aws

Benutzerhandbuch

Service Quotas

Service Quotas: Benutzerhandbuch

Table of Contents

Was ist Service Quotas?

Mit Service Quotas können Sie Ihre Kontingente anzeigen und verwaltenAWS-Servicesvon zentraler Lage aus. Limits, auch Limits in genanntAWS-Services, sind die Höchstwerte für die Ressourcen, Aktionen und Elemente in Ihrem.AWS-Kontoaus. EACHAWS-Servicedefiniert seine Kontingente und legt Standardwerte für diese Kontingente fest. Je nach Ihren geschäftlichen Anforderungen können Sie Ihre Service-Kontingentwerte erhöhen. Service Quotas ermöglichen es Ihnen, Ihre Service-Quoten nachzuschlagen und Erhöhungen anzufordern.AWS Supportkann Ihre Anfragen genehmigen, ablehnen oder teilweise genehmigen.

Inhalt

Merkmale von Service Quotas

Servicekontingente bieten folgende Funktionen:

Sehen Sie Ihre Servicekontingente an

Die Konsole Servicekontingente bietet schnellen Zugriff aufAWSStandardkontingentwerte für Ihr Konto für alleAWS-Regionenaus. Wenn Sie einen Service in der Service-Quotas-Konsole auswählen, sehen Sie die Kontingente und ob das Kontingent anpassbar ist. Angewandte Kontingentesind Überschreibungen oder Erhöhungen für eine bestimmte Quote über dieAWSStandardwert.

Anfordern einer Service-Kontingenterhöhung

Für anpassbare Service Quotas können Sie Servicekontingente verwenden, um eine Kontingenterhöhung zu beantragen. Um eine Kontingenterhöhung zu beantragen, wählen Sie in der Konsole Servicekontingente den Service und das spezifische Kontingent aus und wählen Sie dannKontingenterhöhung anfordernaus. Sie können auch Service Quotas API-Operationen oder dieAWS CLITools zur Anforderung von Servicekontingenterhöhungen.

Aktuelle Auslastung der Ressourcen anzeigen

Nachdem Ihr Konto für einen bestimmten Zeitraum aktiv wurde, können Sie ein Diagramm Ihrer Ressourcenauslastung anzeigen.

Servicekontingente in

Die folgenden Begriffe sind für ein Verständnis der Funktionsweise von Servicekontingente wichtig.

Servicekontingent

Die maximale Anzahl von Serviceressourcen oder -operationen, die für eineAWS-Kontooder einAWS-Regionaus. Die Anzahl vonAWS Identity and Access Management(IAM) Rollen pro Konto sind ein Beispiel für ein kontobasiertes Kontingent. Die Anzahl der Virtual Private Clouds (VPCs) pro Region ist ein Beispiel für ein regionsbasiertes Kontingent. Um festzustellen, ob ein Dienstkontingent regionsspezifisch ist, überprüfen Sie die Beschreibung des Dienstkontingents.

Anpassbarer Wert

Ein Kontingentwert, der erhöht werden kann.

angewandte Quote

Der aktualisierte Kontingentwert nach einer Kontingenterhöhung.

Standardwert

Der anfängliche Kontingentwert, der durchAWSaus.

globale Kontingent

Ein Dienstkontingent, das auf Kontoebene angewendet wird. Globale Kontingente sind in allen verfügbarAWS-Regionenaus. Sie können eine Erhöhung eines globalen Kontingents von jeder Region beantragen. Sie können den Status der Erhöhung von der Region verfolgen, in der Sie die Erhöhung angefordert haben. Wenn Sie eine Quotenerhöhung für ein globales Kontingent beantragen, können Sie keine Erhöhung für dasselbe Kontingent von einer anderen Region beantragen, bis die erste Anfrage abgeschlossen ist. Nachdem die erste Anforderung abgeschlossen ist, ist der angewendete Kontingentwert in allen Regionen sichtbar, in denen angewendete Kontingente verfügbar sind.

Nutzung

Die Anzahl der Ressourcen oder Operationen, die für ein Servicekontingent verwendet werden.

Nutzung

Der Prozentsatz eines verwendeten Servicekontingents. Wenn der Kontingentwert beispielsweise 200 Ressourcen beträgt und 150 Ressourcen verwendet werden, beträgt die Auslastung 75 Prozent.

Zugreifen auf Service Quotas

Sie können Servicekontingente wie folgt nutzen:

AWS Management Console

Die Konsole Servicekontingenteist eine browserbasierte Oberfläche, über die Sie Ihre Servicekontingente anzeigen und verwalten können. Sie können fast jede Aufgabe im Zusammenhang mit Ihren Servicekontingente über die Konsole ausführen. Sie können von jedem aus auf Service Quotas zugreifenAWS Management Consoleindem Sie es in der oberen Navigationsleiste auswählen oder nach Service Quotas imAWS Management Consoleaus.

AWS Command Line InterfaceWerkzeuge

Durch die Verwendung desAWS Command Line Interface-Tools können Sie Befehle in der Befehlszeile Ihres Systems ausgeben, um Service Quotas und andereAWS-Aufgaben. Dies kann ein schnellerer und bequemer Ansatz sein als die Verwendung der Konsole. Die Befehlszeilen-Tools sind auch hilfreich, wenn Sie Skripts erstellen möchten, die AWS-Aufgaben ausführen.

AWS bietet zwei Sätze an Befehlszeilen-Tools: AWS Command Line Interface und AWS Tools for Windows PowerShell. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im AWS Command Line InterfaceLeitfaden. Informationen zu der Installation und Verwendung der Tools for Windows PowerShell finden Sie im AWS Tools for Windows PowerShell-Leitfaden.

AWS-SDKs

DieAWSDie -SDKs bestehen aus Bibliotheken und Beispiel-Code für verschiedene Programmiersprachen und Plattformen (beispielsweiseJava,Python,Ruby,.NET,iOS und Android, undandere) enthalten. Mit den SDKs werden auch Aufgaben wie das kryptografische Signieren, die Verwaltung von Fehlern und die automatische Wiederholung von Anforderungen abgedeckt. Weitere Informationen über die AWS-SDKs, inkl. Herunterladen und Installation, finden Sie unter Tools für Amazon Web Services.

Erste Schritte mit Service Quotas

Wenn Sie die Service Quotas Quotas-Konsole öffnen, zeigt das Dashboard Karten für bis zu neun Dienste an. Jede Karte listet die Anzahl der Service-Kontingente fürAWS-Serviceaus. Wenn Sie eine Karte auswählen, wird eine Seite geöffnet, auf der die Kontingente für den Service angezeigt werden. Sie können auswählen, welche Dienste im Dashboard angezeigt werden.

So ändern Sie die Dashboard-Dienstkarten

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie im -DashboardÄndern Sie Dashboard-Kartenaus.
3. Die derzeit ausgewählten Dienste werden auf der rechten Seite angezeigt. Wenn Sie neun Dienste ausgewählt haben, müssen Sie einen Dienst entfernen, bevor Sie einen anderen Service hinzufügen können. Wählen Sie für jeden Dienst, den Sie im Dashboard nicht benötigenRemoveaus.
4. Um einen Service zum Dashboard hinzuzufügen, wählen Sie ihn ausWählen Sie Diensteaus.
5. Wenn Sie mit dem Hinzufügen und Entfernen der Dienste fertig sind, wählen SieSaveaus.

Nächste Schritte

- Anzeigen von Servicekontingenten
- Beantragen einer Kontingenterhöhung

Anzeigen von Servicekontingenten

Service Quotas ermöglichen es Ihnen, den Wert eines bestimmten nachzuschauenKontingent, auch alsBegrenzungaus. Sie können auch alle Kontingente nachlesenAWS-Serviceaus.

So zeigen Sie die Kontingente für einen Service an

1. Melden Sie sich bei der anAWS Management ConsoleÖffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie im Navigationsbereich AWS-Services.
3. Wählen Sie eineAWS-ServiceGeben Sie den Namen des Service in das Suchfeld ein. Für jedes Kontingent zeigt die Konsole den Namen, das angewendete Kontingent, das Standardkontingent und die Einstellung an, ob das Kontingent einstellbar ist. Wenn der angewendete Wert nicht verfügbar ist, wird die Konsole angezeigtNicht verfügbaraus.
4. Wählen Sie den Kontingentnamen, um zusätzliche Informationen zu einem Kontingent anzuzeigen, z. B. seine Beschreibung und den Amazon-Ressourcennamen (ARN).

Beantragen einer Kontingenterhöhung

Für einstellbare -Kontingente können Sie eine Kontingenterhöhung beantragen. Kleinere Erhöhungen werden automatisch genehmigt und größere Anfragen werden anAWS Supportaus. Sie können Ihren Anforderungsfall in der AWS Support-Konsole verfolgen. Anfragen zur Erhöhung der Servicekontingente erhalten keinen bevorzugten Support. Wenn Sie eine dringende Anfrage haben, wenden Sie sich bitte anAWS Supportaus.

AWS Supportkann Ihre Anfragen genehmigen, ablehnen oder teilweise genehmigen.

So beantragen Sie eine Service-Kontingenterhöhung

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie im Navigationsbereich AWS-Services.
3. Wählen Sie einAWS-ServiceÜber die Liste oder geben Sie den Namen des Service in das Suchfeld ein.
4. Wenn das Kontingent einstellbar ist, können Sie die Schaltfläche oder den Namen auswählen und dann auswählenKontingenterhöhung beantragenaus.
5. Geben Sie unter Change quota value (Kontingentwert ändern) den neuen Wert ein. Der neue Wert muss größer als der aktuelle Wert sein.
6. Wählen Sie Request (Anfrage).

Um ausstehende oder kürzlich genehmigte Anfragen anzuzeigen, wählen Sie im Navigationsbereich die Option Dashboard . Wählen Sie für ausstehende Anfragen den Status der Anfrage, um die Anfrage zu öffnen. Der Anfangsstatus einer Anfrage istAusstehendaus. Nachdem der Status sich in geändert hatAnforderungskontingentfinden Sie die Fallnummer mitAWS Supportaus. Wählen Sie die Fallnummer, um das Ticket für Ihre Anfrage zu öffnen.

Nachdem die Anfrage genehmigt wurde, wird Applied quota value (Angewandter Kontingentwert) für das Kontingent auf den neuen Wert eingestellt.

Verlauf der Kontingentanforderung anzeigen

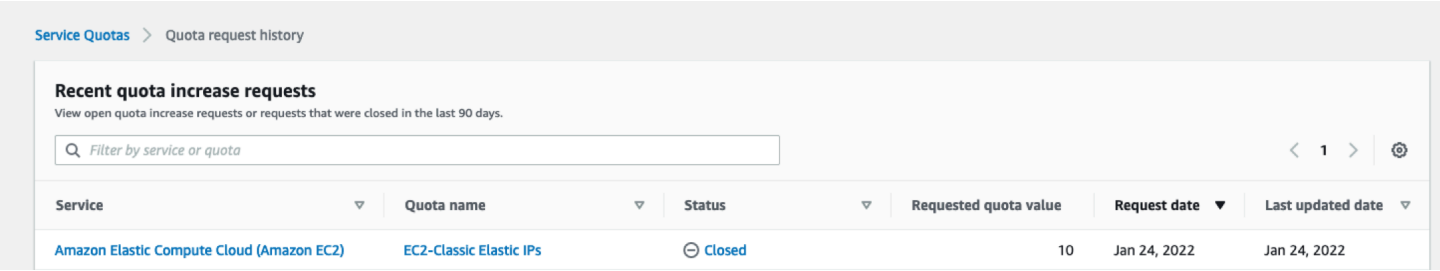
Informationen zum Anfordern finden Sie in der Service Quotas Quotas-Konsole. Die Konsole zeigt alle offenen Kontingenterhöhungsanträge sowie Kontingentanträge an, die in den letzten 90 Tagen geschlossen wurden.

> **Note**
>
> Importieren in &S3;AWS-Service, wie IAM, ist möglicherweise nur in bestimmten Regionen verfügbar. Wenn Sie Quotenerhöhungsanträge in verschiedenen Regionen haben, wählen Sie zuerst die entsprechende Region aus.

Gehen Sie wie folgt vor, um den Verlauf der Kontingentanforderung anzuzeigen:

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Um ausstehende oder kürzlich genehmigte Anfragen anzuzeigen, wählen SieKontingentanforderungsverlaufÜber den Navigationsbereich.

DieLetzte Anträge auf Kontingenterhöhungzeigt Informationen über Ihre offenen Anfragen zur Erhöhung der Quotenerhöhung und alle Anfragen an, die innerhalb von 90 Tagen geschlossen wurden.



- -Service— Zeigt den Dienstnamen an, der für die Anforderung ausgewählt wurde.
- Kontingentname— Zeigt den Kontingentnamen an, der für die Quotenerhöhung ausgewählt wurde.
- Status— Zeigt den Status eines Antrags auf eine Quotenerhöhung an.

  Möglicherweise sehen Sie die folgenden Statusarten:

  - Closed (Abgeschlossen)— Quotenerhöhung genehmigt und Antrag geschlossen.
  - Kontingentanforderung genehmigt— Quotenerhöhung wird automatisch genehmigt.

  - Anforderungskontingent— Antrag auf Quotenerhöhung ausstehendAWS Supportgenehmigungen.
- Anforderungskontingentwert— Der erhöhte Kontingentwert, den Sie für das Kontingent angefordert haben.
- Anforderungsdatum— Das Datum, an dem Sie die Quotenerhöhung angefordert haben.
- Datum der letzten Aktualisierung— Das letzte Datum, an dem die Anfrage ein Update erhalten hat.

Zeigen Sie Details zu einem Dienst, Kontingentnamen und Status imKontingentanforderungsverlauf-Tabelle, indem Sie einen der Einträge auswählen.

Markieren von Ressourcen in Service Quotas

Ein Tag ist eine benutzerdefinierte Attributskennzeichnung, die Sie zu einer AWS-Ressource hinzufügen, damit sich Ressourcen einfacher identifizieren, organisieren und finden lassen. Jedes Tag besteht aus zwei Teilen:

- EINTag-Schlüssel, wie beispielsweise`CostCenter`,`Environment`, oder`Project`aus. Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- EIN-Tag-Wert, wie beispielsweise`111122223333`oder`Production`aus. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht Null festlegen. Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge. Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß-/Kleinschreibung unterschieden.

Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren.

Tags sind für folgende Aktivitäten nützlich:

- Identifizieren und Organisieren Ihrer AWS-Ressourcen. Viele Amazon Web Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services denselben Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind.
- Überwachen von AWS-Kosten. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. Weitere Informationen finden Sie unter Use cost allocation tags (Verwendung von Kostenzuordnungs-Tags) im AWS Billing-Benutzerhandbuch.
- Kontrollieren Sie den Zugriff auf Ihre AWS-Ressourcen. Weitere Informationen finden Sie unter Controlling access using tags (Zugriffssteuerung mit Tags) im IAM-Benutzerhandbuch.

Themen

- Verwalten von Service-Kontingent-Tags (AWSAPI)
- Zugriffssteuerung mit Service Quotas-Tags

Ressourcen, die das Markieren von Service Quotas unterstützen

Die Service-Kontingente-Ressourcen für die Tagging-UnterstützungAngewandte Kontingente, zuvor beantragte Quotenerhöhungen genehmigt vonAWS Supportaus.

> **Important**
>
> Sie können Kontingente nur kennzeichnen, wenn sie einen angewendeten Kontingentwert haben. Kontingente mit Standardkontingentwerten können nicht markiert werden. Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Tags sind nicht für private oder sensible Daten gedacht.

Tag (Markierung)-Einschränkungen

Für Tags in Servicekontingente-Ressourcen gelten die folgenden Einschränkungen:

- Die maximale Anzahl der Tags, die Sie einer Ressource zuweisen können – 50.
- Maximale Schlüssellänge – 128 Unicode-Zeichen.
- Maximale Wertlänge – 256 Unicode-Zeichen.
- Valid characters for key and value – a-z, A-Z, 0-9, space, and the following characters: _ . : / = + - and @
- Bei Schlüsseln und Werten wird die Groß-/Kleinschreibung berücksichtigt.
- Verwenden Sie nicht`aws:`als Präfix für den Schlüssel, da es für reserviert istAWSVerwendung von Verwendung von

Erforderliche Berechtigungen für das Markieren von Servicekontingenten-Ressourcen

Sie müssen Berechtigungen konfigurieren, damit Ihre Benutzer oder Rollen Tags in Servicekontingenten verwalten können. Die Berechtigungen, die für die Verwaltung von Tags erforderlich sind, entsprechen in der Regel den API-Operationen für die Aufgabe.

Um sicherzustellen, dass Benutzer und Rollen die Service Quotas Konsole für Tagging-Vorgänge verwenden können, hängen Sie die`ServiceQuotasReadOnlyAccess` AWSVerwaltete Richtlinie für die Entitäten. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

- Um Tags zu angewendeten Kontingenten hinzufügen zu können, müssen Sie über die folgenden Berechtigungen verfügen:

  `servicequotas:ListTagsForResource`

  `servicequotas:TagResource`
- Zum Anzeigen von Tags für ein angewendetes Kontingent benötigen Sie die folgenden Berechtigungen:

  `servicequotas:ListTagsForResource`
- Um vorhandene Tags aus einem angewendeten Kontingent zu entfernen, müssen Sie über die folgenden Berechtigungen verfügen:

  `servicequotas:UntagResource`
- Um vorhandene Tag-Werte für angewendete Kontingente zu bearbeiten, müssen Sie über die folgenden Berechtigungen verfügen:

  `servicequotas:ListTagsForResource`

  `servicequotas:TagResource`

  `servicequotas:UntagResource`

Verwalten von Service Quotas-Tags (Konsole)

Sie können Service-Kontingent-Tags verwalten, indem Sie dieAWS Management Consoleaus.

1. Melden Sie sich bei derAWS Management ConsoleÖffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie auf der NavigationsseiteAWSDienstleistungenaus.
3. Wählen Sie einAWS-ServiceGeben Sie aus der Liste aus oder geben Sie den Namen des Service in das Suchfeld ein.
4. Wählen Sie einen Service mit einem Wert in derAngewandter Kontingentwertcolumn.

5. Wählen Sie im Abschnitt Tags (Markierungen) die Option Manage tags (Tags (Markierungen) verwalten). Diese Option ist für Kontingente ohne angewendeten Kontingentwert nicht verfügbar.
6. Sie können Tags hinzufügen oder entfernen oder Tag-Werte für vorhandene Tags bearbeiten. Geben Sie einen Namen für das Tag ein inSchlüsselaus. Sie können einen optionalen Wert für das Tag unter Value (Wert) hinzufügen.
7. Nachdem Sie alle Ihre Änderungen an Tags vorgenommen haben, wählen SieSpeichern Sie die Änderungenaus.

Wenn der Vorgang erfolgreich ist, kehren Sie zur Kontingentdetailseite zurück, auf der Sie Ihre Änderungen überprüfen können. Wenn der Vorgang fehlschlägt, befolgen Sie bitte die Anweisungen in der Fehlermeldung, um ihn zu beheben.

Verwalten von Service-Kontingent-Tags (AWS CLI)

Sie können Service-Kontingent-Tags verwalten, indem Sie dieAWS Command Line Interface(AWS CLI) enthalten.

- So fügen Sie Tags zu angewendeten Kontingenten hinzu

  `aws service-quotas tag-resource`
- So zeigen Sie Tags für eine angewendete Kontingent an

  `aws service-quotas list-tags-for-resource`
- So löschen Sie vorhandene Tag-Werte für angewendete Kontingente

  `aws service-quotas untag-resource`

Verwalten von Service-Kontingent-Tags (AWSAPI)

Sie können Service-Kontingent-Tags mithilfe der Service-Quotas-API verwalten.

- So fügen Sie Tags zu angewendeten Kontingenten hinzu

  `TagResource`
- So zeigen Sie Tags für eine angewendete Kontingent an

  `ListTagsForResource`

- So löschen Sie vorhandene Tag-Werte für angewendete Kontingente

  `UntagResource`

Zugriffssteuerung mit Service Quotas-Tags

Um den Zugriff auf Servicekontingentressourcen basierend auf Tags zu steuern, stellen Sie Tag-Informationen in der Condition -Element einer Richtlinie unter Verwendung von `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder `aws:TagKeys` Bedingungsschlüssel. Weitere Informationen über diese Bedingungsschlüssel finden Sie unter Steuern des Zugriffs auf AWS-Ressourcen mit Ressourcen-Tags im IAM User Guide aus.

Wenn Sie z. B. die folgende Richtlinie an AWS Identity and Access Management (IAM) Benutzer oder Rolle, diese Entität kann eine Erhöhung auf Amazon Athena angewendete Kontingente, die mit dem Tag-Schlüssel gekennzeichnet sind **`Owner`** und Tag-Wert **`admin`** aus.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["servicequotas:RequestServiceQuotaIncrease"],
            "Resource": "arn:aws:servicequotas:*:*:athena/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "admin"}
            }
        }
    ]
}
```

Sie können Tags auch an IAM-Entitäten (Benutzer oder Rollen) anfügen, um die attributbasierte Zugriffskontrolle (ABAC) zu verwenden. ABAC ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. 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.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Informationen zum Anzeigen eines Tutorials mit Schritten zum Einrichten von ABAC finden Sie unterIAM-Tutorial: Definieren Sie ZugriffsberechtigungenAWS-Ressourcen basierend auf TagsimIAM User Guideaus.

Verwenden von Anforderungsvorlagen für Servicekontingente

EINKontingent-Anforderungsvorlagehilft Ihnen, Zeit zu sparen, wenn Sie Kontingente für neue anpassenAWS-KontenIn Ihrer Organisation. Um eine Vorlage zu verwenden, konfigurieren Sie die gewünschten Service-Kontingenterhöhungen für neue Konten. Aktivieren Sie dann die Vorlagenzuordnung. Dies verknüpft die Vorlage mit Ihrer Organisation inAWS Organizationsaus. Immer wenn neue Konten in Ihrer Organisation erstellt werden, fordert die Vorlage automatisch Kontingenterhöhungen für Sie an.

Um eine Anforderungsvorlage verwenden zu können, müssen SieAWS Organizations- und die neuen Konten müssen in derselben Organisation erstellt werden. Ihre Organisation muss alle Funktionen aktiviert haben,Alle Funktionenaus. Wenn Sie nur die konsolidierten Fakturierung verwenden, können Sie keine Kontingentanforderungsvorlagen verwenden.

Sie können die Anforderungsvorlage aktualisieren, indem Sie Dienstkontingente hinzufügen oder entfernen. Sie können auch die Werte für einstellbare Kontingente erhöhen. Sobald Sie die Vorlage anpassen, werden diese Service-Kontingentwerte für neue Konten angefordert. Durch das Aktualisieren einer Anforderungsvorlage werden keine Kontingentwerte für vorhandene Konten aktualisiert.

So aktivieren Sie die Vorlage

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie im Navigationsbereich und dann aus.Kontingent-Anforderungsvorlageaus. Wenn das SymbolKontingent-AnforderungsvorlageIst nicht sichtbar, wählen Sie aus.Organisationum es zu öffnen.
3. In derZuordnung von VorlagenWählen Sie die Option aus.Aktivieren vonaus.

So fügen Sie Ihrer Anforderungsvorlage ein Kontingent hinzu

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.

2. Wählen Sie im Navigationsbereich und dann aus.Kontingent-Anforderungsvorlageaus. Wenn das SymbolKontingent-AnforderungsvorlageIst nicht sichtbar, wählen Sie aus.Organisationum es zu öffnen.
3. In derKontingenteWählen Sie die Option aus.Kontingent hinzufügenaus.

> **Note**
>
> Sie addieren Ihrer Anfragevorlage bis zu 10 Kontingente.

4. Auf derKontingent hinzufügen-Seite und wählen Sie eineRegion,-Service,Quota, undGewünschter KontingentwertUnd dann wählen Sie aus.Addaus.

So entfernen Sie ein Kontingent aus Ihrer Anforderungsvorlage

Sie können Service-Kontingentanfragen aus der Vorlage entfernen, unabhängig davon, ob die Vorlage einer Organisation zugeordnet ist. Wenn Sie die maximale Anzahl von Servicekontingentanfragen erreichen, müssen Sie möglicherweise einige Kontingente aus Ihrer Anforderungsvorlage entfernen.

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie im Navigationsbereich und dann aus.Kontingent-Anforderungsvorlageaus. Wenn das SymbolKontingent-AnforderungsvorlageIst nicht sichtbar, wählen Sie aus.Organisationum es zu öffnen.
3. In derKontingenteWählen Sie das Optionsfeld für das Kontingent aus, das Sie entfernen möchten.
4. Wählen Sie Remove (Entfernen) aus.

So deaktivieren Sie die Vorlagenzuordnung

Wenn Sie das Kontingent deaktivieren, erhalten neue KontenAWSStandardkontingentwerte für alle Kontingente. Durch das Deaktivieren der Vorlagenzuordnung aus der Organisation werden die Service-Kontingentanfragen nicht aus der Vorlage gelöscht. Sie können die Service-Kontingente in der Vorlage weiterhin bearbeiten.

1. Melden Sie sich beim anAWS Management ConsoleUnd öffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.

2. Wählen Sie im Navigationsbereich und dann aus.Kontingent-Anforderungsvorlageaus. Wenn das SymbolKontingent-AnforderungsvorlageIst nicht sichtbar, wählen Sie aus.Organisationum es zu öffnen.
3. In derZuordnung von VorlagenWählen Sie die Option aus.Deaktivieren vonaus.

Servicekontingente für Sicherheit in

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

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

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

Diese Dokumentation erläuterte, wie das Modell der geteilten Verantwortung bei der Verwendung von Service Quotas zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Servicekontingente zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfiguriert werden. Sie erfahren außerdem, wie man andere benutztAWS-Servicesdie Ihnen helfen, Ihre Service Quotas -Ressourcen zu überwachen und zu schützen.

Inhalt

Datenschutz in Service Quotas

DieAWS Modell der übertragung der übergilt für den Datenschutz in Service Quotas. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt enthält die Sicherheitskonfigurations- und Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services. 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 die GDPR im Blog zur AWS-Sicherheit.

Wir empfehlen aus Gründen des Datenschutzes, dass Sie AWS-Konto-Anmeldeinformationen schützen und die Benutzerkonten jeweils mit AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Factor Authentication (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über 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 wie z. B. im Feld Name keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Service Quotas oder anderen arbeitenAWSDienste, die die Konsole verwenden, API,AWS CLI, oderAWSSDKs. Alle Daten, die Sie in Tags (Markierungen) oder Freiformfelder 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, Sie keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Protokollieren und Überwachen von Service Quotas

Übersicht

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Performance von Service Quotas und Ihren anderenAWS-Lösungen.AWSbietet die folgenden Überwachungstools zur Beobachtung von Service-Kontingenten, zur Meldung, wenn etwas schiefgeht, und zur automatischen Erggleiten von Gegenmaßnahmen bei Bedarf:

- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Konto-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.
- Amazon CloudWatch überwacht Ihre AWS-Ressourcen und die in AWS ausgeführten Anwendungen in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise CloudWatch Sie erfassen mit die CPU-Auslastung oder andere Metriken Ihrer Amazon EC2 EC2-Instances und starten Sie bei Bedarf automatisch neue Instances. Weitere Informationen finden Sie im .Amazon CloudWatch -Benutzerhandbuchaus.

Protokollieren von Servicekontingent-API-Aufrufen mithilfeAWS CloudTrail

Service Quotas sind integriert inAWS CloudTrail, ein Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS-Servicein Service Quotas. CloudTrail erfasst alle API-Aufrufe für Service Quotas Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Servicekontingente-Konsole und Codeaufrufe der Service Quotas API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Service Quotas. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in CloudTrail -Konsole inEreignisverlauf desaus. Mit den von CloudTrail erfassten Informationen können Sie die an Servicekontingente

gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

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

Service Quotas in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Konto für Sie aktiviert. Erfolgen Aktivitäten im Servicekontingente, werden diese als CloudTrail Event zusammen mit anderenAWS-ServiceEreignisse inEreignisverlauf desaus. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unterAnzeigen von Ereignissen mit CloudTrail Ereignisverlauf desaus.

Für eine kontinuierliche Aufzeichnung von Ereignissen inAWS-KontoErstellen Sie einen Trail, einschließlich Ereignissen für Servicekontingente. EINWanderwegaktiviert CloudTrail um Protokolldateien an einen Amazon S3 S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere konfigurierenAWS-Servicesum die in erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren CloudTrail protokolliert. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen CloudTrail Protokolldateien aus mehreren RegionenundEmpfangen CloudTrail Protokolldateien von mehreren Konten

Alle Servicekontingent-Aktionen werden von protokolliert CloudTrail und sind imAPI-Servicekontingenteaus. Zum Beispiel werden durch AufrufeGetServiceQuota,RequestServiceQuotaIncreaseundListAWSDefaultServiceQuotasAkt generieren Einträge im CloudTrail -Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Grundlegendes Service Quotas -Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket übermittelt werden. CloudTrail -Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne 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 Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der den`RequestQuotaIncrease`Aktion

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA123456789012Example",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "ASIA123456789012Example",
        "userName": " admin",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-01-24T16:57:04Z",
                "mfaAuthenticated": "true"
            }
        }
    },
    "eventTime": "2022-01-24T17:00:15Z",
    "eventSource": "servicequotas.amazonaws.com",
    "eventName": "RequestServiceQuotaIncrease",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.21.16.1",
    "userAgent": "aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.147-83.259.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
    "requestParameters": {
        "serviceCode": "ec2",
        "quotaCode": "L-CEED54BB",
        "desiredValue": 10
    },
    "responseElements": {
        "requestedQuota": {
            "id": "cd3ad3d9-2776-4ef1-a904-4c229d1642ee",
            "serviceCode": "ec2",
            "serviceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
            "quotaCode": "L-CEED54BB",
            "quotaName": "EC2-Classic Elastic IPs",
            "desiredValue": 10,
            "status": "PENDING",
            "created": "Jan 24, 2022 5:00:15 PM",
            "requester": "{\"accountId\":\"111122223333\",\"callerArn\":
\"arn:aws:iam::111122223333:user/admin\"}",
            "quotaArn": "arn:aws:servicequotas:us-east-1:111122223333:ec2/L-CEED54BB",
            "globalQuota": false,
            "unit": "None"
        }
    },
    "requestID": "3d3f5cdc-af30-4121-b69a-84b2f5c33be5",
    "eventID": "0cb51588-e460-4e00-bc48-a9d4820cad83",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Dieses Beispiel zeigt, dass der Benutzer, Admin, am 24. Januar 2022 eine Anfrage nach zusätzlichen Amazon Elastic Compute Cloud Elastic IP-Adressen generiert hat. Die beantragte Erhöhung betrug 10, was eine Erhöhung von 5 gegenüber der Ausfallquote von 5.

Das Folgende ist ein Beispiel für eine genehmigte Quotenerhöhung der Service Quotas:


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "servicequotas.amazonaws.com"
    },
    "eventTime": "2022-01-24T17:02:17Z",
    "eventSource": "servicequotas.amazonaws.com",
    "eventName": "UpdateServiceQuotaIncreaseRequestStatus",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "servicequotas.amazonaws.com",
    "userAgent": "servicequotas.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "e331b0a0-9395-4895-aeba-73cbab9ebcb0",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "requestId": "cdc5f1f78739459e6642407bb2bZKO8GKUM",
        "newStatus": "CASE_CLOSED",
        "createTime": "2022-01-24T17:00:15.363Z",
        "newQuotaValue": "10.0",
        "serviceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
        "quotaName": "EC2-Classic Elastic IPs",
        "unit": "None"
    },
    "eventCategory": "Management"
}
```


Aus`serviceEventDetails`können Sie feststellen, dassAWS Supportgenehmigte den Antrag auf eine Quotenerhöhung auf 10 Elastic IP-Adressen und schloss die Anfrage. Die`newQuotaValue`zeigt 10 als neues Kontingent an.

Service Quotas und Amazon CloudWatch Alarme

Sie können Amazon erstellen CloudWatch Alarme, um Sie zu benachrichtigen, wenn Sie sich in der Nähe eines Quotenwert-Schwellenwerts befinden. Wenn Sie einen Alarm einstellen, können Sie warnen, wenn Sie eine Erhöhung des Kontingents beantragen müssen.

Erstellen eines CloudWatch -Alarm für ein Kontingent

1. Melden Sie sich beim anAWS Management ConsoleÖffnen Sie die Service Quotas Quotas-Konsole unterhttps://console.aws.amazon.com/servicequotas/homeaus.
2. Wählen Sie im Navigationsbereich ausAWSDienstleistungenWählen Sie dann einen Service aus.
3. Wählen Sie ein Kontingent aus, das unterstützt CloudWatch -Alarme.

   Wenn Sie das Kontingent aktiv verwenden, wird die Auslastung unter der Kontingentbeschreibung angezeigt. Der Abschnitt CloudWatch-Alarme erscheint unten auf der Seite.
4. In :Amazon CloudWatch Alarme, wählenGeben Sie einen Namen für den Benutzer ein und klicken Sie dann aufaus.
5. FürAlarmschwellenwert, wählen Sie einen Schwellenwert.
6. Geben Sie für Alarmname einen Namen für den Alarm ein. Dieser Name muss innerhalb derAWS-Kontoaus.
7. Wählen Sie Create (Erstellen) aus.
8. So fügen Sie eine Benachrichtigung hinzu: CloudWatch Alarm, sieheErstellen einer CloudWatch -Alarm basierend auf einem CloudWatch metrischimAmazon CloudWatch - Benutzerhandbuchaus.

Löschen eines CloudWatch Alarm

1. Wählen Sie das Service-Kontingent mit dem Alarm aus.
2. Wählen Sie den Alarm aus.
3. Wählen Sie Delete (Löschen).

Identitäts- und Zugriffsverwaltung für Service Quotas

AWS verwendet Sicherheitsanmeldeinformationen, um Sie zu identifizieren und Ihnen Zugriff auf Ihre AWS-Ressourcen zu gewähren. Sie können Funktionen vonAWS Identity and Access Management(IAM) um anderen Benutzern, Diensten und Anwendungen die Nutzung IhresAWSRessourcen vollständig oder in begrenzter Weise. Sie können dies tun, ohne Ihre Sicherheitsanmeldeinformationen zu teilen.

IAM-Benutzer sind standardmäßig nicht berechtigt, AWS-Ressourcen zu erstellen, anzuzeigen oder zu ändern. Um einem IAM-Benutzer den Zugriff auf Ressourcen wie einen Load Balancer und das Ausführen von Aufgaben zu ermöglichen, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine IAM-Richtlinie, die dem IAM-Benutzer die Berechtigung zur Nutzung der jeweiligen Ressourcen und API-Aktionen erteilt, die er benötigt.
2. Fügen Sie die Richtlinie dem IAM-Benutzer oder der Gruppe an, zu der der IAM-Benutzer gehört.

Wenn Sie einem Benutzer oder einer Benutzergruppe eine Richtlinie zuordnen, wird den Benutzern die Ausführung der angegebenen Aufgaben für die angegebenen Ressourcen gestattet oder verweigert.

Sie können beispielsweise IAM verwenden, um Benutzer und Gruppen unterAWS-Kontoaus. Ein IAM-Benutzer kann eine Person, ein System oder eine Anwendung sein. Anschließend gewähren Sie den Benutzern und Gruppen Berechtigungen, um bestimmte Aktionen für die angegebenen Ressourcen mithilfe einer IAM-Richtlinie durchzuführen.

Erteilen Sie Berechtigungen mithilfe von IAM-Richtlinien

Wenn Sie einem Benutzer oder einer Benutzergruppe eine Richtlinie zuordnen, wird den Benutzern die Ausführung der angegebenen Aufgaben für die angegebenen Ressourcen gestattet oder verweigert.

Eine IAM-Richtlinie ist ein JSON-Dokument, das eine oder mehrere Anweisungen enthält. Jedes Statement ist dem folgenden Beispiel entsprechend strukturiert.

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect": "effect",
    "Action": "action",
    "Resource": "resource-arn",
    "Condition": {
      "condition": {
        "key":"value"
      }
    }
  }]
}
```

- **`Effect`**— Der Wert für**`effect`**kann eines der Folgenden sein`Allow`oder`Deny`aus. IAM-Benutzer verfügen standardmäßig nicht über die Berechtigung zur Verwendung von Ressourcen und API-Aktionen. Daher werden alle Anfragen abgelehnt. Dieser Standardwert kann durch eine explizite Zugriffserlaubnis überschrieben werden. Eine explizite Zugriffsverweigerung überschreibt jedwede Zugriffserlaubnis.
- **`Action`**— Der Wert für**`action`**ist die API-Aktion, für die Sie Berechtigungen erteilen oder verweigern. Weitere Informationen über das Angeben`Action`finden Sie unterAPI-Aktionen für Service Quotasaus.
- `Resource`: die Ressource, die von der Aktion betroffen ist. Mit einigen -API-Aktionen für Servicekontingente können Sie die erteilten oder verweigerten Berechtigungen auf ein bestimmtes Kontingent beschränken. Geben Sie dazu den Amazon Resource Name (ARN) in diesem Statement an. Ansonsten können Sie das Platzhalterzeichen (*) um alle Service-Kontingentsressourcen anzugeben. Weitere Informationen finden Sie unter Ressourcen Service Quotas Servicekontingente.
- `Condition`: Sie können optional Bedingungen verwenden, um zu steuern, wann die Richtlinie wirksam ist. Weitere Informationen finden Sie unter Bedingungsschlüssel für -Service-Quotas.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch.

API-Aktionen für Service Quotas

In der`Action`In Ihrer IAM-Richtlinienanweisung können Sie eine beliebige API-Aktion angeben, die Service Quotas bietet. Dem Namen der Aktion muss wie im folgenden Beispiel die Zeichenfolge `servicequotas:` in Kleinbuchstaben vorangestellt werden.

```
"Action": "servicequotas:GetServiceQuota"
```

Wenn Sie mehrere Aktionen in einer einzigen Anweisung angeben möchten, setzen Sie sie in eckige Klammern und trennen Sie sie wie im folgenden Beispiel dargestellt durch Kommas.

```
"Action": [
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota"
]
```

Sie können auch mehrere Aktionen mithilfe des Platzhalters (*) enthalten. Das folgende Beispiel gibt alle API-Aktionsnamen für Service Quotas an, die mit beginnen`Get`aus.

```
"Action": "servicequotas:Get*"
```

Um alle -API-Aktionen für Service Quotas anzugeben, verwenden Sie das Platzhalterzeichen (*), wie im folgenden Beispiel gezeigt.

```
"Action": "servicequotas:*"
```

Eine Liste der API-Aktionen für Service Quotas finden Sie unterAktionen von Servicekontingenteaus.

Ressourcen Service Quotas Servicekontingente

Berechtigungen auf Ressourcenebene bedeutet, dass Sie angeben können, für welche Ressourcen die Benutzer Aktionen ausführen dürfen. Bei API-Aktionen, die Berechtigungen auf Ressourcenebene unterstützen, können Sie steuern, welche Ressourcen Benutzer mit der Aktion verwenden dürfen. Um eine Ressource in einer Richtlinienanweisung anzugeben, müssen Sie dessen Amazon-Ressourcennamen (ARN) verwenden.

Der ARN für ein Kontingent hat das im folgenden Beispiel gezeigte Format.

```
arn:aws:servicequotas:region-code:account-id:service-code/quota-code
```

Bei API-Aktionen, die Berechtigungen auf Ressourcenebene nicht unterstützen, müssen Sie die Ressourcenanweisung wie im folgenden Beispiel dargestellt angeben.

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

Berechtigungen auf Ressourcenebene für Service Quotas

Die folgenden Service Quotas unterstützen keine Berechtigungen auf Ressourcenebene:

- PutServiceQuotaIncreaseRequestintoTemplate
- RequestServiceQuotaIncrease

Weitere Informationen finden Sie unterVon Service Quotas definierte AktionenimService Authorization-Referenzaus.

Bedingungsschlüssel für -Service-Quotas

Beim Erstellen einer Richtlinie können Sie die Bedingungen angeben, die steuern, wann die Richtlinie wirksam wird. Jede Bedingung enthält ein oder mehrere Schlüssel-Wert-Paare. Es gibt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel.

Die`servicequotas:service`Schlüssel ist spezifisch für Service Quotas. Die folgenden API-Aktionen für Service Quotas unterstützen diesen Schlüssel:

- PutServiceQuotaIncreaseRequestintoTemplate
- RequestServiceQuotaIncrease

Weitere Informationen über diese Bedingungsschlüssel finden Sie unterAWSGlobale - Bedingungskontextschlüsselim IAM User Guideaus.

VordefiniertAWSverwaltete Richtlinien für Service Quotas

Die von AWS erstellten verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für häufige Anwendungsfälle. Sie können diese Richtlinien Ihren IAM-Benutzern entsprechend dem benötigten Zugriff auf Servicekontingente hinzufügen:

- `ServiceQuotasFullAccess`— Gewährt vollen Zugriff, der für die Verwendung von Service-Quotas-Funktionen erforderlich ist.
- `ServiceQuotasReadOnlyAccess`: gewährt Lesezugriff auf Service Quotas.

Compliance-Validierung für Service Quotas

Externe Auditoren bewerten im Rahmen verschiedener -Dienstleistungen die Sicherheit und Compliance vonAWSCompliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Für eine ListeAWS-Servicesin den Geltungsbereich bestimmter Compliance-Programme sieheAWS-Dienstleistungen in Scope nach Compliance-Programmaus. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

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

Ihre Compliance-Verantwortung bei Verwendung von Service Quotas hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab.AWSstellt folgende Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit bei Service Quotas

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

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

Infrastruktursicherheit in Service Quotas

Als gemanagtAWS-Service, Service Quotas sind durch dieAWSglobale Verfahren zur Gewährleistung der Netzwerksicherheit, die in derAmazon Web Services: Übersicht über die SicherheitsprozesseWhitepaper.

Du benutztAWSveröffentlichte API-Aufrufe, um über das Netzwerk auf Service Quotas zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder höher. Clients müssen außerdem Cipher Suites mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen 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.

Service Quotas für Servicekontingente

In den folgenden Tabellen werden die Standardmaximalwerte für Service-Kontingentsressourcen für IhreAWS-Kontoaus. Alle diese Kontingentwerte sind proAWS-Region, sofern nicht anders angegeben. Sie können diese Kontingentwerte nicht anpassen.

Erhöhte Anforderungen

Quota	Standard
Aktive Anforderungen zur Erhöhung des Servicekontingents pro -Konto	20
Aktive Anforderungen zur Erhöhung des Servicekontingents pro Region	2
Aktive Anforderungen zur Erhöhung des Servicekontingents pro Kontingent	1

API-Anforderungen

Quota	Standard
`GetAWSDefaultServiceQuota` Anforderungen pro Sekunde	5
Zusätzliches`GetAWSDefaultServiceQuota` Anfragen pro Sekunde in einem Burst gesendet	5
`GetRequestedServiceQuotaChange` Anforderungen pro Sekunde	5
Zusätzliches`GetRequestedServiceQuotaChange` Anfragen pro Sekunde in einem Burst gesendet	5
`GetServiceQuota` Anforderungen pro Sekunde	5
Zusätzliches`GetServiceQuota` Anfragen pro Sekunde in einem Burst gesendet	5
`ListAWSDefaultServiceQuotas` Anforderungen pro Sekunde	10

Quota	Standard
ZusätzlichesListAWSDefaultServiceQuotas Anfragen pro Sekunde in einem Burst gesendet	10
ListRequestedServiceQuotaChangeHistory Anforderungen pro Sekunde	5
ZusätzlichesListRequestedServiceQuotaChangeHistory Anfragen pro Sekunde in einem Burst gesendet	5
ListRequestedServiceQuotaChangeHistoryByQuota Anforderungen pro Sekunde	5
ZusätzlichesListRequestedServiceQuotaChangeHistoryByQuota Anfragen pro Sekunde in einem Burst gesendet	5
ListServiceQuotas Anforderungen pro Sekunde	10
ZusätzlichesListServiceQuotas Anfragen pro Sekunde in einem Burst gesendet	10
ListServices Anforderungen pro Sekunde	10
ZusätzlichesListServices Anfragen pro Sekunde in einem Burst gesendet	10
ListTagsForResource Anforderungen pro Sekunde	10
ListTagsForResource Anfragen pro Sekunde in einem Burst gesendet	10
RequestServiceQuotaIncrease Anforderungen pro Sekunde	3
ZusätzlichesRequestServiceQuotaIncrease Anfragen pro Sekunde in einem Burst gesendet	3
TagResource Anforderungen pro Sekunde	10
TagResource Anfragen pro Sekunde in einem Burst gesendet	10

Quota	Standard
`UntagResource` Anforderungen pro Sekunde	10
`UntagResource` Anfragen pro Sekunde in einem Burst gesendet	10

Kontingentanforderungsvorlage API-Anforderungsraten

Quota	Standard
`AssociateQuotaTemplate` Anforderungen pro Sekunde	1
Zusätzliches`AssociateQuotaTemplate` Anfragen pro Sekunde in einem Burst gesendet	1
`DeleteServiceQuotaIncreaseRequestFromTemplate` Anforderungen pro Sekunde	2
Zusätzliches`DeleteServiceQuotaIncreaseRequestFromTemplate` Anfragen pro Sekunde in einem Burst gesendet	1
`DisassociateQuotaTemplate` Anforderungen pro Sekunde	1
Zusätzliches`DisassociateQuotaTemplate` Anfragen pro Sekunde in einem Burst gesendet	1
`GetAssociationForQuotaTemplate` Anforderungen pro Sekunde	2
Zusätzliches`GetAssociationForQuotaTemplate` Anfragen pro Sekunde in einem Burst gesendet	2
`GetServiceQuotaIncreaseRequestFromTemplate` Anforderungen pro Sekunde	2
Zusätzliches`GetServiceQuotaIncreaseRequestFromTemplate` Anfragen pro Sekunde in einem Burst gesendet	1
`ListServiceQuotaIncreaseRequestsInTemplate` Anforderungen pro Sekunde	2

Quota	Standard
Zusätzliches`ListServiceQuotaIncreaseRequestsInTemplate` Anfragen pro Sekunde in einem Burst gesendet	1
`PutServiceQuotaIncreaseRequestIntoTemplate` Anforderungen pro Sekunde	1
Zusätzliches`PutServiceQuotaIncreaseRequestIntoTemplate` pro Sekunde in einem Burst gesendet	1

Dokumentverlauf für Servicekontingente

In der folgenden Tabelle werden wichtige Änderungen an der Dokumentation seit der letzten Veröffentlichung von Service Quotas beschrieben.

Änderung	Beschreibung	Datum
Veröffentlichter Leitfaden auf GitHub	Sie können jetzt Aktualisierungen des Service-Kontingenten-Benutzerhandbuchs anfordern, indem Sie Pull-Anfragen auf unserer GitHub-Repository beihttps://github.com/awsdocs/service-quotas-user-guideaus.	23. März 2021
Service Quotas von Ressourcen markieren	Sie können jetzt Tags an angewendete Kontingente anhängen und Richtlinien schreiben, um den Zugriff auf diese Kontingente zu steuern.	21. Dezember 2020
Erstversion	In dieser Version werden Servicekontingente eingeführt.	24. Juni 2019

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.