Sie die Möglichkeit, die Erstellung der Berechtigungen während der Rollenerstellung zu überspringen und nach dem Erstellen der Rolle eine Inline-Richtlinie zu erstellen. Wählen Sie in der Meldung zur erfolgreichen Rollenerstellung die Option Rolle anzeigen aus und wählen Sie auf der Registerkarte Berechtigungen in der Dropdownliste Berechtigungen hinzufügen die Option Inline-Richtlinie erstellen aus.

6. Kopieren Sie die folgende Berechtigungsrichtlinie und fügen Sie sie in das JSON-Feld ein. *YOUR_ACCOUNT_ID*Ersetzen `Resource` Sie den ARN durch Ihre eigene Konto-ID, geben Sie die Region oder ein Sternchen (`*`) an und wählen Sie Weiter:Tags.

   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 für einen Workload aktiviert Trusted Advisor ist und die Ressourcendefinition auf AppRegistryoder Alle gesetzt ist, müssen alle Konten, die eine Ressource in der mit dem Workload verknüpften AppRegistry Anwendung besitzen, 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 Richtliniennamen aus, den Sie gerade erstellt haben, und wählen Sie Weiter aus.
11. Geben Sie den Rollennamen ein, der die folgende Syntax verwenden muss: `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* und wählen Sie Rolle erstellen aus. *`WORKLOAD_OWNER_ACCOUNT_ID`*Ersetzen Sie ihn durch die Konto-ID des Workload-Besitzers.

    Sie sollten oben auf der Seite eine Erfolgsmeldung erhalten, 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 Sie nach dem `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* Namen. Wählen Sie den Namen der Rolle aus, um zu überprüfen, ob die Beziehungen zwischen Berechtigungen und Vertrauen korrekt sind.

Deaktivierung Trusted Advisor für einen Workload

So deaktivieren Sie Trusted Advisor für einen Workload

Sie können die Funktion Trusted Advisor für jeden Workload aus dem deaktivieren, AWS WA Tool indem Sie Ihren Workload bearbeiten und die Option Aktivieren deaktivieren. Trusted Advisor Weitere Informationen zum Bearbeiten von Workloads finden Sie unter. the section called “Einen Workload bearbeiten”

Durch die Deaktivierung Trusted Advisor von werden die in IAM erstellten Rollen AWS WA Tool nicht gelöscht. Das Löschen von Rollen aus IAM erfordert eine separate Bereinigungsmaßnahme. Workload-Besitzer oder Besitzer verknüpfter Konten sollten die IAM-Rollen löschen, die bei Trusted Advisor der Deaktivierung in erstellt wurden AWS WA Tool, oder um die Erfassung AWS WA Tool von Trusted Advisor Daten für den Workload einzustellen.

Um das in IAM zu löschen **`WellArchitectedRoleForTrustedAdvisor`**

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

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

Weitere Informationen zum Löschen einer Rolle aus IAM finden Sie unter Löschen einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Definition eines Workloads

Der nächste Schritt besteht darin, einen Workload zu definieren.

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/.
2. Wenn Sie den Dienst zum ersten Mal verwenden AWS WA Tool, wird eine Seite angezeigt, auf der Sie mit den Funktionen des Dienstes vertraut gemacht werden. 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.

   Einzelheiten dazu, wie Ihre Workload-Daten AWS verwendet werden, finden Sie unter Warum werden diese Daten AWS benötigt 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 Regions (Regionen) die Regionen für Ihren Workload aus:
   - AWS-Regionen— Wählen Sie nacheinander aus, AWS-Regionen wo Ihr Workload ausgeführt wird.
   - AWS Nicht-Regionen — Geben Sie die Namen der Regionen ein, außerhalb derer Ihr AWS Workload ausgeführt wird. Sie können bis zu fünf eindeutige Regionen angeben, die durch Kommas getrennt sind.

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

   Wenn Trusted Advisor aktiviert, werden alle angegebenen Konto-IDs verwendet, um Daten von abzurufen Trusted Advisor. Informationen zum Erteilen von AWS WA Tool Berechtigungen AWS Trusted Advisor zum Abrufen von Trusted Advisor Daten in Ihrem Namen innerhalb von IAM finden Sie unter Aktivierung für einen Workload.
9. (Optional) Geben Sie im Feld Anwendung den Anwendungs-ARN einer Anwendung ein AWS Service Catalog AppRegistry, die Sie diesem Workload zuordnen möchten. Pro Workload kann nur ein ARN angegeben werden, und die Anwendung und der 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 in dem Trusted AdvisorAbschnitt Aktivieren aus, um Trusted Advisor Prüfungen für Ihren Workload zu aktivieren Trusted Advisor. Für Konten, die mit Ihrem Workload verknüpft sind, ist möglicherweise eine zusätzliche Einrichtung erforderlich. Weitere

Informationen finden the section called “Wird aktiviert Trusted Advisor” Sie unter Erteilung von AWS WA Tool Berechtigungen zum Abrufen von Trusted Advisor Daten in Ihrem Namen. Wählen Sie unter Ressourcendefinition Workload-Metadaten oder Alle aus AppRegistry, um zu definieren, welche Ressourcen für die Ausführung von Trusted Advisor Prüfungen AWS WA Tool verwendet werden.

14. (Optional) Wählen Sie im Abschnitt Jira die Option Einstellungen auf Kontoebene überschreiben aus, um die Jira-Sync-Einstellungen 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 der Einrichtung und Konfiguration des AWS Well-Architected Tool Connectors finden Sie unter Connector für Jira. Wählen Sie zwischen Workload nicht synchronisieren, Workload synchronisieren — Manuell und Workload synchronisieren — Automatisch aus und geben Sie optional einen Jira-Projektschlüssel ein, mit dem synchronisiert werden soll.

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

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

    Weitere Informationen zu Tags finden Sie unterMarkieren Ihrer AWS WA Tool-Ressourcen.

16. Wählen Sie Weiter aus.

    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 wählen, um ein Profil zu erstellen. Wählen Sie Weiter aus.

18. Wählen Sie die Linsen aus, die für diesen Workload gelten. Bis zu 20 Objektive können zu einem Workload hinzugefügt werden. Eine Beschreibung der offiziellen AWS Objektive finden Sie unter Objektive.

    Objektive können aus dem Bereich Benutzerdefinierte Objektive (Objektive, die Sie selbst erstellt haben oder die mit Ihnen geteilt wurden AWS-Konto), dem Objektivkatalog (AWS offizieller Objektivkatalog, der allen Benutzern zur Verfügung steht) oder beidem ausgewählt werden.

> **Note**
>
> Der Abschnitt Benutzerdefinierte Objektive ist leer, wenn Sie kein benutzerdefiniertes Objektiv erstellt haben oder kein benutzerdefiniertes Objektiv mit Ihnen geteilt haben.

> **Haftungsausschluss**
>
> Indem Sie auf benutzerdefinierte Brillengläser zugreifen und/oder diese anwenden, die von einem anderen AWS Benutzer oder Konto erstellt wurden, erkennen Sie an, dass benutzerdefinierte Brillengläser, die von anderen Benutzern erstellt und mit Ihnen geteilt 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 dokumentieren

Nachdem ein Workload definiert wurde, dokumentieren Sie dessen Status.

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-Prüfung, die Sie verwenden können, um den Workload-Überprüfungsprozess zu beschleunigen.
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 Informationen erhalten Sie, wenn Sie „Info“ auswählen und sich die Informationen im Hilfebereich ansehen.

   - 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.

   Wenn Sie weitere Informationen zu einem beliebigen Element benötigen, wählen Sie Info und sehen Sie sich die Informationen im Hilfebereich an.

b. (Optional) Wenn eine oder mehrere bewährte Methoden auf Ihren Workload nicht zutreffen, wählen Sie Als Best Practice (s) kennzeichnen, die für diesen Workload nicht zutreffen, und wählen Sie sie 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.

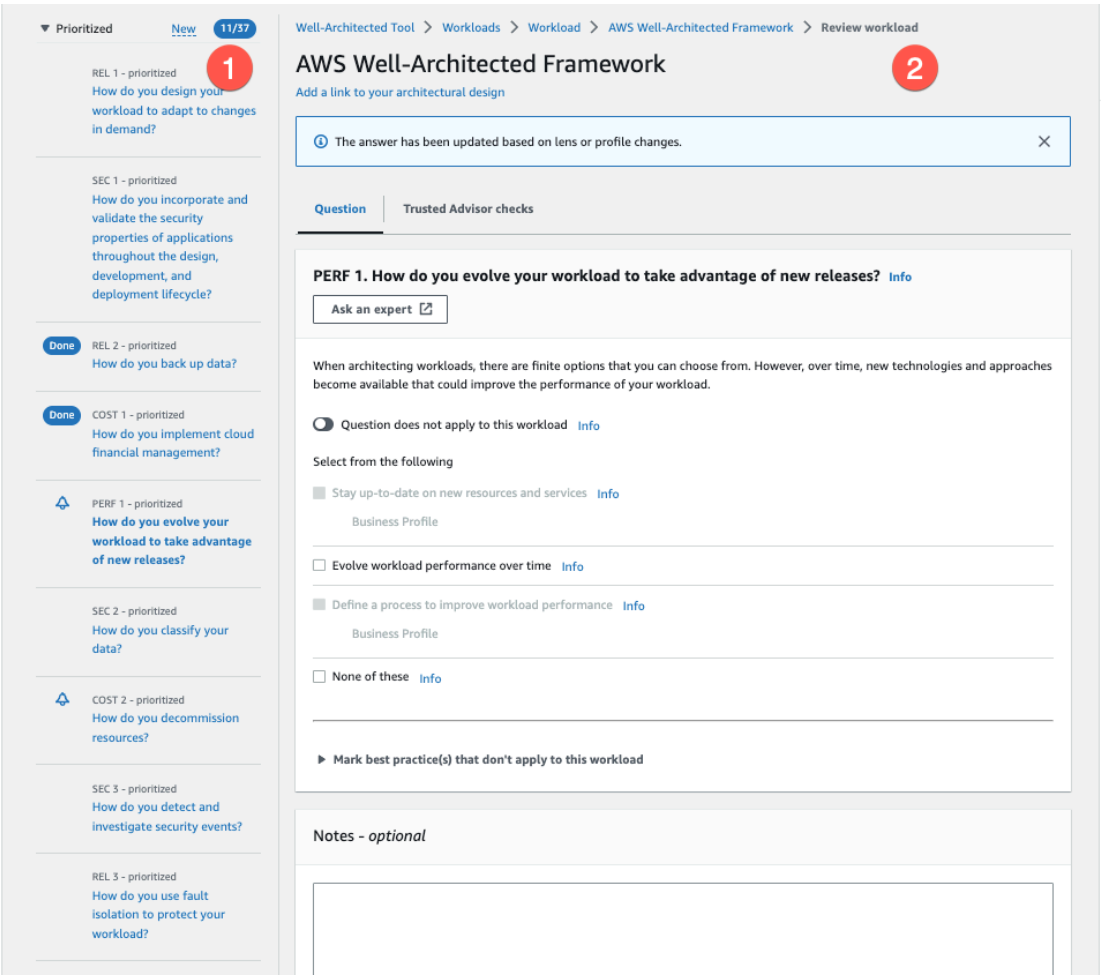
   Wiederholen Sie diese Schritte für jede Frage in jeder Säule.

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

Um zu den Fragen zurückzukehren, gehen Sie zur Detailseite des Workloads und klicken Sie auf Continue review (Überprüfung fortsetzen).

Überprüfen Sie die Workload-Seite

Die Seite „Workload überprüfen“ besteht aus drei Bereichen.



1. Im linken Navigationsbereich werden die Fragen für jede Säule angezeigt. Fragen, die Sie beantwortet haben, sind als Erledigt 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, AWS WA Tool verwendet es dann 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 der Arbeitslast zu beschleunigen. Neben Fragen, die neu zur Liste der priorisierten Fragen 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 Fragen Sie einen Experten, um Zugang zur AWS

re:POST-Community zu erhalten, die Well-Architected gewidmet AWS ist. AWS re:POST ist ein themenorientierter Community-Ersatz für Foren. question-and-answer AWS Mit re:POST kannst du Antworten finden, Fragen beantworten, einer Gruppe beitreten, beliebten Themen folgen und über deine Lieblingsfragen und -antworten abstimmen.

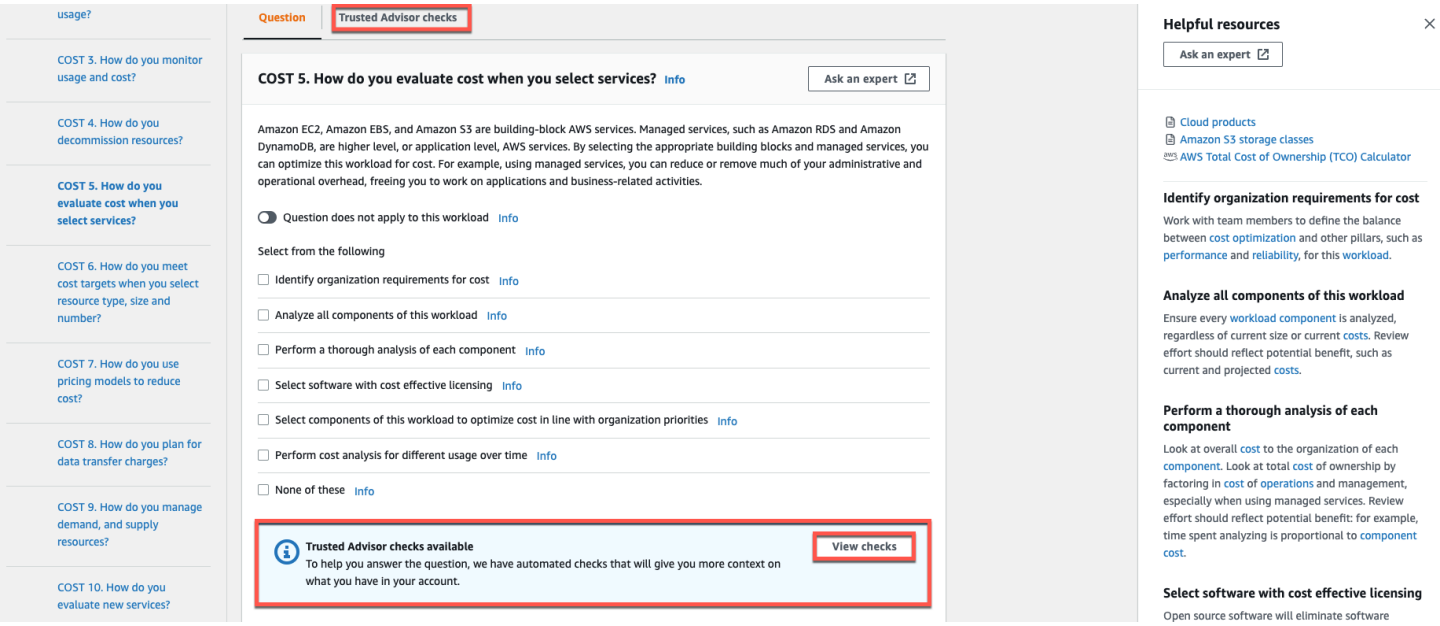
(Optional) Um eine oder mehrere bewährte Methoden als nicht zutreffend zu kennzeichnen, wählen Sie Bewährte Verfahren markieren, die für diesen Workload nicht zutreffen, und wählen Sie sie aus.

Verwenden Sie die Schaltflächen am unteren Rand dieses Bereichs, um zur nächsten Frage zu wechseln, zur vorherigen Frage zurückzukehren oder Ihre Änderungen zu speichern und den Vorgang zu beenden.

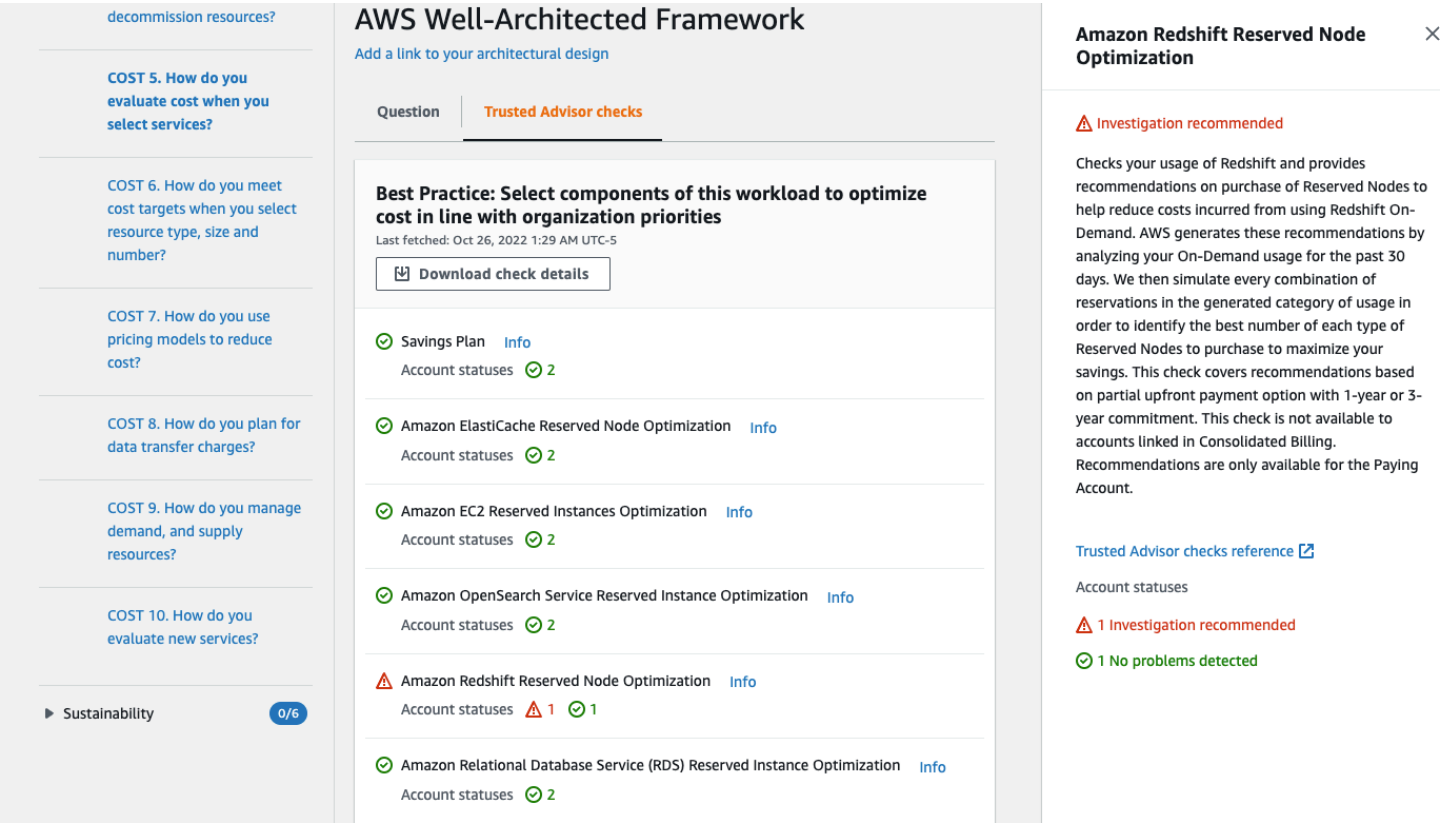
3. Im rechten Hilfebereich werden zusätzliche Informationen und hilfreiche Ressourcen angezeigt. Wählen Sie Fragen Sie einen Experten, um Zugang zur AWS re:POST-Community zu erhalten, die Well-Architected gewidmet AWS ist. In dieser Community kannst du Fragen zum Entwerfen, Erstellen, Bereitstellen und Betreiben von Workloads stellen. AWS

Trusted Advisor prüft

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



Auf der Registerkarte „Trusted Advisor Prüfungen“ finden Sie detailliertere Informationen zu den bewährten Prüfungen von Trusted Advisor, Links zur Trusted Advisor Dokumentation im Bereich „Hilferessourcen“ oder „Prüfdetails herunterladen“, wo Sie einen Bericht über die Trusted Advisor Prüfungen und den Status der einzelnen bewährten Methoden in einer CSV-Datei finden.



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

- Empfohlene Maßnahme (rot) — Trusted Advisor empfiehlt eine Aktion für die Prüfung.
- Untersuchung empfohlen (gelb) — Trusted Advisor erkennt ein mögliches Problem bei der Überprüfung.
- Es wurden keine Probleme festgestellt (grün) — es wird Trusted Advisor kein Problem für die Prüfung erkannt.
- 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 Trusted Advisor bereitgestellten Prüfungen finden Sie im AWS Support Benutzerhandbuch unter Check-Kategorien anzeigen.

Wenn Sie neben jeder Trusted Advisor Prüfung auf den Link Info klicken, werden Informationen zu der Prüfung im Bereich Hilferessourcen angezeigt. Weitere Informationen finden Sie in der AWS Trusted Advisor Prüfreferenz im AWS Support Benutzerhandbuch.

Einen Meilenstein speichern

Sie können einen Meilenstein 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 Speichern.

Nachdem ein Meilenstein gespeichert wurde, können Sie die Daten des Workloads, die in diesem Meilenstein erfasst wurden, nicht mehr ändern.

Weitere Informationen finden Sie unter Meilensteine.

Tutorial

In diesem Tutorial wird AWS Well-Architected Tool die Verwendung zur Dokumentation und Messung einer Arbeitslast beschrieben. 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 “Definition eines Workloads”.

So definieren Sie einen Workload

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

   > **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.

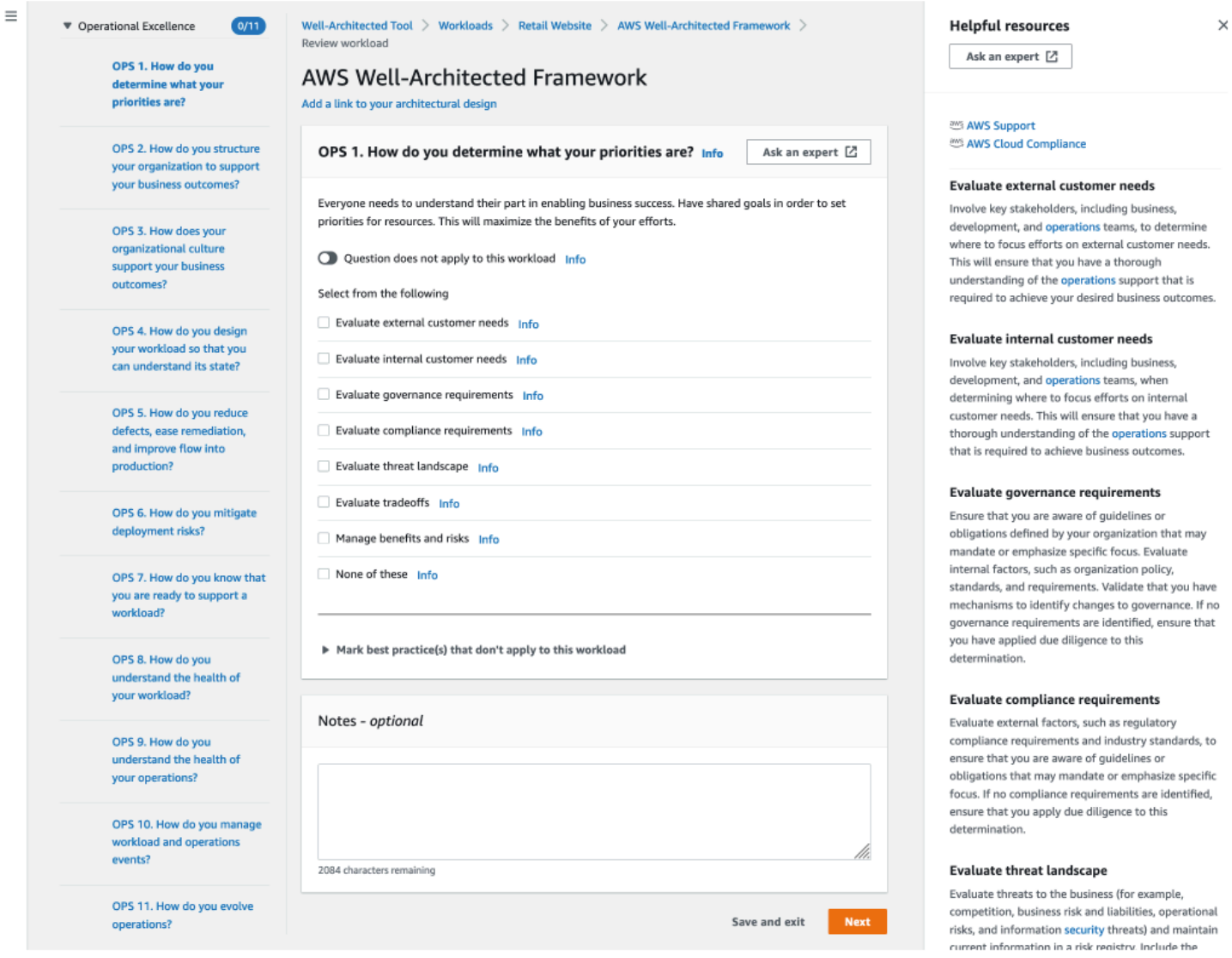
6. Geben Sie im Feld Umgebung an, dass sich der Workload in einer Produktionsumgebung befindet.
7. Unser Workload wird AWS sowohl in unserem lokalen Rechenzentrum als auch in unserem lokalen Rechenzentrum ausgeführt:
    a. Wählen Sie AWS-Regionendie beiden Regionen in Nordamerika aus, in denen der Workload ausgeführt wird.
    b. Wählen Sie außerdem AWS Nicht-Regionen aus und geben Sie einen Namen für das lokale Rechenzentrum ein.
8. Das Feld Konto-IDs ist optional. Ordnen Sie diesem AWS-Konten Workload keine zu.
9. Das Anwendungsfeld ist optional. Geben Sie keinen Anwendungs-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 aus.
15. Der Schritt Profil anwenden ist optional. Wenden Sie kein Profil für diesen Workload an. Wählen Sie Weiter aus.
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.

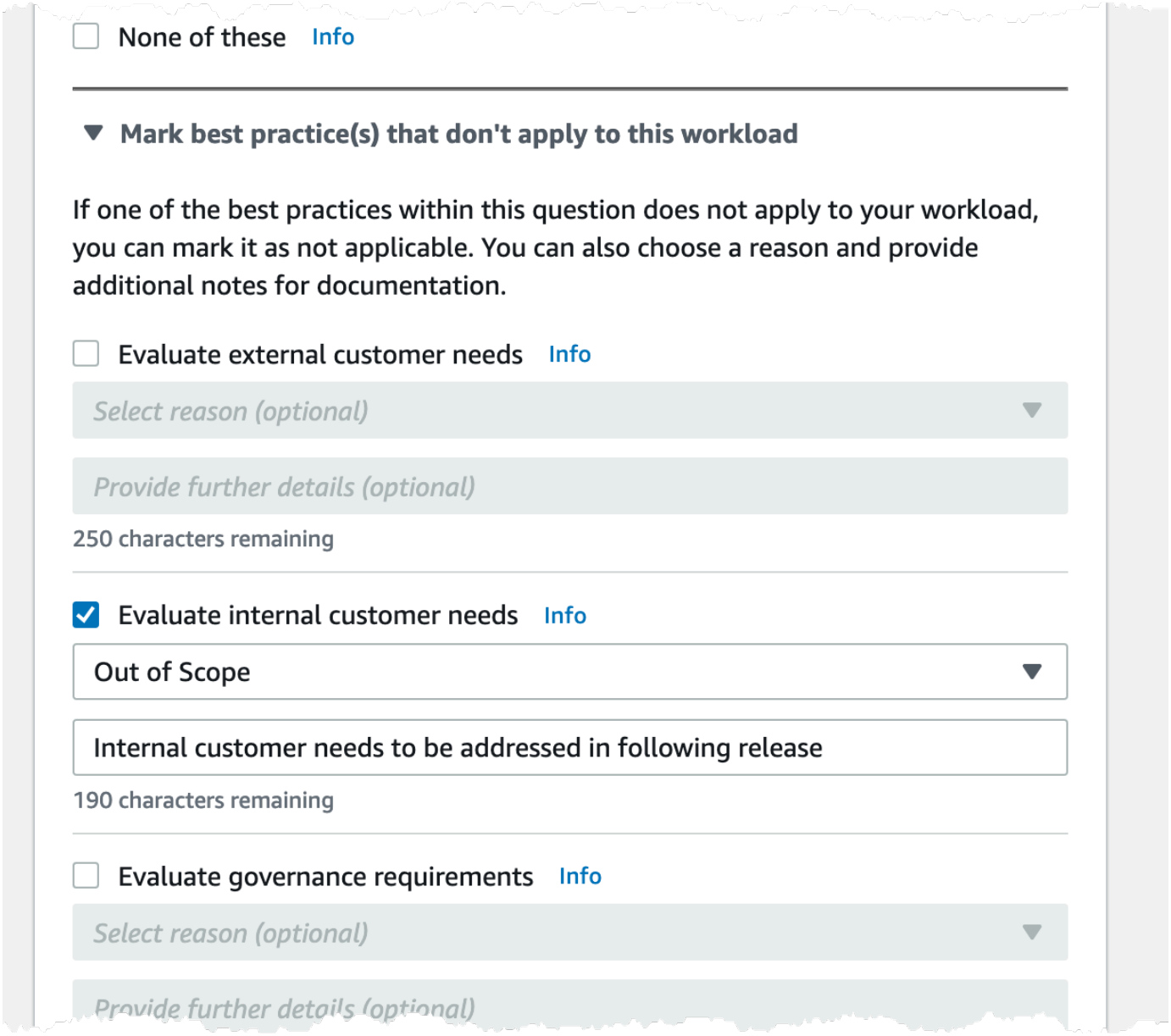
Wählen Sie Fragen Sie einen Experten, um Zugang zur AWS re:POST-Community zu erhalten, die Well-Architected gewidmet AWS ist. In dieser Community kannst du Fragen zum Entwerfen, Erstellen, Bereitstellen und Betreiben von Workloads stellen. AWS



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 Speichern.
4. Um einen Workload-Bericht zu generieren, wählen Sie die gewünschte Linse aus und klicken Sie auf Generate report (Bericht generieren). Es wird eine PDF-Datei erstellt. Diese Datei enthält den Status des Workloads, die Anzahl der erkannten Risiken und eine Liste der empfohlenen Verbesserungen.

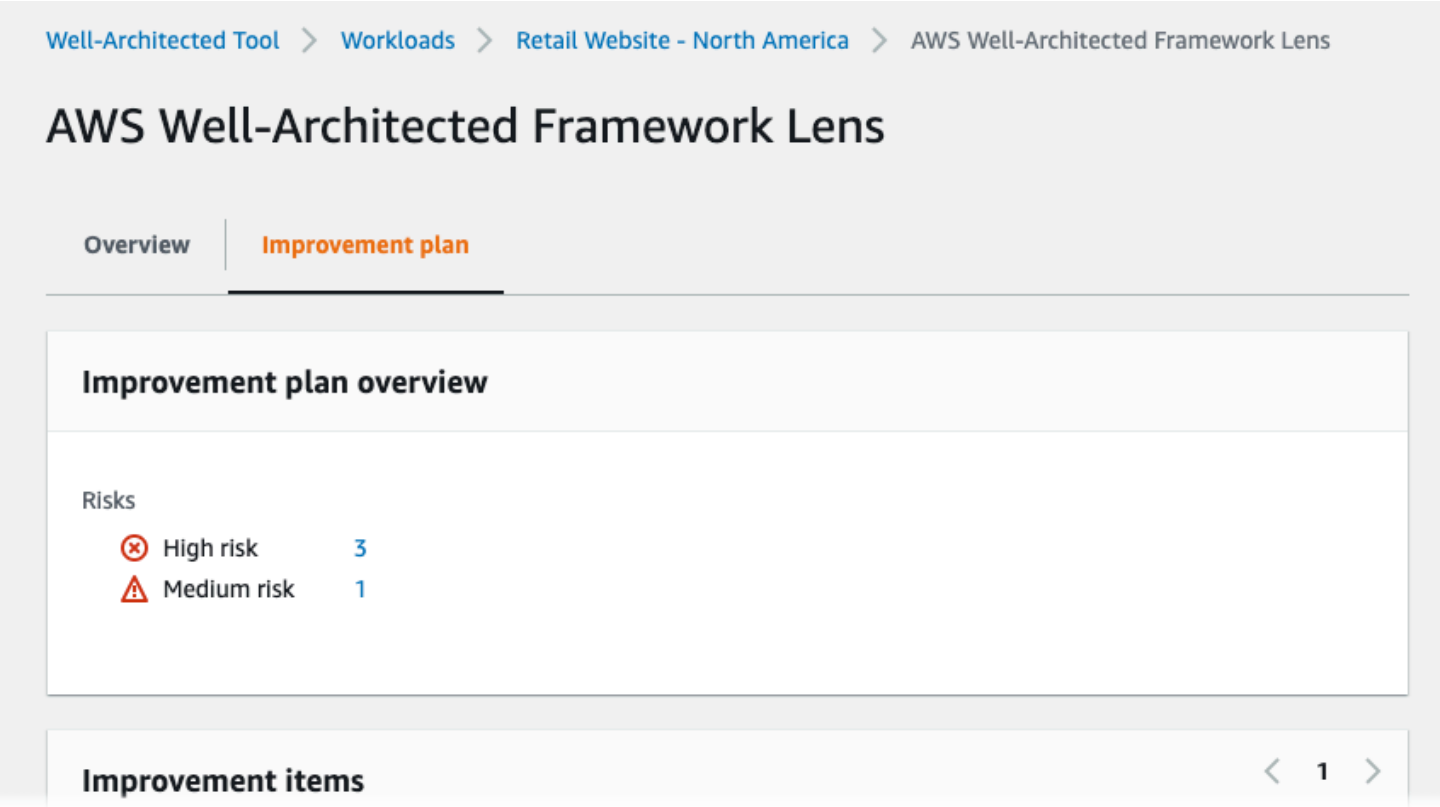
Schritt 3: Überprüfen Sie den Verbesserungsplan

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.

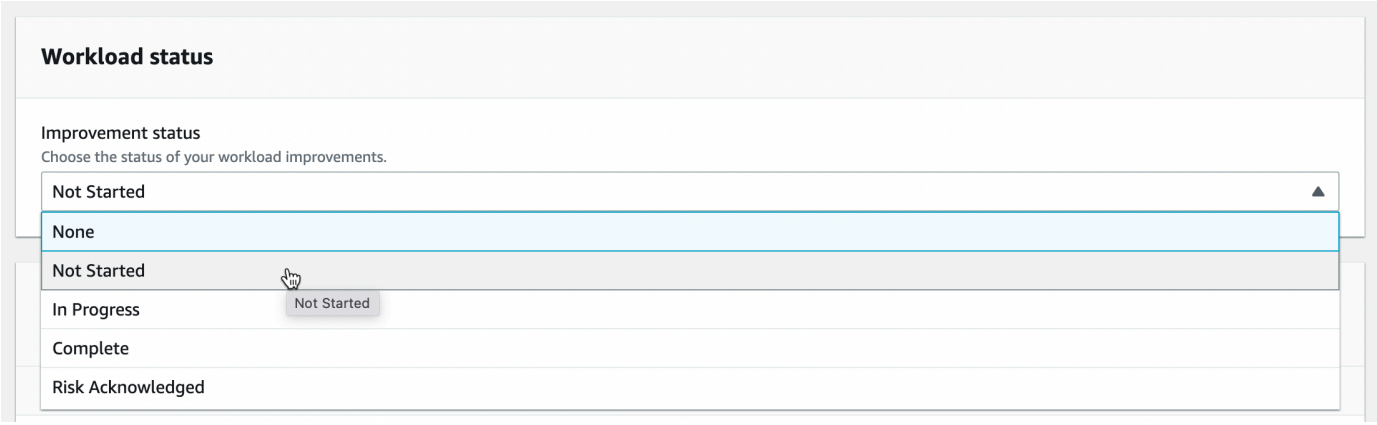
Für diesen speziellen Workload wurden drei Probleme mit hohem Risiko und ein Problem mit mittlerem Risiko durch die AWS Well-Architected Framework Lens identifiziert.



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.

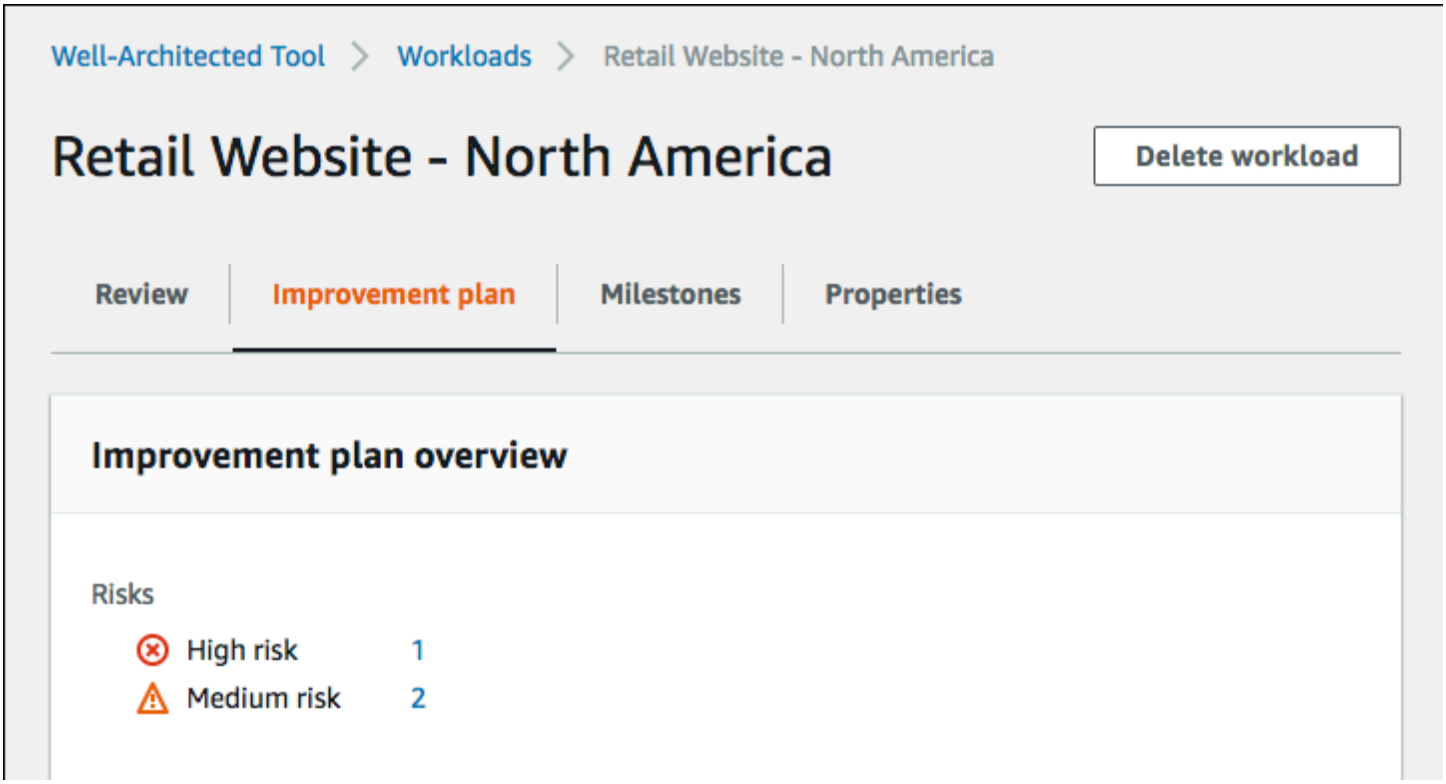
Wenn der Arbeitslast ein Profil zugeordnet ist, wird die Anzahl der priorisierten Risiken im Abschnitt Übersicht über den Verbesserungsplan angezeigt. Sie können die Liste der Verbesserungselemente filtern, indem Sie nach Profil priorisiert auswählen. In der Liste der Verbesserungselemente wird die Bezeichnung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

Ein Workload 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 (High Risk Issues – HRI).

Mittlere Risiken

Die Anzahl der identifizierten Probleme mit mittlerem Risiko (Medium Risk Issues – MRIs).

Verbesserungsstatus

Der Verbesserungsstatus, den Sie für den Workload festgelegt haben:

- Keine
- 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 des Workloads mit anderen AWS-Konten Benutzern oder Organisationseinheiten (OUs) zu verwalten, wählen Sie Details anzeigen und dann Shares 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 (HRI) und Problemen mit mittlerem Risiko (MRIs)

Probleme mit hohem Risiko (HRI), die AWS Well-Architected Tool in Bezug auf architektonische und betriebliche Entscheidungen identifiziert AWS wurden, können erhebliche negative Auswirkungen auf ein Unternehmen haben. Diese HRI können sich auf organisatorische Vorgänge, Vermögenswerte und Einzelpersonen auswirken. Probleme mit mittlerem Risiko (MRIs) können sich ebenfalls negativ auf das Geschäft auswirken, aber 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. AWSschlägt vor, dass Kunden diese Gründe und ihre Auswirkungen auf die bewährten Verfahren in den Arbeitsauslastungsnotizen dokumentieren. AWSschlägt vor, dass Kunden für alle identifizierten HRI und MRTs die in der definierten bewährten Verfahren anwenden. 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, die bewährte Methode nicht umzusetzen, AWS schlägt vor, dass sie die entsprechende Genehmigung auf Unternehmensebene und die Gründe für die Nichtumsetzung dokumentieren.

Definition eines Workloads

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 die Dropdownliste 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 “Definition eines Workloads”, 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 einer 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.

Einen Workload anzeigen

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.

Einen Workload bearbeiten

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

So bearbeiten 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, 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 Definition eines Workloads.

   > **Note**
   >
   > Wenn Sie einen vorhandenen Workload aktualisieren, können Sie Activate Trusted Advisor verwenden. 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 “Aktivierung Trusted Advisor in IAM”.

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.

Einen Workload teilen

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

> **Note**
>
> Sie können Workloads nur innerhalb derselben AWS-Region Einheit gemeinsam nutzen. Wenn der Empfänger ein Workload mit einem anderen teiltAWS-Konto, kann er die Einladung zum Teilen nicht annehmen, wenn er nicht über die `wellarchitected:UpdateShareInvitation` entsprechende Genehmigung verfügt. Beispiele the section called “Bereitstellung des Zugriffs auf AWS WA Tool” 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 den 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 Organizationsden Zugriff aktivieren.

Um einen Workload mit Ihrer Organisation oder Organisationseinheiten 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 Shares to Organizations.
5. Wählen Sie auf der Seite Workload-Sharing erstellen aus, ob Sie der gesamten Organisation oder einer oder mehreren Organisationseinheiten Berechtigungen gewähren 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 den Workload gemeinsam zu nutzen.

Um zu sehen, wer einen gemeinsamen Zugriff auf einen Workload hat, wählen Sie Shares (Freigaben) auf der Seite Einzelheiten zur Arbeitslast.

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, auch mit anderen BenutzernAWS-Konten, Ihrer Organisation und den Organisationseinheiten in derselben Umgebung teilenAWS-Region. Einzelheiten finden Sie unterEin benutzerdefiniertes Objektiv teilen.

Überlegungen zur Freigabe

Ein Workload kann mit bis zu 20 verschiedenen AWS-Konten Endbenutzern gemeinsam genutzt 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 aktivierenAWS Management Console. Weitere Informationen finden Sie unter AWSGlobale Infrastruktur.

Sie können einen Workload mit einemAWS-Konto, einzelnen Benutzern in einem Konto oder mit beiden teilen. Wenn Sie einen Workload mit einem teilenAWS-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 bestimmtAWS-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 Organisationseinheiten teilen, bestimmt die Workload-Einladung mit den Berechtigungen der höchsten Ebene, welche Berechtigungen das Konto für den Workload hat.

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 Settings (Einstellungen) aus.
3. Wählen Sie AWS OrganizationsSupport aktivieren aus.

4. Wählen Sie Save settings (Einstellungen speichern).

Gemeinsamer Zugriff wird gelöscht

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.

Gemeinsamer Zugriff ändern

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 Speichern aus.

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

Workload-Einladungen annehmen und ablehnen

Eine Workload-Einladung ist eine Anfrage, 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 Einzelheiten zur Arbeitslast Seite für den Workload die Option Freigabe ablehnen aus.

Einen Workload löschen

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 eines Workload-Berichts

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.

Einzelheiten zur Arbeitslast

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

Registerkarte Overview (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.

Registerkarte „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.

Registerkarte „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 Definition eines Workloads.

Registerkarte „Aktien“

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 teilenAWS-Region, wählen Sie Create. Ein Workload kann mit bis zu 20 verschiedenen AWS-Konten AND-Benutzern geteilt 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).

Linsen

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

Bei eine 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 Objektiven, die auf Ihre Workloads angewendet werden können: Objektive aus dem Katalog von Objektiven und Objektive nach Maß.

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

Einem Workload können jeweils fünf Objektive hinzugefügt werden, wobei maximal 20 Objektive auf einen 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.

Einer Arbeitslast eine Linse hinzufügen

So fügen Sie einer Workload eine Linse hinzu

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 das hinzuzufügende Objektiv aus und klicken Sie auf Speichern.

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

Zu einem Workload können bis zu 20 Objektive hinzugefügt werden.

Weitere Informationen zum AWS Objektivkatalog finden Sie unter AWS Well-Architected Lenses. Beachten Sie, dass nicht jedes Whitepaper zu Objektiven im Objektivkatalog als Linse angeboten wird.

> **Haftungsausschluss**
>
> Indem Sie auf benutzerdefinierte Brillengläser zugreifen und/oder diese anwenden, die von einem anderen AWS Benutzer oder Konto erstellt wurden, erkennen Sie an, dass benutzerdefinierte Brillengläser, die von anderen Benutzern erstellt und mit Ihnen geteilt wurden, Inhalte Dritter sind, wie in der AWS Kundenvereinbarung definiert.

Ein Objektiv aus einem Workload entfernen

So entfernen Sie eine Linse aus einer 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 die Workload aus und klicken Sie auf View details (Details ansehen).
4. Deaktivieren Sie das Objektiv, das Sie entfernen möchten, und wählen Sie Speichern.

   Das AWS Well-Architected Framework Lens kann nicht aus einem Workload entfernt werden.

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

Einzelheiten zum Objektiv

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 „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 „Aktien“

Für ein benutzerdefiniertes Objektiv enthält die Registerkarte Shares eine Liste der IAM-Principals, mit denen das Objektiv gemeinsam genutzt wurde.

Benutzerdefinierte Objektive

Sie können benutzerdefinierte Objektive mit Ihren eigenen Säulen, Fragen, bewährten Methoden und Verbesserungsplänen erstellen. Sie wenden benutzerdefinierte Objektive auf dieselbe Weise auf eine Arbeitslast an, wie Sie AWS bereitgestellte Kontaktlinsen anwenden. Sie können auch benutzerdefinierte Objektive, die Sie erstellen, mit anderen teilen AWS-Konten, und benutzerdefinierte Objektive, die anderen gehören, können mit Ihnen geteilt werden.

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

Themen

Benutzerdefinierte Objektive anzeigen

Sie können die Details von benutzerdefinierten Objektiven, die Sie besitzen, und von benutzerdefinierten Objektiven, die mit Ihnen geteilt wurden, einsehen.

Um ein Objektiv anzusehen

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 Benutzerdefinierte Objektive aus.

   > **Note**
   >
   > Der Abschnitt Benutzerdefinierte Objektive ist leer, wenn Sie kein benutzerdefiniertes Objektiv erstellt haben oder kein benutzerdefiniertes Objektiv mit Ihnen geteilt haben.

3. Wählen Sie aus, welche benutzerdefinierten Objektive Sie sich ansehen möchten:
   - Gehört mir — Zeigt benutzerdefinierte Objektive an, die Sie erstellt haben.
   - Mit mir geteilt — Zeigt benutzerdefinierte Objektive an, die mit Ihnen geteilt wurden.
4. Wählen Sie das benutzerdefinierte Objektiv aus, das Sie auf eine der folgenden Arten betrachten möchten:
   - Wählen Sie den Namen des Objektivs.
   - Wählen Sie das Objektiv aus und wählen Sie Details anzeigen.

Die Seite Einzelheiten zum Objektiv wird angezeigt.

Die Seite „Benutzerdefinierte Objektive“ enthält die folgenden Felder:

Name

Der Name des Objektivs.

Eigentümer

Die AWS-Konto ID, der das benutzerdefinierte Objektiv gehört.

Status

Der Status VERÖFFENTLICHT bedeutet, dass die benutzerdefinierte Linse veröffentlicht wurde und auf Workloads angewendet oder mit anderen AWS-Konten geteilt werden kann.

Der Status ENTWURF bedeutet, dass die benutzerdefinierte Linse zwar erstellt, aber noch nicht veröffentlicht wurde. Eine benutzerdefinierte Linse muss veröffentlicht werden, bevor sie auf Workloads angewendet oder gemeinsam genutzt werden kann.

Version

Der Versionsname des benutzerdefinierten Objektivs.

Letzte Aktualisierung

Datum und Uhrzeit der letzten Aktualisierung der kundenspezifischen Objektive.

Ein benutzerdefiniertes Objektiv erstellen

Um ein benutzerdefiniertes Objektiv zu erstellen

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 Benutzerdefinierte Objektive aus.
3. Wählen Sie Benutzerdefiniertes Objektiv erstellen aus.
4. Wählen Sie Datei herunterladen, um die JSON-Vorlagendatei herunterzuladen.
5. Öffnen Sie die JSON-Vorlagendatei mit Ihrem bevorzugten Texteditor und fügen Sie die Daten für Ihr benutzerdefiniertes Objektiv hinzu. Zu diesen Daten gehören Ihre Säulen, Fragen, bewährte Verfahren und Links zu Verbesserungsplänen.

   Weitere Einzelheiten finden Sie unter Spezifikation des Objektivformats. Eine benutzerdefinierte Linse darf eine Größe von 500 KB nicht überschreiten.
6. Wählen Sie 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 „Senden und Vorschau“, um eine Vorschau des benutzerdefinierten Objektivs anzuzeigen, oder „Senden“, um das benutzerdefinierte Objektiv ohne Vorschau einzureichen.

   Wenn Sie Ihr benutzerdefiniertes Objektiv einreichen und in der Vorschau anzeigen möchten, können Sie auf Weiter klicken, um durch die Objektivvorschau zu navigieren, oder auf Vorschau beenden klicken, um zu den benutzerdefinierten Objektiven zurückzukehren.

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

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

Nachdem eine benutzerdefinierte Linse erstellt wurde, befindet sie sich im Status ENTWURF. Sie müssen die Linse veröffentlichen, bevor sie auf Workloads angewendet oder mit anderen AWS-Konten geteilt werden kann.

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

> **Haftungsausschluss**
>
> Geben oder sammeln Sie keine personenbezogenen Daten (PII) von Endbenutzern oder anderen identifizierbaren Personen in oder über Ihre benutzerdefinierten Brillengläser. Wenn Ihre benutzerdefinierte Linse oder die mit Ihnen geteilten und in Ihrem Konto verwendeten Linsen personenbezogene Daten enthalten oder sammeln, 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 eines benutzerdefinierten Brillenglases

Um eine Vorschau eines benutzerdefinierten Objektivs anzuzeigen

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 Benutzerdefinierte Objektive aus.
3. Nur Objektive mit dem Status ENTWURF können in der Vorschau angezeigt werden. Wählen Sie das gewünschte benutzerdefinierte DRAFT-Objektiv aus und wählen Sie „Erlebnisvorschau“.
4. Wählen Sie „Weiter“, um durch die Objektivvorschau zu navigieren.
5. (Optional) Sie können Ihren Verbesserungsplan überprüfen, indem Sie für jede Frage in der Vorschau die besten Methoden auswählen und 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 „Vorschau beenden“, um zur benutzerdefinierten Linse zurückzukehren.

> **Note**
>
> Sie können auch eine Vorschau eines benutzerdefinierten Objektivs anzeigen, indem Sie beim Erstellen eines benutzerdefinierten Objektivs die Option Senden und Vorschau auswählen.

Erstmaliges Veröffentlichen eines benutzerdefinierten Objektivs

Um ein benutzerdefiniertes Objektiv zu veröffentlichen

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 Benutzerdefinierte Objektive aus.
3. Wählen Sie das gewünschte benutzerdefinierte Objektiv aus und klicken Sie auf Linse veröffentlichen.
4. Geben Sie im Feld 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 Benutzerdefiniertes Objektiv veröffentlichen.

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

Die benutzerdefinierte Linse kann jetzt auf Workloads angewendet oder mit anderen AWS-Konten Benutzern geteilt werden.

Veröffentlichung eines Updates für ein benutzerdefiniertes Objektiv

Um ein Update für ein vorhandenes benutzerdefiniertes Objektiv zu veröffentlichen

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 Benutzerdefinierte Objektive aus.

3. Wählen Sie das gewünschte benutzerdefinierte Objektiv aus und klicken Sie auf Bearbeiten.
4. Wenn Sie keine aktualisierte JSON-Datei bereit haben, wählen Sie Datei herunterladen, um eine Kopie der aktuellen benutzerdefinierten Linse herunterzuladen. Bearbeiten Sie die heruntergeladene JSON-Datei mit Ihrem bevorzugten Texteditor und nehmen Sie die gewünschten Änderungen vor.
5. Wählen Sie „Datei auswählen“, um Ihre aktualisierte JSON-Datei auszuwählen, und wählen Sie „Senden und Vorschau“, um eine Vorschau der benutzerdefinierten Linse anzuzeigen, oder „Senden“, um die benutzerdefinierte Linse ohne Vorschau einzureichen.

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

   Nach der AWS WA Tool Validierung Ihrer JSON-Datei wird Ihre benutzerdefinierte Linse im Status ENTWURF unter Benutzerdefinierte Objektive angezeigt.
6. Wählen Sie erneut die benutzerdefinierte Linse aus und wählen Sie Linse veröffentlichen.
7. Wählen Sie „Änderungen vor der Veröffentlichung überprüfen“, um zu überprüfen, ob die an Ihrem benutzerdefinierten Objektiv vorgenommenen Änderungen korrekt sind. Dies beinhaltet die Überprüfung von:

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

   Wählen Sie Weiter aus.
8. Geben Sie die Art der Versionsänderung an.

   Hauptversion

   Zeigt an, dass wesentliche Änderungen am Objektiv vorgenommen wurden. Wird für Änderungen verwendet, die sich auf die Bedeutung des benutzerdefinierten Objektivs auswirken.

   Bei Workloads, bei denen das Objektiv angewendet wurde, wird eine Benachrichtigung darüber angezeigt, dass eine neue Version des benutzerdefinierten Objektivs verfügbar ist.

   Größere Versionsänderungen werden nicht automatisch auf Workloads angewendet, bei denen das Objektiv verwendet wird.

Unterversion

Zeigt an, dass geringfügige Änderungen am Objektiv vorgenommen wurden. Wird für kleine Änderungen verwendet, z. B. Textänderungen oder Aktualisierungen der URL-Links.

Kleinere Versionsänderungen werden mithilfe der benutzerdefinierten Linse automatisch auf Workloads angewendet.

Wählen Sie Weiter aus.

9. Geben Sie im Feld 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 Benutzerdefiniertes Objektiv veröffentlichen.

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

Die aktualisierte benutzerdefinierte Linse kann jetzt auf Workloads angewendet oder mit anderen AWS-Konten Benutzern geteilt werden.

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

Kleinere Versionsupdates werden automatisch und ohne Benachrichtigung installiert.

Sie können bis zu 100 Versionen eines benutzerdefinierten Objektivs erstellen.

Ein benutzerdefiniertes Objektiv teilen

Sie können eine benutzerdefinierte Linse mit anderen AWS-Konten Benutzern und Organisationseinheiten (OUs) teilen. AWS Organizations

Um eine benutzerdefinierte Linse 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 Benutzerdefinierte Objektive aus.

3. Wählen Sie die benutzerdefinierte Linse aus, die geteilt werden soll, und wählen Sie Details anzeigen aus.
4. Wählen Sie auf der Einzelheiten zum Objektiv Seite Shares aus. Wählen Sie dann Create and Create and Create Shares to users or accounts, um eine Lens-Share-Einladung zu erstellen.
5. Geben Sie die 12-stellige AWS-Konto ID oder den ARN des Benutzers ein, mit dem Sie das benutzerdefinierte Objektiv teilen möchten.
6. Wählen Sie Erstellen, um eine Einladung zur gemeinsamen Nutzung von Objektiven an den angegebenen Benutzer AWS-Konto oder zu senden.

Sie können benutzerdefinierte Objektive mit bis zu 300 AWS-Konten oder mehr Benutzern teilen.

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

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

Um eine benutzerdefinierte Linse mit Ihrer Organisation oder Ihren Organisationseinheiten 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 Benutzerdefinierte Objektive aus.
3. Wählen Sie die benutzerdefinierte Linse aus, die geteilt werden soll.
4. Wählen Sie auf der Einzelheiten zum Objektiv Seite Shares aus. Wählen Sie dann Create and Create Shares to Organizations.
5. Wählen Sie auf der Seite Benutzerdefinierte Linsenfreigabe erstellen aus, ob Sie der gesamten Organisation oder einer oder mehreren Organisationseinheiten Berechtigungen gewähren möchten.
6. Wählen Sie Erstellen, um die benutzerdefinierte Linse mit anderen zu teilen.

Um zu sehen, wer gemeinsam Zugriff auf eine benutzerdefinierte Linse hat, wählen Sie auf der Einzelheiten zum Objektiv Seite Shares aus.

> **Haftungsausschluss**
>
> Indem Sie Ihre benutzerdefinierten Brillengläser mit anderen teilen AWS-Konten, erklären Sie sich damit einverstanden, dass AWS Ihre benutzerdefinierten Objektive auch für diese anderen Konten verfügbar sind. Diese anderen Konten können weiterhin auf Ihre geteilten benutzerdefinierten Brillengläser zugreifen und diese verwenden, auch wenn Sie die benutzerdefinierten Brillengläser aus Ihren eigenen löschen AWS-Konto oder Ihre löschen AWS-Konto.

Hinzufügen von Tags zu einer benutzerdefinierten Linse

Um einem benutzerdefinierten Objektiv Tags hinzuzufügen

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 Benutzerdefinierte Objektive aus.
3. Wählen Sie das benutzerdefinierte Objektiv aus, das Sie aktualisieren möchten.
4. Wählen Sie im Bereich „Tags“ die Option „Tags verwalten“.
5. Wählen Sie Neues Tag hinzufügen aus und geben Sie den Schlüssel und den Wert für jedes Tag ein, das Sie hinzufügen möchten.
6. Wählen Sie Speichern.

Um ein Tag zu entfernen, klicken Sie neben dem Tag, das Sie entfernen möchten, auf Entfernen.

Löschen einer benutzerdefinierten Linse

Um ein benutzerdefiniertes Objektiv 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 im linken Navigationsbereich die Option Benutzerdefinierte Objektive aus.
3. Wählen Sie das benutzerdefinierte Objektiv aus, das gelöscht werden soll, und wählen Sie Löschen.
4. Wählen Sie Löschen aus.

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

Haftungsausschluss

Indem Sie Ihre benutzerdefinierten Objektive mit anderen teilen AWS-Konten, erkennen Sie an, AWS dass Ihre benutzerdefinierten Objektive diesen anderen Konten zur Verfügung stehen. Diese anderen Konten können weiterhin auf Ihre geteilten benutzerdefinierten Brillengläser zugreifen und diese verwenden, auch wenn Sie die benutzerdefinierten Brillengläser aus Ihren eigenen löschen AWS-Konto oder Ihre löschen AWS-Konto.

Spezifikation des Objektivformats

Objektive 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 Objektive verwenden, da sie die Grundstruktur für die Säulen, Fragen, bewährten Methoden und den Verbesserungsplan definiert.

Abschnitt „Objektive“

In diesem Abschnitt werden die Attribute für das benutzerdefinierte Objektiv selbst definiert. Dies ist sein Name und seine Beschreibung.

- `schemaVersion`: Die Version des benutzerdefinierten Linsenschemas, die verwendet werden soll. In der Vorlage festgelegt, nicht ändern.
- `name`: Name des Objektivs. Der Name kann bis zu 128 Zeichen lang sein.
- `description`: Textbeschreibung des Objektivs. Dieser Text wird angezeigt, wenn Sie Objektive auswählen, die während der Workload-Erstellung hinzugefügt werden sollen, oder wenn Sie eine Linse auswählen, die später auf einen vorhandenen 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 „Säulen“

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

Sie können bis zu 10 Säulen in einer benutzerdefinierten Linse definieren.

- `id`: ID für die Säule. Die ID kann zwischen 3 und 128 Zeichen lang sein und nur alphanumerische Zeichen und Unterstriche („_“) enthalten. Die in einer Säule verwendeten IDs müssen 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 bis zu 128 Zeichen lang sein.

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

```
            .
            .
        }
    ]
```

Abschnitt „Fragen“

In diesem Abschnitt werden die Fragen im Zusammenhang mit einer Säule definiert.

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

> **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 „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 definieren.

- `id`: ID für die Auswahl. Die ID kann zwischen 3 und 128 Zeichen lang sein und nur alphanumerische Zeichen und Unterstriche („_“) enthalten. Für jede Auswahl in einer Frage muss eine eindeutige ID angegeben werden. Wenn Sie eine Auswahl mit dem Suffix von hinzufügen, gilt _no dies als `None of these` Auswahlmöglichkeit für die Frage.
- `title`: Titel der Wahl. Der Titel kann bis zu 128 Zeichen lang sein.
- `helpfulResource displayText`: Optional. Text, der hilfreiche Informationen zu einer Auswahl enthält. Der Text kann bis zu 2048 Zeichen lang sein. Muss enthalten sein, falls `helpfulResource url` angegeben.
- `helpfulResource url`: Optional. Eine URL-Ressource, die die Auswahl genauer erklärt. Die URL muss mit `http://` oder beginnen`https://`.

- `improvementPlan displayText`: Text, der beschreibt, wie eine Auswahl verbessert werden kann. Der Text kann bis zu 2048 Zeichen lang sein. Eine `improvementPlan` ist für jede Auswahl erforderlich, außer für eine `None of these` Auswahl.
- `improvementPlan url`: Optional. Eine URL-Ressource, die bei der Verbesserung helfen kann. Die URL muss mit `http://` oder beginnen`https://`.
- `additionalResources type`: Optional. Die Art der zusätzlichen Ressourcen. Der Wert kann entweder `HELPFUL_RESOURCE` oder sein`IMPROVEMENT_PLAN`.
- `additionalResources content`: Optional. Gibt die `url` Werte `displayText` und für die zusätzliche Ressource an. Für eine Auswahl können bis zu fünf zusätzliche hilfreiche Ressourcen und bis zu fünf zusätzliche Verbesserungsplanelemente angegeben werden.
  - `displayText`: Optional. Text, der die hilfreiche Ressource oder den Verbesserungsplan beschreibt. Der Text kann bis zu 2048 Zeichen lang sein. Muss enthalten sein, falls `url` angegeben.
  - `url`: Optional. Eine URL-Ressource für die hilfreiche Ressource oder den Verbesserungsplan. Die URL muss mit `http://` oder beginnen`https://`.

> **Note**
>
> Wenn ein benutzerdefinierter Lens-Workload mit Jira synchronisiert wird, werden in den Auswahlmöglichkeiten die „ID“ der Frage und der Auswahl sowie der „Titel“ der Auswahl 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 „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 der Auswahlmöglichkeiten, der einer Risikostufe für die Frage zugeordnet wird, oder. `default`

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

Die Reihenfolge Ihrer Risikoregeln ist signifikant. Die ersten`condition`, die bewertet, `true` 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.

Beispielsweise:

```
"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 ausgewählt und ausgewählt `choice_2` `choice_3` ist, besteht ein mittleres Risiko.
- Wenn `choice_1` nicht ausgewählt, aber ausgewählt `choice_3` ist, besteht ebenfalls ein mittleres Risiko.
- Wenn keine dieser Vorbedingungen zutrifft, besteht ein hohes Risiko.

Objektiv-Upgrades

Das AWS Well-Architected Framework Lens und andere von bereitgestellte Objektive AWS werden aktualisiert, sobald neue Dienste eingeführt, bestehende Best Practices für cloudbasierte Systeme verfeinert und neue Best Practices hinzugefügt werden. Wenn eine neue Version eines Objektivs verfügbar ist, wird es aktualisiert, AWS WA Tool um die neuesten Best Practices widerzuspiegeln. Alle neuen Workloads, die definiert werden, verwenden die neue Version des Objektivs.

Ein Objektiv-Upgrade findet auch statt, wenn für ein benutzerdefiniertes Objektiv, das Sie auf einen Workload oder eine Review-Vorlage angewendet haben, eine neue Hauptversion veröffentlicht wurde.

Ein Objektiv-Upgrade kann aus einer beliebigen Kombination von folgenden Komponenten bestehen:

- 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 Objektiv-Upgrade nicht rückgängig machen. Nachdem ein Workload auf die neueste Objektivversion aktualisiert wurde, können Sie nicht zur vorherigen Version des Objektivs zurückkehren.

Auswahl eines Objektiv-Upgrades

Auf der Seite „Benachrichtigungen“ werden Informationen für jeden Workload angezeigt, der nicht die aktuelle Lens-Version verwendet.

Für jede Workload werden die folgenden Informationen angezeigt:

Ressource

Der Name des Workloads oder der Überprüfungsvorlage.

Ressourcentyp

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

Zugeordnete Ressource

Der Name des Objektivs.

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 — Der Workload verwendet eine Version des Objektivs, die nicht mehr den Best Practices entspricht. Aktualisieren auf die aktuelle Linsen-Version.

- Gelöscht — Der Workload verwendet eine Linse, die von ihrem Besitzer gelöscht wurde.

Verwendete Version

Die derzeit für die Workload verwendete Linsen-Version.

Aktuell verfügbare Version

Die für ein Upgrade verfügbare Objektivversion oder Keine, wenn das Objektiv 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).

Ein Objektiv aufrüsten

Objektive können für Workloads und zur Überprüfung von Vorlagen aktualisiert werden.

> **Note**
>
> Ein Objektiv-Upgrade kann nicht rückgängig gemacht werden. Nachdem eine Workload- oder Review-Vorlage auf die neueste Version des Objektivs aktualisiert wurde, können Sie nicht mehr zur vorherigen Version des Objektivs zurückkehren.

Ein Objektiv für einen Workload aktualisieren

1. Wählen Sie auf der Seite Benachrichtigungen einen Workload aus, der aktualisiert werden soll, und wählen Sie dann Linsenversion aktualisieren aus. In den einzelnen Säulen werden Informationen darüber angezeigt, was sich geändert hat.

   > **Note**
   >
   > Sie können auch auf der Registerkarte Workload-Übersicht die Option Verfügbare Upgrades anzeigen auswählen.

2. Bevor Sie ein Objektiv für einen Workload aktualisieren, wird ein Meilenstein erstellt, um den Status Ihres vorhandenen Workloads zum future Nachschlagen zu speichern. Geben Sie im Feld Meilensteinname einen eindeutigen Namen für den Meilenstein ein.
3. Aktivieren Sie das Bestätigungsfeld neben Ich verstehe und akzeptiere diese Änderungen und wählen Sie Speichern.

Sobald das Objektiv aktualisiert wurde, können Sie die vorherige Version des Objektivs auf der Registerkarte Meilensteine anzeigen.

Ein Objektiv für eine Testvorlage aufrüsten

1. Um das Objektiv für eine Testvorlage aufzurüsten, wählen Sie
2. Wählen Sie auf der Seite „Benachrichtigungen“ eine Testvorlage aus, die Sie aktualisieren möchten, und wählen Sie dann „Objektivversion aktualisieren“. Informationen darüber, was sich in den einzelnen Säulen geändert hat, werden angezeigt.

   > **Note**
   >
   > Sie können auch auf der Registerkarte „Übersicht“ der Bewertungsvorlage die Option Verfügbare Upgrades anzeigen auswählen.

3. Aktivieren Sie das Bestätigungsfeld neben Ich verstehe und akzeptiere diese Änderungen und wählen Sie Aktualisieren und Vorlagenantworten bearbeiten, um die Antworten auf bewährte Verfahren für Ihre Bewertungsvorlage anzupassen, oder Upgrade, um das Objektiv zu aktualisieren, ohne Ihre Vorlagenantworten zu ändern.

Objektiv-Katalog

Der Objektivkatalog ist eine Sammlung offizieller, von uns AWS entwickelter Objektive, AWS WA Tool die up-to-date Technologie und branchenspezifische Best Practices bieten. Diese Objektive stehen allen Benutzern zur Verfügung und erfordern keine zusätzliche Installation.

In der folgenden Tabelle werden alle AWS offiziellen Objektive beschrieben, die derzeit im Objektivkatalog erhältlich sind.

Name	Beschreibung
AWS Well-Architected Framework	Wird standardmäßig auf alle Workloads angewendet. Sammlung von bewährten Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme in der Cloud.

Name	Beschreibung
Vernetzte Mobilität	Bewährte Verfahren für die Integration von Technologie in Verkehrssysteme und die Verbesserung des allgemeinen Mobilität serlebnisses.
Container bauen	Bietet bewährte Methoden für den Entwurfs- und Build-Prozess von Containern.
Datenanalytik	Enthält Erkenntnisse aus realen Fallstudien und hilft Ihnen, die wichtigsten Designelemente von Well-Architected-Analytics-Workloads sowie Verbesserungsempfehlungen kennenzulernen. AWS
DevOps	Beschreibt einen strukturierten Ansatz, den Unternehmen jeder Größe verfolgen können, um eine schnelle, sicherheitsorienti erte Unternehmenskultur zu schaffen, die mithilfe moderner Technologien und bewährter Verfahren einen erheblichen Geschäftswert bieten kann. DevOps
Regierung	Bewährte Verfahren für die Gestaltung und Erbringung staatlicher Dienstleistungen am AWS.
Gesundheitsbranche	Bewährte Verfahren und Anleitungen für die Gestaltung, Bereitstellung und Verwaltung Ihrer Workloads im Gesundheitswesen in der AWS Cloud.
IoT	Bewährte Methoden für die Verwaltung Ihrer IoT-Workloads (Internet of Things) in AWS.

Name	Beschreibung
Wertschöpfung durch Fusionen und Übernahmen	Enthält eine Reihe zusätzlicher Fragen, die Sie bei der Suche nach Möglichkeiten zur Förderung des Unternehmenswachstums berücksichtigen sollten, z. B. bei Fusionen und Übernahmen von Private-Equity-Unternehmen.
Machine Learning	Bewährte Methoden für die Verwaltung Ihrer Ressourcen und Workloads für Machine Learning in AWS.
Migration	Bewährte Methoden für die Migration zum 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
Serverlose Anwendungen	Bewährte Methoden für die Erstellung serverloser Workloads auf. AWS Deckt Szenarien wie RESTful-Mikroservices, Backends für mobile Apps, Stream-Verarbeitung und Webanwendungen ab.

Vorlagen überprüfen

Sie können Bewertungsvorlagen erstellenAWS 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. Außerdem tragen sie 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 Methoden zu beantworten oder Notizen zu erstellen, die dann mit einem anderen IAM-Benutzer oder Konto oder einer Organisation oder Organisationseinheit derselben Organisation oder Organisationseinheit 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 einer Bewertungsvorlage

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 Linsen, 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.

Eine Bewertungsvorlage bearbeiten

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.

Eine Bewertungsvorlage teilen

Bewertungsvorlagen können mit Benutzern oder Konten oder mit einer gesamten Organisation oder Organisationseinheit geteilt 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 die Benutzer- oder 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 Organizationsden Zugriff aktivieren.

Definieren eines Workloads anhand einer Vorlage

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 “Ein Objektiv aufrüsten”.

> **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:GetReviewTemplate`,

`wellarchitected:GetReviewTemplateAnswerwellarchitected:ListReviewTemplateAns` und`wellarchitected:GetReviewTemplateLensReview`. Weitere Informationen zu IAM-Berechtigungen finden Sie im AWSIdentity 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 “Definition eines Workloads”.
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

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 aus.

Sie können aus einer gelöschten Bewertungsvorlage keinen neuen Workload erstellen. Wenn Sie eine Bewertungsvorlage, die Sie gelöscht haben, für andere IAM-Benutzer, Konten oder Organisationen freigegeben haben, können diese keine Workloads daraus erstellen.

Profile

Sie können Profile erstellen, um Ihren Geschäftskontext bereitzustellen, und Ziele festlegen, die Sie bei der Durchführung einer Well-Architected-Überprüfung erreichen möchten. AWS Well-Architected Toolverwendet die in Ihrem Profil gesammelten Informationen, um Ihnen zu helfen, sich während der Workload-Überprüfung auf eine priorisierte Liste von Fragen zu konzentrieren, die für Ihr Unternehmen relevant sind. Wenn Sie Ihrem Workload ein Profil zuordnen, können Sie auch sehen, welche Risiken für Sie priorisiert sind, damit Sie mit Ihrem Verbesserungsplan umgehen können.

Sie können auf der Seite Profile ein Profil erstellen und es einem neuen Workload zuordnen, oder Sie können einem vorhandenen Workload 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, die für Ihr Unternehmen im Plan zur Überprüfung und Verbesserung der Arbeitslast priorisiert wurden, zu verfeinern, wählen Sie im Abschnitt mit den Profilfragen die Antworten aus, die für Ihr Unternehmen am relevantesten sind.
5. (Optional) Fügen Sie im Abschnitt Schlagworte alle Tags hinzu, die Sie dem Profil zuordnen möchten.

   Weitere Informationen zu Tags finden Sie unterMarkieren Ihrer AWS WA Tool-Ressourcen.
6. Wählen Sie Speichern. 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, Beschreibung, ARN, Erstellungs- und Aktualisierungsdaten sowie Antworten auf die Profilfragen. Auf der Profilübersichtsseite kannst du dein Profil bearbeiten, löschen oder teilen.

Ein Profil bearbeiten

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 Speichern.

Ein Profil teilen

Profile können mit Benutzern oder Konten oder mit einer gesamten Organisation oder Organisationseinheit geteilt 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 Aktien.
4. Um Inhalte für einen Benutzer oder ein Konto freizugeben, wählen Sie Erstellen und anschließend Freigaben für IAM-Benutzer oder Konten erstellen aus. Geben Sie im Feld Einladungen senden die Benutzer- oder Konto-IDs an und wählen Sie Erstellen aus.
5. Um Inhalte für eine Organisation oder Organisationseinheit freizugeben, wählen Sie „Erstellen“ und anschließend „Freigaben für Organisationen erstellen“. Um für eine gesamte Organisation freizugeben, wählen Sie Berechtigungen für die gesamte Organisation gewähren aus. Um mit einer Organisationseinheit zu teilen, wählen Sie Berechtigungen für einzelne Organisationseinheiten gewähren aus, geben Sie die Organisationseinheit in dem Feld an und wählen Sie Erstellen.

> **Important**
>
> Bevor Sie ein Profil für eine Organisation oder Organisationseinheit (OU) freigeben, müssen Sie AWS Organizationsden Zugriff aktivieren.

Hinzufügen eines Profils zu einem Workload

Sie können einem vorhandenen Workload oder bei der Definition eines Workloads ein Profil hinzufügen, um den Prozess der Workload-Überprüfung zu beschleunigen. AWS WA Toolverwendet 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 “Definition eines Workloads”.

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**
   >
   > Nur ein Profil kann einem Workload 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 werden die Anzahl der beantworteten priorisierten Fragen und die priorisierten Risiken auf der Grundlage der Informationen im zugehörigen Profil angezeigt. 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 Beschreibung, der ARN, die Version und das Datum der letzten Aktualisierung für das dem Workload zugeordnete Profil angezeigt.

Ein Profil aus einem Workload entfernen

Wenn Sie ein Profil aus dem Workload entfernen, wird der Workload auf die Version zurückgesetzt, vor der das Profil damit verknüpft war, und Fragen und Risiken zur Workload-Überprüfung werden nicht mehr priorisiert.

So entfernen Sie ein Profil aus einem Workload

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.

Eine Benachrichtigung, dass das Profil erfolgreich aus dem Workload entfernt wurde, wird angezeigt. Durch das Entfernen eines Profils wird die Arbeitslast auf die Version zurückgesetzt, in der das Profil dem Profil zugeordnet wurde, und Fragen und Risiken zur Workload-Überprüfung 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 löschenAWS WA Tool.

Wenn Sie ein Profil von der Profilseite löschen, wird das Profil nicht aus den zugehörigen Workloads entfernt. Sie können weiterhin Profile verwenden, die vor dem Löschen geteilt und mit einem Workload verknüpft 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 teilenAWS-Konten, erkennen Sie an, dass AWS Ihre Profile diesen anderen Konten zur Verfügung stehen. Diese anderen Konten können weiterhin auf Ihre geteilten Profile zugreifen und diese verwenden, auch wenn Sie das Profil aus Ihrem eigenen löschen AWS-Konto oder Ihr Profil kündigenAWS-Konto.

Um ein Profil aus Ihrer Profilliste zu entfernen

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.

Informationen dazu, wie Sie ein Profil in Ihrer Profilliste behalten, es aber aus einem Workload entfernen möchten, finden Sie 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 den Text 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 Ihren AccessKeyIdund 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 eines AccessKeyIdgeheimen Schlüssels für Sie finden Sie AWS-Konto 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.

In Ihrem Jira-Konto sind keine weiteren Aktionen erforderlich, um den Connector zu installieren.

Um den Status des Connectors zu überprüfen 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“.
   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
- Heben Sie die Verknüpfung mit Ihrem AWS-Konto in Jira auf
- 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. Wählen Sie 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 “Ein Objektiv aufrüsten” 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

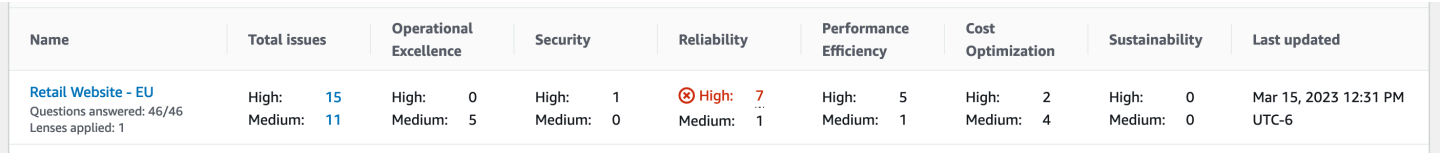
Der Abschnitt Well-Architected Framework-Probleme pro Säule zeigt eine grafische Darstellung der Anzahl der Probleme mit hohem und mittlerem Risiko pro Säule für alle Workloads.

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 in AWS Well-Architected Tool

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Well-Architected Tool, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. 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 gemeinsamen Verantwortung bei der Nutzung anwenden können AWS WA Tool. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS WA Tool , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS WA Tool Ressourcen unterstützen.

Themen

Datenschutz in AWS Well-Architected Tool

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Well-Architected Tool. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. 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, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. 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, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen 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 AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 Konsole, der API AWS WA Tool oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS 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 Daten, die von gespeichert werden, AWS WA Tool sind im Ruhezustand verschlüsselt.

Verschlüsselung während der Übertragung

Alle Daten, die zu und von AWS WA Tool ihnen gesendet werden, werden bei der Übertragung verschlüsselt.

Wie AWS werden Ihre Daten verwendet

Das AWS Well-Architected-Team sammelt aggregierte Daten von AWS Well-Architected Tool , um den AWS WA Tool Service für Kunden bereitzustellen und zu verbessern. Individuelle Kundendaten können an AWS-Konto Teams weitergegeben werden, um unsere Kunden bei der Verbesserung ihrer Workloads und Architektur zu unterstützen. Das AWS Well-Architected-Team kann nur auf Workload-Eigenschaften und ausgewählte Optionen für jede Frage zugreifen. AWS gibt keine Daten von AWS WA Tool außerhalb weiter. AWS

Zu den Workload-Eigenschaften, auf die das AWS Well-Architected-Team Zugriff hat, gehören:

- 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

Identitäts- und Zugriffsmanagement für AWS Well-Architected Tool

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS WA Tool IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS WA Tool

Dienstbenutzer — Wenn Sie den AWS WA Tool Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS WA Tool Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung bei AWS Well-Architected Tool Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS WA Tool haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS WA Tool Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS WA Tool. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS WA Tool Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von

IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS WA Tool, finden Sie unterWie AWS Well-Architected Tool funktioniert 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 AWS WA Tool identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. AWS Well-Architected Tool Beispiele für identitätsbasierte Richtlinien

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

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

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

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

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, 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 sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, 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 in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, 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 Verwenden von IAM-Rollen 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 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. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen 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 verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Diensten könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS

Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. 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.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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 Rolleninformationen von der AWS Management Console AWS CLI, der oder der 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 Erstellen von IAM-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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete 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 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF 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 verbreitete 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 Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs 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 darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Well-Architected Tool funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS WA Tool, mit welchen IAM-Funktionen Sie arbeiten können. AWS WA Tool

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

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

Einen allgemeinen Überblick darüber, wie AWS WA Tool und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte AWS WA Tool -Richtlinien

Unterstützt Richtlinienaktionen	Ja

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

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 der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation 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 innerhalb 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos 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 Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS WA Tool

Unterstützt Richtlinienaktionen	Ja

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

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 der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation 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.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS WA Tool verwendet:`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 Aktionen Definiert von AWS Well-Architected Tool in der Serviceautorisierungsreferenz.

Richtlinienressourcen

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen 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 Ressourcen definiert von AWS Well-Architected Tool in der Service Authorization Reference. 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 hat den folgenden ARN:

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

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (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 für eine bestimmte Ressource 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 Resources Defined by AWS Well-Architected Tool in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Well-Architected Tool definierte Aktionen.

Schlüssel zur Richtlinienbedingung für AWS WA Tool

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. 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, AWS wertet die Bedingung mithilfe 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

AWS WA Tool stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt aber die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel in der Service Authorization Reference.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. 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, AWS wertet die Bedingung mithilfe 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen 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 an viele AWS Ressourcen anhängen. 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 Was ist ABAC? 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 funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären

Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. 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 zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für AWS WA Tool

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Diensten könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.

Mit Diensten verknüpfte Rollen für AWS WA Tool

Unterstützt serviceverknüpfte Rollen	Nein

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. 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 Tool Beispiele 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 mit der AWS Management Console AWS CLI, oder AWS API ausführen. 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
- Vollzugriff auf Workloads gewähren
- Nur-Lese-Zugriff auf Workloads gewähren
- Zugriff auf einen Workload

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:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. 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 zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, 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 Konfigurieren eines MFA-geschützten API-Zugriffs 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 zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS WA Tool Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. 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, fügen Sie den Entitäten außerdem die folgende AWS verwaltete Richtlinie hinzu:

```
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.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. 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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

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

Vollzugriff auf Workloads gewähren

In diesem Beispiel möchten Sie einem Benutzer AWS-Konto vollen Zugriff auf Ihre Workloads gewähren. Vollzugriff ermöglicht es dem Benutzer, alle Aktionen in AWS WA Tool durchzuführen. 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": "*"
     }
   ]
}
```

Nur-Lese-Zugriff auf Workloads gewähren

In diesem Beispiel möchten Sie einem Benutzer in Ihrer Umgebung AWS-Konto nur Lesezugriff auf Ihre Workloads gewähren. 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": "*"
     }
   ]
}
```

Zugriff auf einen Workload

In diesem Beispiel möchten Sie einem Benutzer in Ihrer Region AWS-Konto nur Lesezugriff auf einen Ihrer Workloads gewähren. `99999999999955555555555566666666` `us-west-2` 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/99999999999955555555555666666666"
     }
   ]
}
```

AWS verwaltete Richtlinien für AWS Well-Architected Tool

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service 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 gewährt nur Lesezugriff auf. AWS Well-Architected Tool

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 gewährt Administratorberechtigungen AWS Organizations , die zur Unterstützung der AWS Well-Architected Tool Integration mit Organizations erforderlich sind. Diese Berechtigungen ermöglichen es dem Organisationsverwaltungskonto, die gemeinsame Nutzung von Ressourcen mit zu ermöglichen AWS WA Tool.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht Prinzipalen zu überprüfen, ob der AWS Dienstzugriff für AWS WA Tool aktiviert ist.
- `organizations:DescribeAccount`— Ermöglicht Prinzipalen das Abrufen von Informationen über ein Konto in der Organisation.
- `organizations:DescribeOrganization`— Ermöglicht Prinzipalen das Abrufen von Informationen über die Organisationskonfiguration.
- `organizations:ListAccounts`— Ermöglicht Prinzipalen das Abrufen der Liste der Konten, die zu einer Organisation gehören.
- `organizations:ListAccountsForParent`— Ermöglicht Prinzipalen, die Liste der Konten, die zu einer Organisation gehören, von einem bestimmten Stammknoten in der Organisation abzurufen.
- `organizations:ListChildren`— Ermöglicht Prinzipalen, die Liste der Konten und Organisationseinheiten, die zu einer Organisation gehören, von einem bestimmten Stammknoten in der Organisation abzurufen.
- `organizations:ListParents`— Ermöglicht Prinzipalen das Abrufen der Liste der unmittelbaren Eltern, die von der Organisationseinheit oder dem Konto innerhalb einer Organisation angegeben wurden.
- `organizations:ListRoots`— Ermöglicht Prinzipalen das Abrufen 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 Dienste und Ressourcen, die sich auf AWS WA Tool Ressourcen beziehen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `trustedadvisor:DescribeChecks`— Listet die verfügbaren Trusted Advisor Schecks auf.
- `trustedadvisor:DescribeCheckItems`— Ruft Trusted Advisor Prüfdaten ab, einschließlich Status und Ressourcen, die mit gekennzeichnet sind. Trusted Advisor
- `servicecatalog:GetApplication`— Ruft Details einer Anwendung ab. AppRegistry
- `servicecatalog:ListAssociatedResources`— Listet Ressourcen auf, die einer AppRegistry Anwendung zugeordnet sind.
- `cloudformation:DescribeStacks`— Ruft Details zu Stacks ab. AWS CloudFormation
- `cloudformation:ListStackResources`— Listet die mit den Stacks verknüpften Ressourcen auf. AWS CloudFormation
- `resource-groups:ListGroupResources`— Listet Ressourcen aus einem auf. ResourceGroup
- `tag:GetResources`— Erforderlich für ListGroupResources.
- `servicecatalog:CreateAttributeGroup`— Erstellt bei Bedarf eine vom Service verwaltete Attributgruppe.

- `servicecatalog:AssociateAttributeGroup`— Ordnet einer Anwendung eine vom Dienst verwaltete Attributgruppe zu. AppRegistry
- `servicecatalog:UpdateAttributeGroup`— Aktualisiert eine vom Dienst verwaltete Attributgruppe.
- `servicecatalog:DisassociateAttributeGroup`— Trennt eine vom Dienst verwaltete Attributgruppe von einer Anwendung. AppRegistry
- `servicecatalog:DeleteAttributeGroup`— Löscht bei Bedarf eine vom Service verwaltete Attributgruppe.

```
{
 "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 der verwalteten AWS Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS WA Tool seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS WA Tool Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWS WA Tool hat die verwaltete Richtlinie geändert	`"wellarchitected:Export*"` wurde `WellArchitectedCon`	22. Juni 2023

Änderung	Beschreibung	Datum
	`soleReadOnlyAccess` hinzugefügt.	
AWS WA Tool Richtlinie für Servicerollen hinzugefügt	Es wurde hinzugefü gt`AWSWellArchitected DiscoveryServiceRo lePolicy` , AWS Well-Arch itected Tool um den Zugriff auf AWS Dienste und Ressource n zu ermöglichen, die sich auf AWS WA Tool Ressourcen beziehen.	3. Mai 2023
AWS WA Tool Berechtigungen wurden hinzugefügt	Es wurde eine neue Aktion `ListAWSServiceAcce ssForOrganization` AWS WA Tool zum Gewähren hinzugefügt, mit der überprüft werden kann, ob der AWS Dienstzugriff aktiviert ist AWS WA Tool.	22. Juli 2022
AWS WA Tool hat begonnen, Änderungen zu verfolgen	AWS WA Tool hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	22. Juli 2022

Fehlerbehebung bei AWS Well-Architected Tool Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS WA Tool und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS WA Tool

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS WA Tool

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer *mateojackson* versucht, die `DeleteWorkload` Aktion über die Konsole auszuführen, aber nicht über die erforderlichen Berechtigungen verfügt.

```
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.

Reaktion auf Vorfälle in AWS Well-Architected Tool

Die Reaktion auf Vorfälle AWS Well-Architected Tool ist eine AWS Verantwortung. AWS verfügt über eine formelle, dokumentierte Richtlinie und ein Programm, die die Reaktion auf Vorfälle regeln.

AWS Betriebsprobleme mit weitreichenden Auswirkungen werden im AWS Service Health Dashboard veröffentlicht.

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

Konformitätsprüfung für AWS Well-Architected Tool

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

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

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services 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.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS Well-Architected Tool

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander 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 zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS Well-Architected Tool

Als verwalteter Dienst AWS Well-Architected Tool ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS WA Tool über das Netzwerk. 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.

Konfiguration und Schwachstellenanalyse in AWS Well-Architected Tool

Konfiguration und IT-Steuerung liegen in der gemeinsamen Verantwortung AWS von Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit dem verwirrten Stellvertreter 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 Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS Well-Architected Tool Ressource einen anderen Dienst gewähren. 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. z. B. `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 Linse sein.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, AWS WA Tool 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 Toolist in integriertAWS CloudTrail, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS -Service durchgeführten Aktionen in bereitstelltAWS WA Tool. CloudTrail erfasst alle API-Aufrufe fürAWS 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 in einem Amazon-S3-Bucket, einschließlich Ereignisse fürAWS WA Tool Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an gestellte AnfrageAWS WA Tool, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und weitere Angaben bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

AWS WA ToolInformationen in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres -Kontos für Sie aktiviert. Die inAWS WA Tool auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderenAWS -Serviceereignissen in Event history (Ereignisverlauf) aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -API-API-API-API-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 andereAWS -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
- CloudTrail Unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS CloudTrail

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

AlleAWS WA Tool Aktionen werden protokolliert CloudTrail und sind in Aktionen definiert von dokumentiertAWS Well-Architected Tool. Beispielsweise generieren Aufrufe der`CreateWorkloadShare` Aktionen`CreateWorkload`, `DeleteWorkload` und und 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 Anforderung mit Benutzer- oder Root-Benutzeranmeldeinformationen ausgeführt wurde
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

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 -Protokolleinträge können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. 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`CreateWorkload` Aktion 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 Toolsendet Ereignisse an Amazon EventBridge wenn Maßnahmen zu Well-Architecteding-Ressourcen ergriffen werden. Sie können EventBridge und diese Ereignisse zum Schreiben von Regeln, die Aktionen ausführen. Beispit können Sie benachrichtigt werden, wenn eine Ressourcenänderung auftritt. Weitere Informationen finden Sie unter Was ist Amazon EventBridge?

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

Die folgenden Aktionen führen zu EventBridge ereignisse:

- Workload-bezogene
  - Erstellen oder Löschen einer Arbeitslast
  - Erstellen eines Meilensteins
  - Aktualisieren der Eigenschaften einer Workload
  - Teilen oder Aufheben der Freigabe einer Workload
  - Aktualisieren des Status einer Freigabe-Einladung
  - Hinzufügen oder Entfernen von Tags
  - Aktualisieren einer Antwort
  - Aktualisieren von Bewertungsnotizen
  - Hinzufügen oder Entfernen eines Objektivs aus einer Workload
- Linsen-bezogene
  - Importieren oder Exportieren eines benutzerdefinierten Objektivs
  - Veröffentlichen einer benutzerdefinierten Linse
  - Löschen einer benutzerdefinierten Linse
  - Teilen oder Aufheben der Freigabe einer benutzerdefinierten Linse
  - Aktualisieren des Status einer Freigabe-Einladung
  - Hinzufügen oder Entfernen eines Objektivs aus einer Workload

Beispielereignisse ausAWS WA Tool

Dieser Abschnitt enthält Beispielereignisse aus AWS Well-Architected Tool.

Aktualisieren einer Antwort in einer 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 einer benutzerdefinierten Linse


```
{
   "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: 16. April 2024

Änderung	Beschreibung	Datum
Jira	In dieser Version wurde der AWS Well-Architected Tool Connector für Jira hinzugefügt.	16. April 2024
Neue Objektive	In dieser Version wurden dem Objektivkatalog neue Objektive hinzugefügt.	26. März 2024
Aktualisierte Funktionalität	Diese Version fügt die Objektiv-Katalog-Funktion hinzu AWS WA Tool.	26. November 2023
Aktualisierte Funktionalität	Diese Version fügt die Funktion „Vorlagen überprüfen“ hinzu AWS WA Tool.	3. Oktober 2023
WellArchitectedConsoleReadOnlyAccess Die verwaltete Richtlinie wurde aktualisiert	`"wellarchitected:ExportLens"` wurde `WellArchitectedConsoleReadOnlyAccess` hinzugefügt.	22. Juni 2023
Aktualisierte Funktionalität	Diese Version fügt die Profilfunktion zu hinzu AWS WA Tool.	13. Juni 2023
Aktualisierte Funktionalität	Diese Version verbessert die AWS Service Catalog AppRegistry Integration	3. Mai 2023

	AWS Trusted Advisor und fügt die AWS verwalteten Richtlinien `AWS WellArchitectedDiscoveryServiceRolePolicy` hinzu.	
Aktualisierung des Inhalts	Die Dashboard-Seite wurde aktualisiert und enthält nun detaillierte Informationen zum Risiko- und Verbesserungsplan. Die Möglichkeit, einen konsolidierten Workload-Bericht zu erstellen, wurde ebenfalls hinzugefügt.	30. März 2023
Aktualisierung des Inhalts	Der Name der WellArchitectedConsoleReadOnlyAccess Richtlinie wurde korrigiert.	19. Januar 2023
Die IAM-Leitlinien für wurden aktualisiert AWS WA Tool	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	4. Januar 2023
Aktualisierte Funktionalität	In dieser Version wird das FTR-Objektiv aus dem Werkzeug entfernt.	14. Dezember 2022
Aktualisierte Funktionalität	In dieser Version wird die AWS Service Catalog AppRegistry Integration AWS Trusted Advisor und hinzugefügt.	7. November 2022

Aktualisierung des Inhalts	Ein Problem im JSON-Beispiel für benutzerd efinierte Objektive wurde behoben`choices`.	29. September 2022
Aktualisierung des Inhalts	Der `choices` Abschnitt der JSON-Spezifikation für benutzerdefinierte Objektive wurde aktualisiert.	02.August 2022
Aktualisierte Funktionalität	In dieser Version wurde die Nachverfolgung von Änderungen für die AWS verwalteten Richtlinien hinzugefügt. Außerdem wurde eine neue Aktion hinzugefügt, mit der die `ListAWSServiceAcce ssForOrganization` Genehmigung erteilt werden kann`AWSWellArchitected OrganizationsServi ceRolePolicy` .	22. Juli 2022
Teilen von Organisationen hinzugefügt	Diese Version bietet die Möglichkeit, Workloads und benutzerdefinierte Objektive mit einer Organisation und Organisationseinheiten (OUs) gemeinsam zu nutzen.	30. Juni 2022

Aktualisierte Funktionalität	Diese Version bietet die Möglichkeit, zusätzliche Ressourcen für Auswahlmöglichkeiten in einer benutzerdefinierten Linse anzugeben, eine Vorschau einer benutzerdefinierten Linse anzuzeigen, bevor sie veröffentlicht wird, und benutzerdefinierte Objektive mit Tags zu versehen.	21. Juni 2022
Aktualisierte Funktionalität	Diese Version bietet die Möglichkeit, auf re:POST auf die AWS Well-Architected-Community zuzugreifen. AWS	31. Mai 2022
Aktualisierte Funktionalität	Diese Version fügt dem Tutorial die Säule Nachhaltigkeit und kleinere Updates hinzu.	31. März 2022
EventBridge Unterstützung hinzugefügt	AWS WA Tool sendet jetzt ein Ereignis an Amazon, EventBridge wenn eine Änderung an einer Well-Architected-Ressource vorgenommen wird.	3. März 2022
Benutzerdefinierte Objektive hinzugefügt	Die Möglichkeit, benutzerdefinierte Objektive hinzuzufügen, wurde hinzugefügt.	29. November 2021
Aktualisierte Funktionalität	Einzelne bewährte Verfahren können jetzt als nicht zutreffend markiert werden.	14. Juli 2021

Ressourcen-Tagging verfügbar	Diese Version bietet die Möglichkeit, Workloads Tags hinzuzufügen.	3. März 2021
Die API ist jetzt verfügbar	Diese Version fügt die AWS WA Tool API hinzu. AWS CloudTrail Protokollierungsinformationen hinzugefügt.	16. Dezember 2020
Aktualisierte Funktionalität	Diese Version erweitert das Tool um die FTR- und SaaS-Objektive.	3. Dezember 2020
Der Datenschutz wurde aktualisiert	Datenschutzinformationen aktualisiert.	5. November 2020
Aktualisierung des Inhalts	Es wurde klargestellt, dass Sie nach dem Upgrade eines Workloads zur Verwendung eines neuen Objektivs nicht zur vorherigen Version zurückkehren können.	8. Juli 2020
Aktualisierung des Inhalts	Klares Teilen in, AWS-Regionen das 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

Aktualisierung der Inhalte	Definitionen für Probleme mit hohem Risiko (HRI) und Probleme mit mittlerem Risiko (MRIs) wurden hinzugefügt.	12. Juni 2020
Aktualisierung des Inhalts	Ein Abschnitt darüber, wie Ihre Daten AWS verwendet werden, wurde 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
Aktualisierung des Inhalts	Es wurde klargestellt, dass AWS-Region Workload-Shares spezifisch sind.	10. Januar 2020
Aktualisierte Funktionalität	Diese Version fügt die Workload-Freigabe hinzu.	9. Januar 2020
Aktualisierung des Inhalts	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 Verbesser ungsplanelemente in den Workload-Bericht ein.	29. Juli 2019
Aktualisierte Funktionalität	Die Version fügt die DeleteWor kload Aktion der Richtlinie hinzu.	18. Juli 2019

Aktualisierung des Inhalts	Der Inhalt in diesem Handbuch wurde aktualisiert und enthält jetzt kleinere Fehlerbeh ebungen.	19. Juni 2019
Aktualisierung des Inhalts	Der Inhalt in diesem Handbuch wurde aktualisiert und enthält jetzt kleinere Fehlerbeh ebungen.	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	Diese Version bietet die Möglichkeit,AWS-Regionen bei der Definition eines Workloads anzugeben, was nicht.	14. Februar 2019
AWS Well-Architected Tool allgemeine Verfügbarkeit	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.