aws

Benutzerhandbuch

Application Cost Profiler

Application Cost Profiler: Benutzerhandbuch

Table of Contents

AWS Application Cost Profiler wird bis zum 30. September 2024 eingestellt und akzeptiert keine Neukunden mehr.

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 ?AWSApplication Cost Profiler?

AWSApplication Cost Profiler hilft Ihnen, IhreAWSAbrechnung und Kosten durch die Mieter Ihres Dienstes. EINMieterkann ein Benutzer, eine Benutzergruppe oder ein Projekt sein.

EINRessourceist eine Entität, mit der Benutzer arbeiten könnenAWSwie eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Stellen Sie sicher, dass Sie Ihre Ressourcennutzung durch den von Ihnen gewählten Mandanten identifizieren können.

TypischeAWSDie Ressourcennutzung umfasst Shared Services, die mehrere Mandanten in Ihrem Unternehmen unterstützen. Bestimmte Ressourcen verwenden zeitbasierte Dimensionen. Um Kosten- und Abrechnungsinformationen nach dem Mandanten und nicht nach stündlicher Nutzung für die Ressource zu erhalten, können Sie Ihre Ressourcen in Application Cost Profiler integrieren. Mit diesem granularen Ansatz können Sie verstehen, wieAWSRessourcen werden in einer gemeinsamen Softwarelösung verbraucht.

Die folgenden Ressourcen, die entweder zeitbasierte Dimensionen oder stündliche Nutzung verwenden können, sind für Application Cost Profiler aktiviert:

- Amazon EC2 EC2-Instanzen (nur bei Bedarf und Spot-Instances)
- Amazon-Simple-Queue-Service-(Amazon-SQS)-Warteschlangen
- Amazon Simple Notification Service (Amazon SNS)-Themen
- Amazon DynamoDB liest und schreibt

> **Note**
>
> Im Gegensatz zu den meisten Ressourcen wird die Nutzung von Amazon SQS, Amazon SNS und DynamoDB nicht nach der Zeit berechnet. In ihrem Fall wird die Verwendung während einer Stunde (z. B. eine Reihe von Lese- und Schreibvorgängen in DynamoDB) nach dem Prozentsatz der Stunde kategorisiert, die Sie verschiedenen Mandanten zuweisen, unabhängig davon, wann die Lese- oder Schreibvorgänge während der Stunde stattfanden.

Sie integrieren Ihre Dienste in den Application Cost Profiler in drei Schritten:

1. Aktivieren und konfigurieren Sie einen Bericht— Dieser Schritt definiert, wie Ihre endgültige Ausgabe aussehen soll.

2. Senden Sie die Nutzungsdaten des Mandanten an Application Cost Profiler— Dieser Schritt erfordert Code in Ihrem Service, um Nutzungsdaten zu erstellen, die Mandanten mit der Zeit verknüpfen, zu der sie Ihre Ressourcen verwenden, und diese Nutzungsdaten dann an Application Cost Profiler zu senden.
3. Abrufen von Berichten— Application Cost Profiler stellt Berichte mit der Trittfrequenz bereit, die Sie in Ihrer Berichtskonfiguration angegeben haben. Die Berichte zeigen die Kosten, die mit der Nutzung jedes Mieters verbunden sind, und geben Ihnen einen detaillierten Überblick über Ihre Abrechnung.

Weitere Informationen zu diesen Schritten finden Sie unterErste Schritteaus.

Erste Schritte mit Application Cost Profiler

AWS Application Cost Profiler hilft Ihnen dabei, Kosteninformationen über Ihre AWS Ressourcen zu erhalten, indem die Ressourcennutzung nach Mandanten und nicht für die gesamte Ressource gemeldet wird. Ein Mandant kann ein Benutzer, eine Benutzergruppe oder ein Projekt sein. Stellen Sie sicher, dass Sie Ihre Ressourcennutzung anhand des von Ihnen ausgewählten Mandanten identifizieren können. Um Kostenberichte zur Mandantennutzung zu erhalten, konfigurieren Sie einen Bericht und senden Nutzungsdaten an Application Cost Profiler. In diesem Abschnitt werden die Voraussetzungen beschrieben, die Sie erfüllen müssen, bevor Sie Application Cost Profiler verwenden können.

Themen

Melden Sie sich an für eine AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt von der Art des Benutzers ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		• Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Spezifische Voraussetzungen für Application Cost Profiler

Bevor Sie mit Application Cost Profiler beginnen können, müssen Sie die folgenden Voraussetzungen erfüllen:

- Cost Explorer aktivieren

Aktivieren Sie es AWS Cost Explorer für Ihr AWS Konto. Die Einrichtung eines Kontos bei Cost Explorer kann bis zu 24 Stunden dauern. Sie müssen das Cost Explorer Explorer-Setup abschließen, bevor Application Cost Profiler Ihre täglichen und monatlichen Berichte erstellen kann.

Weitere Informationen finden Sie im AWS Billing and Cost Management Benutzerhandbuch unter Cost Explorer aktivieren.

- S3-Buckets erstellen

  Erstellen Sie mindestens zwei Amazon Simple Storage Service (Amazon S3) -Buckets. Application Cost Profiler verwendet einen S3-Bucket, um Ihnen Berichte zur Verfügung zu stellen. Sie verwenden den anderen S3-Bucket, um Nutzungsdaten in Application Cost Profiler hochzuladen. In der Regel benötigen Sie nur einen S3-Bucket, um Nutzungsdaten hochzuladen. Möglicherweise möchten Sie jedoch mehr als einen S3-Bucket haben, sodass Sie die Nutzung für verschiedene Dienste in separaten S3-Buckets mit unterschiedlichen Berechtigungen verwalten können, falls dies zu Ihrer Sicherheit erforderlich ist. Sie müssen Application Cost Profiler-Berechtigungen für diese S3-Buckets erteilen.

  Weitere Informationen zur Einrichtung der Amazon S3 S3-Buckets für Application Cost Profiler finden Sie unter. Einrichten von Amazon S3 Buckets für Application Cost Profiler

- Tags aktivieren

  Um die Nutzung nach Tag und nicht nach Ressource zu melden, müssen Sie diese Tags in der AWS Billing and Cost Management Konsole aktivieren.

  Weitere Informationen zur Aktivierung AWS generierter Tags finden Sie unter Aktivierung der AWS-Generated Cost Allocation Tags im AWS Billing and Cost Management Benutzerhandbuch. Weitere Informationen zur Aktivierung benutzerdefinierter Tags finden Sie unter Aktivierung benutzerdefinierter Kostenverrechnungs-Tags im AWS Billing and Cost Management Benutzerhandbuch.

Nächste Schritte

Nachdem Sie diese Voraussetzungen erfüllt haben, können Sie:

- Konfigurieren Sie Ihren Bericht und senden Sie Nutzungsdaten an Application Cost Profiler. Weitere Informationen finden Sie unter Bericht erstellen.

- Rufen Sie Ihre generierten Berichte ab und analysieren Sie sie. Weitere Informationen finden Sie unter Verwenden von Application Cost Profiler -Berichten.

Einrichten von Amazon S3 Buckets für Application Cost Profiler

So senden Sie Nutzungsdaten an und empfangen Berichte vonAWSIn Ihrem Application Cost Profiler müssen Sie mindestens einen Amazon Simple Storage Service (Amazon S3) -Bucket in IhremAWS-Kontoum Daten und einen S3-Bucket zu speichern, um Ihre Berichte zu erhalten.

> **Note**
>
> Für Benutzer vonAWS Organizationskönnen sich die Amazon S3 S3-Buckets entweder im Verwaltungskonto oder in einzelnen Mitgliedskonten befinden. Die Daten in S3-Buckets, die dem Verwaltungskonto gehören, können verwendet werden, um Berichte für die gesamte Organisation zu erstellen. In einzelnen Mitgliedskonten können die Daten in den S3-Buckets nur verwendet werden, um Berichte für dieses Mitgliedskonto zu erstellen.

Die S3-Buckets, die Sie erstellen, gehören demAWS-Kontoin dem du sie erschaffst. Die S3-Buckets werden zu Amazon S3 S3-Standardtarifen abgerechnet. Weitere Informationen zum Erstellen eines Amazon S3 S3-Buckets finden Sie unterErstellen eines BucketsimBenutzerhandbuch für Amazon Simple Storage Serviceaus.

Damit Application Cost Profiler die S3-Buckets verwenden kann, müssen Sie den Buckets eine Richtlinie anfügen, die Application Cost Profiler Berechtigungen zum Lesen und/oder Schreiben in den Bucket gewährt. Wenn Sie die Richtlinie ändern, nachdem Ihre Berichte eingerichtet wurden, können Sie verhindern, dass Application Cost Profiler Ihre Nutzungsdaten lesen oder Ihre Berichte liefern kann.

Die folgenden Themen zeigen, wie Sie Berechtigungen für Ihre Amazon S3 S3-Buckets einrichten, nachdem Sie sie erstellt haben. Zusätzlich zur Möglichkeit, Objekte zu lesen und zu schreiben, muss Application Cost Profiler auch Zugriff auf dieAWS Key Management Service(AWS KMS) Schlüssel für jeden Bucket.

Themen

- Application Cost Profiler Zugriff auf Ihren S3-Bucket für die Berichtszustellung gewähren
- Application Cost Profiler Zugriff auf Ihre Nutzungsdaten geben S3-Bucket

- Application Cost Profiler Zugriff auf SSE-KMS verschlüsselte S3-Buckets gewähren

Application Cost Profiler Zugriff auf Ihren S3-Bucket für die Berichtszustellung gewähren

Der S3-Bucket, den Sie für Application Cost Profiler konfigurieren, um Ihre Berichte zu liefern, muss eine Richtlinie angehängt sein, mit der Application Cost Profiler die Berichtsobjekte erstellen kann. Außerdem muss der S3-Bucket konfiguriert sein, um die Verschlüsselung zu aktivieren.

> **Note**
>
> Wenn Sie Ihren Bucket erstellen, müssen Sie ihn verschlüsseln. Sie können Ihren Bucket mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder durch Ihren eigenen Schlüssel verschlüsseln, der von verwaltet wirdAWS KMS(SSE-KMS). Wenn Sie Ihren Bucket bereits ohne Verschlüsselung erstellt haben, müssen Sie Ihren Bucket bearbeiten, um Verschlüsselung hinzuzufügen.

So geben Sie Application Cost Profiler Zugriff auf Ihren S3-Bucket für die Berichtsauslieferung

1. Rufen Sie aufAmazon S3-Konsoleund melden Sie sich an.
2. SelectBucketsWählen Sie in der linken Navigation und wählen Sie dann Ihren Bucket aus der Liste aus.
3. Wählen Sie das SymbolBerechtigungenTab, dann nebenBucket-Richtlinie, wählenBearbeitenaus.
4. In der--RichtlinieFügen Sie die folgende Richtlinie ein. Ersetzen*<bucket_name>*durch den Namen Ihres -Buckets und*<AWS-Konto>*durch die ID IhresAWS-Kontoaus.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:PutObject*",
```

```
            "s3:GetEncryptionConfiguration"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<AWS-Konto>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS-
Konto>:*"
            }
          }
        }
      ]
    }
```

In dieser Richtlinie geben Sie den Dienstprinzipal der Application Cost Profiler (`application-cost-profiler.amazonaws.com`) Zugriff auf die Bereitstellung von Berichten an den angegebenen Bucket. Sie macht dies in Ihrem Auftrag und fügt einen Header beiAWS-Kontound einen ARN, der für Ihren Berichtsliefer-Bucket spezifisch ist. Um sicherzustellen, dass Application Cost Profiler nur auf Ihren Bucket zugreift, wenn Sie in Ihrem Namen handeln,`Condition`sucht nach diesen Headern.

5. Klicken Sie aufSpeichern Sie die Änderungenum Ihre Richtlinie zu speichern, die an Ihren Bucket angehängt ist.

   Wenn Sie Ihren Bucket mit SSE-S3-Verschlüsselung erstellt haben, sind Sie fertig. Wenn Sie die SSE-KMS-Verschlüsselung verwendet haben, sind die folgenden Schritte erforderlich, um Application Cost Profiler Zugriff auf Ihren Bucket zu gewähren.

6. (Optional) Wählen Sie dieEigenschaftenRufen Sie für Ihren Bucket und unterStandardverschlüsselungWählen Sie den Amazon-Ressourcennamen (ARN) für IhrenAWS KMSkey. Diese Aktion zeigt dieAWS Key Management Servicekonsolen und zeigt Ihren Schlüssel an.

7. (Optional) Fügen Sie die Richtlinie hinzu, um dem Application Cost Profiler Zugriff auf dieAWS KMSkey. Anweisungen zum Hinzufügen dieser Richtlinie finden Sie unterApplication Cost Profiler Zugriff auf SSE-KMS verschlüsselte S3-Buckets gewährenaus.

Application Cost Profiler Zugriff auf Ihre Nutzungsdaten geben S3-Bucket

Der S3-Bucket, den Sie für Application Cost Profiler konfigurieren, aus dem Ihre Nutzungsdaten gelesen werden kann, muss eine Richtlinie angehängt sein, damit Application Cost Profiler die Nutzungsdatenobjekte lesen kann.

> **Note**
>
> Indem Sie Application Cost Profiler Zugriff auf Ihre Nutzungsdaten gewähren, erklären Sie sich damit einverstanden, dass wir solche Nutzungsdatenobjekte vorübergehend in den USA Ost (N. Virginia) kopieren könnenAWS-Regionwährend der Verarbeitung von Berichten. Diese Datenobjekte werden in der Region USA Ost (Nord-Virginia) aufbewahrt, bis die monatliche Berichtsgenerierung abgeschlossen ist.

So gewähren Sie Application Cost Profiler Zugriff auf Ihre Nutzungsdaten S3-Bucket

1. Rufen Sie aufAmazon S3-Konsoleund melden Sie sich an.
2. SelectBucketsWählen Sie in der linken Navigation und wählen Sie dann Ihren Bucket aus der Liste aus.
3. Wählen Sie das SymbolBerechtigungenTab, dann nebenBucket-Richtlinie, wählenBearbeitenaus.
4. In der--RichtlinieFügen Sie die folgende Richtlinie ein. Ersetzen*<bucket-name>*durch den Namen Ihres -Buckets und*<AWS-Konto>*durch die ID IhresAWS-Kontoaus.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:GetObject*"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
```

```
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<AWS-Konto>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS-
Konto>:*"
            }
          }
        }
      ]
    }
```

In dieser Richtlinie geben Sie den Dienstprinzipal der Application Cost Profiler (`application-cost-profiler.amazonaws.com`) Zugriff, um Daten aus dem angegebenen Bucket zu holen. Sie macht dies in Ihrem Auftrag und fügt einen Header beiAWS-Kontound einen ARN, der für Ihren Nutzungs-Bucket spezifisch ist. Um sicherzustellen, dass Application Cost Profiler nur auf Ihren Bucket zugreift, wenn Sie in Ihrem Namen handeln,`Condition`sucht nach diesen Headern.

5. Klicken Sie aufSpeichern Sie die Änderungenum Ihre Richtlinie zu speichern, die an Ihren Bucket angehängt ist.

Wenn dein Bucket mit verschlüsselt istAWS KMSverwaltete Schlüssel, dann müssen Sie Application Cost Profiler Zugriff auf Ihren Bucket gewähren, indem Sie das Verfahren im nächsten Abschnitt befolgen.

Application Cost Profiler Zugriff auf SSE-KMS verschlüsselte S3-Buckets gewähren

Wenn Sie die S3-Buckets, die Sie für Application Cost Profiler konfigurieren (erforderlich für Berichtsbuckets) mit Schlüsseln verschlüsseln, die inAWS KMS(SSE-KMS) müssen Sie Application Cost Profiler auch Berechtigungen erteilen, um sie zu entschlüsseln. Sie tun dies, indem Sie Zugriff auf dieAWS KMS-Schlüssel, die zum Verschlüsseln der Daten verwendet werden.

> **Note**
>
> Wenn Ihr Bucket mit verwalteten Amazon S3 S3-Schlüsseln verschlüsselt ist, müssen Sie diesen Vorgang nicht ausführen.

So gewähren Sie Application Cost Profiler Zugriff aufAWS KMSfür SSE-KMS verschlüsselte S3-Buckets

1. Rufen Sie aufAWS KMSKonsoleund melden Sie sich an.
2. SelectKundenverwaltete SchlüsselWählen Sie in der linken Navigation und in der anschließend angezeigten Liste den Schlüssel aus, der zum Verschlüsseln Ihres Buckets verwendet wird.
3. SelectWechseln Sie zur RichtlinienansichtWählen Sie dannBearbeitenaus.
4. In der--RichtlinieFügen Sie die folgende Richtlinienanweisung ein.

```
  {
    "Effect": "Allow",
    "Principal": {
        "Service": "application-cost-profiler.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<AWS-Konto>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS-
Konto>:*"
            }
  }
```

5. Klicken Sie aufSpeichern Sie die Änderungenum Ihre Richtlinie zu speichern, die an Ihren Schlüssel angehängt ist.
6. Wiederholen Sie dies für jeden Schlüssel, der einen S3-Bucket verschlüsselt, auf den Application Cost Profiler zugreifen muss.

> **Note**
>
> Die Daten werden beim Import in verwaltete Buckets von Application Cost Profiler (die verschlüsselt sind) aus Ihrem S3-Bucket kopiert. Wenn Sie den Zugriff auf die Schlüssel widerrufen, kann Application Cost Profiler keine neuen Objekte aus dem Bucket abrufen. Alle bereits importierten Daten können jedoch weiterhin zum Generieren von Berichten verwendet werden.

Bericht erstellen

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie den Bericht für Sie konfigurierenAWS-Konto und Ihre Nutzungsdaten anAWS Application Cost Profiler senden. In diesem Abschnitt wird beschrieben, wie der Bericht konfiguriert und die Nutzungsdaten an Application Cost Profiler gesendet werden.

Application Cost Profiler Service

Das folgende Verfahren zeigt, wie Sie den Bericht konfigurieren, den Sie anhand Ihres Nutzungsdatums generieren möchten. Sie konfigurieren Details wie die Häufigkeit, mit der der Bericht generiert wird.

> **Note**
>
> Wenn SieAWS-Konto Teil einerAWS Organisation sind, können Sie den Bericht entweder über das Verwaltungskonto oder ein einzelnes Mitgliedskonto konfigurieren. Für einzelne Konten konfigurierte Berichte enthalten nur Daten für dieses Konto. Mit dem Verwaltungskonto konfigurierte Berichte können Daten für die gesamte Organisation enthalten.
> Der für die Berichtsausgabe verwendete Amazon S3-Bucket muss zu dem Konto gehören, das die Berichtskonfiguration erstellt.

So konfigurieren Sie Ihren Application Cost Profiler-Bericht

1. Öffnen Sie einen Webbrowser und melden Sie sich bei der Application Cost Profiler-Konsole an.
2. Wählen Sie Jetzt loslegen, um einen Bericht zu konfigurieren oder zu ändern.
3. Geben Sie einen Berichtsnamen und eine Berichtsbeschreibung für Ihren Bericht ein.
4. Geben Sie den Namen Ihres S3-Buckets in das Feld S3-Bucket-Namen eingeben und das S3-Präfix in das Feld S3-Präfix eingeben ein. Weitere Informationen zum Erstellen von S3-Buckets und zum Erteilen von Application Cost Profiler-Berechtigungen finden Sie unterEinrichten von Amazon S3 Buckets für Application Cost Profiler.
5. Wählen Sie die Optionen aus, die Ihr Bericht haben soll:

   - Zeitintervall — Wählen Sie aus, ob der Bericht täglich oder monatlich oder beides erstellt wird.

- Berichtsausgabeformat — Wählen Sie den Dateityp aus, der in Ihrem Amazon S3-Bucket erstellt werden soll. Wenn Sie CSV wählen, erstellt Application Cost Profiler eine Textdatei mit kommagetrennten Werten mit GZIP-Komprimierung für die Berichte. Wenn Sie Parquet wählen, wird eine Parquet-Datei für die Berichte generiert.

6. Wählen Sie Konfigurieren, um Ihre Berichtskonfiguration zu speichern.

> **Note**
>
> Sie können auch die AWSApplication Cost Profiler-API verwenden, um Berichte zu konfigurieren.

Überprüfen Sie die Berichtseinstellungen, indem Sie Jetzt starten wählen, um die aktuelle Berichtskonfiguration anzuzeigen.

> **Note**
>
> Sie können nur einen einzigen Bericht konfigurieren. Wenn Sie zur Konfigurationsseite zurückkehren, wird Ihr vorhandener Bericht bearbeitet.

Nachdem Sie Ihren Bericht konfiguriert haben, ist die Datenaufnahme aktiviert. Sie können Ihre Dienste in Application Cost Profiler integrieren, um Nutzungsdaten für Ihre Ressourcen bereitzustellen.

Berichterstattung über die Nutzungsdaten Ihrer Mieter aus Ihren Diensten

Nachdem Sie den Bericht konfiguriert haben, können Sie Daten zur Mandantennutzung aus den Ressourcen oder Diensten in Ihrem Konto senden. Sie müssen Application Cost Profiler informieren, wenn Ihre Ressource für einen bestimmten Mandanten verwendet wird. Wenn Ihr Service beispielsweise API-Aufrufe von verschiedenen Mandanten akzeptiert, zeichnen Sie für jeden Mandanten eine Start- und Endzeit auf, wenn Sie einen API-Aufruf von diesem Mandanten starten und beenden. Application Cost Profiler verwendet diese Daten, um Berichte über die Kosten Ihres Dienstes zu erstellen, aufgeschlüsselt nach der für die Arbeit aufgewendeten Zeit für jeden Mandanten.

Um Cost Profiler Service

- Daten zur Ressourcennutzung vorbereiten — Erstellen Sie Tabellen, die beschreiben, wann eine Ressource für einen bestimmten Mandanten verwendet wird.
- Nutzungsdaten hochladen — Laden Sie die Tabellen in einen Amazon S3-Bucket hoch, für den Sie Application Cost Profiler die Zugriffsberechtigung erteilt haben.
- Nutzungsdaten importieren — Rufen Sie den`ImportApplicationUsage` API-Vorgang auf, um Application Cost Profiler mitzuteilen, dass die Daten zur Verarbeitung bereit sind.

In den folgenden Abschnitten wird jeder dieser Schritte ausführlicher beschrieben.

Themen

Schritt 1: Vorbereiten Ihrer Daten zur Ressourcennutzung

Während eine Ressource in Ihrem Service verwendet wird, verfolgen Sie, welcher Mandant sie verwendet. Notieren Sie diese Daten in einer Tabelle, die Sie später für den Import von Application Cost Profiler hochladen können. Jede Zeile in der Tabelle beschreibt eine Ressource, den Mandanten, der die Ressource verwendet, sowie die Start- und Endzeiten dieser Verwendung. Ein Beispiel für eine Ressource ist eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die verwendet wird.

Für diesen Schritt müssen Sie Code in Ihren Service integrieren, um die richtigen Informationen über die Nutzung auszugeben.

Die Felder in einer Tabelle zur Ressourcennutzung werden in der folgenden Tabelle aufgeführt.

Feld	Beschreibung
ApplicationId	Identifiziert die Anwendung oder das Produkt in Ihrem System, das verwendet wird. Definiert den Umfang der Mandantenmetadaten.

Feld	Beschreibung
TenantId	Eine Kennung in Ihrem System für den Mandanten, der die angegebene Ressource verbraucht. Application Cost Profiler aggregiert auf dieser Ebene innerhalb von ApplicationId.
TenantDesc	(Optional) Zusätzliche Daten über den Mieter für Ihre eigene zusätzliche Berichterstattung.
UsageAccountId	Das Konto, in dem die Ressource läuft (wichtig für Konten, die Teil einer Organisation sind).
StartTime	Zeitstempel (in Millisekunden und Mikrosekunden) von Epoch in UTC. Gibt die Startzeit des Zeitraums für die Nutzung durch den angegebenen Mandanten an.
EndTime	Zeitstempel (in Millisekunden und Mikrosekunden) von Epoch in UTC. Gibt die Endzeit des Zeitraums für die Nutzung durch den angegebenen Mandanten an.
ResourceId	Amazon-Ressourcenname (ARN) für die verwendete Ressource.
Name	(Optional) Als Alternative zur Angabe von a können Sie ein Name-Ressourcen-Tag angeben ResourceId, um Kosten einer Gruppe von Ressourcen zuzuordnen (das Feld muss den Wert enthalten, den Sie für das Name-Tag verwenden möchten). Ressourcen-Tags werden im Rahmen Ihres -Kosten- und -Nutzungsberichts aktiviert. Weitere Informationen zu Ressourcen-Tags finden Sie unter Details zu Ressourcen-Tags im Benutzerhandbuch für Kosten- und Nutzungsberichte.

Die Ausgabe muss in einer CSV-Datei (durch Komma getrennte Werte), die eine CSV-Datei (durch Komma getrennte Werte) enthalten, wie im folgenden Beispiel gezeigt.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

Speichern Sie die Daten als Datei mit der Erweiterung .csv (oder .csv.gzip, wenn sie mit Gzip komprimiert wurde). Wenn Sie diese Daten in Application Cost Profiler hochladen, wird jeder Zeitabschnitt dem zugehörigen Mandanten zugewiesen. In diesem Beispiel enthält der Bericht den Zeitabschnitt der Amazon EC2-Instance-Kosten für diesen Mandanten. Nur für Amazon EC2 EC2-Instances werden Segmente, die keinem bestimmten Mandanten zugeordnet sind, einem Mandanten ohne Zuordnung hinzugefügt. Überlappende Zeitscheiben werden mehrfach gezählt. Es liegt in Ihrer Verantwortung, sicherzustellen, dass die Daten in Ihrer Nutzungstabelle korrekt sind.

> **Note**
>
> Ihre Datei muss eine Stunde lang sein. Wenn eine Ressource über mehrere Stunden genutzt wird, beenden Sie die Nutzung zu jeder Stunde und erstellen Sie einen neuen Datensatz in der nächsten Datei, die zur gleichen Zeit beginnt.
> Sie müssen eine einzelne Datei mit den Daten einer ganzen Stunde einreichen. Wenn mehrere Dateien für die Daten derselben Stunde eingereicht werden, berücksichtigt Application Cost Profiler nur die Daten in der neuesten Datei.

Die folgende Tabelle zeigt beispielsweise, wie Application Cost Profiler die Nutzung für drei Mandanten über eine Stunde (3.600.000 Millisekunden) auf der Grundlage der bereitgestellten Zeitfenster berechnet.

Mieter	Bereitgestellte Zeitfenster	Berechneter Prozentsatz der Stundenkosten
Mieter 1	1.200.000 ms	33,34%
Mieter 2	600.000 ms	16,66%
<unattributed>		50,00%

In diesem Beispiel wird Tenant1 ein Drittel der Stunde und Tenant2 ein Sechstel der Stunde zugewiesen. Die verbleibende halbe Stunde (1.800.000 ms) wird keinem der Clients zugeschrieben, was 50% der Stunde entspricht.

Derzeit sind die folgenden Ressourcen für Application Cost Profiler aktiviert:

- Amazon EC2-Instances (nur On-Demand- und Spot-Instances)
- Lambda-Funktionen (Wenn Sie Daten für eine Lambda-Funktion senden, müssen Sie den ARN für unqualifizierte Ressourcen als sendenResourceId.)
- Amazon Elastic Container Service (Amazon ECS) -Instances Service (Amazon ECS)
- Amazon-Simple-Queue-Service-(Amazon-SQS)-Warteschlangen
- Amazon Simple Notification Service (Amazon SNS)-Themen
- Amazon DynamoDB liest und schreibt

> **Note**
>
> Die s-Nutzung von Amazon SQS, Amazon SNS und DynamoDB wird im Gegensatz zu den meisten Ressourcen nicht nach Zeit abgerechnet. In ihrem Fall wird die Nutzung während einer Stunde (z. B. eine Anzahl von Lese- und Schreibvorgängen in DynamoDB) nach dem Prozentsatz der Stunde kategorisiert, den Sie verschiedenen Mandanten zuweisen, unabhängig davon, wann die Lese- oder Schreibvorgänge während der Stunde stattfanden.

Schritt 2: Deine Ressourcennutzung hochladen

Nachdem Sie eine Nutzungsdatei für den Mandanten haben, laden Sie Ihre Datendatei auf Amazon S3 hoch und stellen Sie sicher, dass Application Cost Profiler die Berechtigung hat, darauf zuzugreifen.

Weitere Informationen zum Erstellen eines S3-Buckets finden Sie unterSpezifische Voraussetzungen für Application Cost Profiler.

Sie müssen sicherstellen, dass Application Cost Profiler Zugriff auf Ihren S3-Bucket hat. Dies muss nur einmal pro S3-Bucket durchgeführt werden (Sie können denselben Bucket für das Hochladen mehrerer Nutzungsdateien wiederverwenden). Hinweise zum Gewähren des Zugriffs auf den Bucket finden Sie unterApplication Cost Profiler Zugriff auf Ihre Nutzungsdaten geben S3-Bucket. Wenn der Bucket verschlüsselt ist, finden Sie weitere Informationen unterApplication Cost Profiler Zugriff auf SSE-KMS verschlüsselte S3-Buckets gewähren.

> **Note**
>
> Es ist nicht erforderlich, dass Sie die S3-Buckets verschlüsseln, die Sie für Nutzungsdaten verwenden.

Laden Sie Ihre Daten in stündlichen Abständen als Datei mit der Erweiterung .csv (oder .csv.gzip, falls mit Gzip komprimiert) in den S3-Bucket hoch. Nachdem Sie eine neue Datei hochgeladen haben, müssen Sie Application Cost Profiler darüber informieren, dass Sie sie hochgeladen haben, damit die Datei in Ihren Bericht importiert werden kann.

> **Note**
>
> Indem Sie Application Cost Profiler Zugriff auf Ihre Nutzungsdaten gewähren, erklären Sie sich damit einverstanden, dass wir diese NutzungsdatenobjekteAWS-Region während der Bearbeitung von Berichten vorübergehend in den Osten der USA (Nord-Virginia) kopieren können. Diese Datenobjekte werden in der Region USA Ost (Nord-Virginia) aufbewahrt, bis die monatliche Berichtserstellung abgeschlossen ist.

Schritt 3: Nutzungsdaten in Application Cost Profiler importieren

Nachdem Sie Nutzungsdaten in einen Amazon S3-Bucket hochgeladen haben, auf den Application Cost Profiler Zugriff hat, teilen Sie Application Cost Profiler mit, dass die Daten vorhanden sind, und informieren Sie Application Cost Profiler darüber, dass die Daten vorhanden sind, und dass Sie sie in Ihren Abschlussbericht importieren müssen. Sie tun dies, indem Sie den`ImportApplicationUsage` Vorgang in der Application Cost Profiler API verwenden.

Informationen zurAWS Application Cost Profiler-API, einschließlich des`ImportApplicationUsage` Vorgangs, finden Sie in der AWSApplication Cost Profiler-API-Referenz.

Im folgenden Beispiel wird gezeigt, wie man anruft`ImportApplicationUsage`. Ersetzen Sie den *`Eingabetext in Klammern`* durch die Werte für Ihren S3-Bucket und das hochgeladene Objekt.

```
POST /ImportApplicationUsage HTTP/1.1
Content-type: application/json

{
    "sourceS3Location" : {
        "bucket": "<bucket-name>",
        "key": "<object-key>",
        "region": "<region-id>"
    }
}
```

> **Note**
>
> Der`region` Parameter ist nur erforderlich, wenn sich Ihr Bucket in einem befindetAWS-Region, der standardmäßig deaktiviert ist. Weitere Informationen finden Sie unter Verwalten von AWS-Regionen im Allgemeine AWS-Referenz.

Application Cost Profiler generiert einen neuen Bericht in der Häufigkeit, die Sie bei der Konfiguration Ihres Berichts angefordert haben, und verwendet dabei die Daten, mit denen Sie importiert haben`ImportApplicationUsage`.

Nachdem Sie Ihren Bericht konfiguriert und den Import Ihrer Nutzungsdaten in Application Cost Profiler automatisiert haben, können Sie Ihre generierten Berichte anzeigen. Weitere Informationen zu Berichten finden Sie unterVerwenden von Application Cost Profiler -Berichten.

Verwenden von Application Cost Profiler -Berichten

Nachdem Sie Ihre Nutzungsdaten mit integriert habenAWSApplication Cost Profiler und sendet die Daten stündlich, erstellt Application Cost Profiler automatisch Ihren Bericht.

Berichte werden entweder täglich oder monatlich erstellt, basierend auf der Option, die Sie beimKonfigurieren Ihres Berichtsaus. Berichte werden an den Amazon Simple Storage Service (Amazon S3) -Buckets geliefert, den Sie bei der Konfiguration des Berichts ausgewählt haben.

Tägliche Berichte, die am ersten Tag des Monats generiert wurden, enthalten die Daten des Vormonats.

In einem Application Cost Profiler-Bericht verfügbare Daten

Die Spalten, die in einem Nutzungsbericht erstellt werden, sind in der folgenden Tabelle aufgeführt.

Spaltenname	Beschreibung
PayerAccountId	Die ID des Verwaltungskontos in einer Organisation oder die Konto-ID, wenn das Konto nicht Teil vonAWS Organizationsaus.
UsageAccountId	Die Konto-ID für das Konto mit Nutzung.
LineItemType	Die Art des Datensatzes. Immer `Usage`.
UsageStartTime	Zeitstempel (in Millisekunden) aus Epoche, in UTC. Gibt die Startzeit des Zeitraums für die Nutzung durch den angegebenen Mandanten an.
UsageEndTime	Zeitstempel (in Millisekunden) aus Epoche, in UTC. Gibt die Endzeit des Zeitraums für die Nutzung durch den angegebenen Mandanten an.

Spaltenname	Beschreibung
ApplicationIdentifier	DieApplicationIdangegeben in den Nutzungsdaten, die an Application Cost Profiler gesendet werden.
TenantIdentifier	DieTenanIDangegeben in den Nutzungsdaten, die an Application Cost Profiler gesendet werden. Daten ohne Aufzeichnung in den Nutzungsdaten werden in`unattributed` aus.
TenantBeschreibung	Die`TenantDesc` angegeben in den Nutzungsdaten, die an Application Cost Profiler gesendet werden.
ProductCode	DieAWSProdukt, das in Rechnung gestellt wird (z. B.`AmazonEC2`) enthalten.
UsageType	Die Art der in Rechnung gestellten Nutzung (z. B.`BoxUsage:c5.large`) enthalten.
Operation	Die in Rechnung gestellte Operation (z.`RunInstances`) enthalten.
ResourceId	Die Ressourcen-ID oder der Amazon-Ressourcenname (ARN) für die in Rechnung gestellte -Ressource.

Spaltenname	Beschreibung
ScaleFactor	Wenn eine Ressource beispielsweise eine Stunde lang überlastet ist, sind die gemeldete n Nutzungsdaten 2 Stunden statt 1 Stunde, es wird ein Skalierungsfaktor angewendet, um die Summe dem tatsächlich abgerechneten Betrag entspricht (in diesem Fall 0,5). In dieser Spalte wird der Skalierungsfaktor angegeben , der für die spezifische Ressource für diese Stunde verwendet wird. Der Skalierungsfaktor ist immer größer als Null (0) und kleiner oder gleich 1.
TenantAttributionPercent	Der Prozentsatz der dem angegebenen Mieter zugerechneten Nutzung (zwischen Null (0) und 1).
UsageAmount	Der Nutzungsbetrag, der dem angegebenen Mieter zugeschrieben wird.
CurrencyCode	Die Währung, in der der Kurs und die Kosten enthalten sind (z.USD) enthalten.
Rate	Der Abrechnungssatz für die Nutzung pro Einheit.
TenantCost	Die Gesamtkosten für diese Ressource für den angegebenen Mandanten.
Region	DieAWSRegion der -Ressource.

Spaltenname	Beschreibung
Name	Wenn Sie Ressourcen-Tags für Ihre Ressourcen im Bericht „Kosten und Nutzung“ oder über die Ressourcennutzungsdaten erstellt haben, wird dieNameTag wird hier angezeigt. Weitere Informationen zu Ressourcen-Tags finden Sie unterDetails zu Ressourcen-TagsimBenutzerhandbuch für Kosten- und Nutzungsberichtaus.

Im Folgenden sehen Sie ein Beispiel für den Ausgabebericht für eine -Ressource für zwei Stunden.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,Te
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattr
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
```

In diesem Beispiel ist die erste Stunde`Tenant1`für die Hälfte der Zeit. Eine halbe Stunde bleibt wie`unattributed`aus. In der zweiten Stunde werden alle vier Mieter die volle Stunde zugewiesen. In diesem Fall skaliert der Skalierungsfaktor sie alle um 0,25 und allen wird eine Viertelstunde zugewiesen. Die endgültigen Kosten können Sie im`TenantCost`column.

AWSKontingente und Endpunkte für Application Cost Profiler Service

Das AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden AWS-Service. Wenn nicht anders angegeben, gilt jedes KontingentAWSRegionsspezifisch. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

In der folgenden Tabelle sind die Service-Kontingente pro Konto aufgeführtAWSRegions-Endpunkte für Application Cost Profiler.

Servicekontingente

Ressource	Standardwert	Beschreibung
Ratenrate von`PutReportDefinition` Anfragen	5	Die maximale Anzahl von`PutReportDefinition` 5 Anforderungen pro Sekunde pro Sekunde pro Sekunde pro Sekunde
Ratenrate von`UpdateReportDefinition` Anfragen	5	Die maximale Anzahl von`UpdateReportDefinition` 5 Anforderungen pro Sekunde pro Sekunde pro Sekunde pro Sekunde
Ratenrate von`GetReportDefinition` Anfragen	5	Die maximale Anzahl von`GetReportDefinition` 5 Anforderungen pro Sekunde pro Sekunde pro Sekunde pro Sekunde
Ratenrate von`DeleteReportDefinition` Anfragen	5	Die maximale Anzahl von`DeleteReportDefinition` 5 Anforderungen pro

Ressource	Standardwert	Beschreibung
		Sekunde pro Sekunde pro Sekunde pro Sekunde
Ratenrate von`ListReportDefinitions` Anfragen	5	Die maximale Anzahl von`ListReportDefinitions` 5 Anforderungen pro Sekunde pro Sekunde pro Sekunde pro Sekunde
Ratenrate von`ImportApplicationUsage` Anfragen	5	Die maximale Anzahl von`ImportApplicationUsage` 5 Anforderungen pro Sekunde pro Sekunde pro Sekunde pro Sekunde
Maximale Größe der Nutzungsdatendatei	10 MB	Die maximale Größe einer stündlichen Nutzungsdatendatei.

Service-Endpunkte

Application Cost Profiler Service. Alle API-Aufrufe müssen an den Endpunkt USA Ost (Nord-Virginia) erfolgen.

- US East (N. Virginia) – `application-cost-profiler.us-east-1.amazonaws.com`

Sicherheit inAWSApplication Cost Profiler Service

Die Sicherheit in der Cloud hat AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud 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. Informationen zu den Compliance-Programmen, die für Application Cost Profiler gelten, finden Sie unterAWS-Services in Scope nach Compliance-Programmaus.
- 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 zum Tragen kommtAWSApplication Cost Profiler Service Es zeigt Ihnen, wie Sie Application Cost Profiler konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie man andere benutztAWS-Services, die Ihnen helfen, Ihre Application Cost Profiler -Ressourcen zu überwachen und zu schützen.

Inhalt

Datenschutz in AWS Application Cost Profiler

Das Modell der AWS gemeinsamen Verantwortung und gilt für den Datenschutz in AWS Application Cost Profiler. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Systeme laufen. 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 im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag im AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre 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 eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit 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 FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

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 Application Cost Profiler oder einem anderen Programm AWS-Services über die Konsole arbeiten,, API oder. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, keine Anmeldeinformationen in den aufzunehmen, URL um Ihre Anfrage an diesen Server zu überprüfen.

Verschlüsselung im Ruhezustand

AWS Application Cost Profiler verschlüsselt immer alle im Dienst gespeicherten Daten im Ruhezustand, ohne dass eine zusätzliche Konfiguration erforderlich ist. Diese Verschlüsselung erfolgt automatisch, wenn Sie Application Cost Profiler verwenden.

Für Amazon S3 S3-Buckets, die Sie bereitstellen, müssen Sie den Berichts-Bucket verschlüsseln und können den Nutzungsdaten-Bucket verschlüsseln und Application Cost Profiler Zugriff gewähren. Weitere Informationen finden Sie unter Einrichten von Amazon S3 Buckets für Application Cost Profiler.

Verschlüsselung während der Übertragung

AWS Application Cost Profiler verwendet Transport Layer Security (TLS) und clientseitige Verschlüsselung für die Verschlüsselung bei der Übertragung. Die Kommunikation mit Application Cost Profiler erfolgt immer über das Internet, HTTPS sodass Ihre Daten bei der Übertragung immer verschlüsselt werden. Diese Verschlüsselung ist standardmäßig konfiguriert, wenn Sie Application Cost Profiler verwenden.

Identitäts- und Zugriffsmanagement für AWS Application Cost Profiler

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um die Ressourcen von Application Cost Profiler zu verwenden. IAMist eine AWS-Service , die Sie ohne zusätzliche Kosten verwenden können.

Themen

- Fehlerbehebung bei AWS Application Cost Profiler: Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Application Cost Profiler ausführen.

Dienstbenutzer — Wenn Sie den Application Cost Profiler-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Funktionen von Application Cost Profiler verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Application Cost Profiler nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter. Fehlerbehebung bei AWS Application Cost Profiler: Identität und Zugriff

Dienstadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen von Application Cost Profiler verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Application Cost Profiler. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Application Cost Profiler Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen Application Cost Profiler verwenden IAM kann, finden Sie unterWie funktioniert AWS Application Cost Profiler mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Application Cost Profiler zu verwalten. Beispiele für identitätsbasierte Richtlinien von Application Cost Profiler, die Sie in verwenden können, finden Sie unter. IAM AWS Beispiele für identitätsbasierte Richtlinien von Application Cost Profiler

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 übernehmen. 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 (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-

Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, 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 der 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 IAMBenutzerhandbuch 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) 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 im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen

Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. 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 AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- 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 im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen 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 beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
  - Dienstbezogene Rolle — Eine dienstverknüpfte 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 dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance

ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie unter Wann sollte eine IAM Rolle (anstelle eines Benutzers) erstellt werden? im IAMBenutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern 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 in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, 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. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

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 zur Auswahl zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Dienststeuerungsrichtlinien (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 AWS-Konten Unternehmenseigentümer. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung 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 im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

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 IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie funktioniert AWS Application Cost Profiler mit IAM

Bevor Sie IAM den Zugriff auf Application Cost Profiler verwalten, sollten Sie wissen, welche IAM Funktionen für die Verwendung mit Application Cost Profiler verfügbar sind. Einen allgemeinen Überblick darüber, wie Application Cost Profiler und andere AWS Services zusammenarbeitenIAM, finden Sie unter AWS Services That Work with IAM im IAM Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien von Application Cost Profiler
- Ressourcenbasierte Richtlinien von Application Cost Profiler
- Autorisierung auf der Grundlage von Application Cost Profiler-Tags
- Rollen in Application Cost Profiler IAM

Identitätsbasierte Richtlinien von Application Cost Profiler

Mit IAM identitätsbasierten Richtlinien können Sie zusätzlich zu den Bedingungen, unter denen Aktionen zugelassen oder verweigert werden, zulässige oder verweigerte Aktionen und Ressourcen angeben. Application Cost Profiler unterstützt bestimmte Aktionen. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden, finden Sie im IAMBenutzerhandbuch unter IAMJSONPolicy Elements Reference.

Aktionen

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.

Das `Action` Element 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, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API 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.

Für Richtlinienaktionen in Application Cost Profiler wird vor der Aktion das folgende Präfix verwendet:. `application-cost-profiler:` Um beispielsweise jemandem die Erlaubnis zu erteilen, die Details Ihrer Application Cost Profiler-Berichtsdefinition einzusehen, nehmen Sie die `application-cost-profiler:GetReportDefinition` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Application Cost Profiler definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service ausführen können.

Um mehrere -Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie folgendermaßen durch Kommas.

```
"Action": [
      "application-cost-profiler:ListReportDefinitions",
      "application-cost-profiler:GetReportDefinition"
```

Im Folgenden sind die in Application Cost Profiler verfügbaren Aktionen aufgeführt. Jede ermöglicht die API Aktion mit dem gleichen Namen. Weitere Informationen zum Application Cost Profiler API finden Sie unter AWS Application Cost Profiler API Reference.

- `application-cost-profiler:ListReportDefinitions`— Ermöglicht das Auflisten der Berichtsdefinition für Ihr AWS Konto, falls vorhanden.
- `application-cost-profiler:GetReportDefinition`— Ermöglicht das Abrufen der Details der Berichtsdefinition für Ihren Application Cost Profiler-Bericht.
- `application-cost-profiler:PutReportDefinition`— Ermöglicht das Erstellen einer neuen Berichtsdefinition.
- `application-cost-profiler:UpdateReportDefinition`— Ermöglicht die Aktualisierung einer Berichtsdefinition.
- `application-cost-profiler:DeleteReportDefinition`— Ermöglicht das Löschen eines Berichts (nur über den Application Cost Profiler verfügbarAPI).
- `application-cost-profiler:ImportApplicationUsage`— Ermöglicht das Anfordern des Imports von Nutzungsdaten durch Application Cost Profiler aus einem bestimmten Amazon S3 S3-Bucket.

Ressourcen

Application Cost Profiler unterstützt nicht die Angabe von Amazon Resource Names (ARNs) für Ressourcen in einer Richtlinie.

Bedingungsschlüssel

Application Cost Profiler stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt aber die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAMBenutzerhandbuch.

Beispiele

Beispiele für identitätsbasierte Richtlinien von Application Cost Profiler finden Sie unter. AWS Beispiele für identitätsbasierte Richtlinien von Application Cost Profiler

Ressourcenbasierte Richtlinien von Application Cost Profiler

Application Cost Profiler unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Grundlage von Application Cost Profiler-Tags

Application Cost Profiler unterstützt weder das Markieren von Ressourcen noch die Steuerung des Zugriffs auf der Grundlage von Tags.

Rollen in Application Cost Profiler IAM

Eine IAMRolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit Application Cost Profiler

Sie können temporäre Anmeldeinformationen verwenden, um sich bei Federation anzumelden, eine IAM Rolle anzunehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API Operationen wie AssumeRoleoder GetFederationTokenaufrufen.

Application Cost Profiler unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Mit Diensten verknüpfte Rollen werden in Ihrem IAM Konto angezeigt und gehören dem Dienst. Ein -Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Application Cost Profiler unterstützt keine dienstbezogenen Rollen.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM Konto angezeigt und gehören dem Konto. Dies bedeutet, dass ein -Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Application Cost Profiler unterstützt keine Servicerollen.

AWS Beispiele für identitätsbasierte Richtlinien von Application Cost Profiler

Standardmäßig sind IAM Benutzer und Rollen nicht berechtigt, AWS Application Cost Profiler-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein Administrator muss IAM Richtlinien erstellen, die Benutzern und Rollen die Erlaubnis gewähren, die spezifischen API Operationen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien dann den IAM Benutzern oder Gruppen zuordnen, für die diese Berechtigungen erforderlich sind.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter Richtlinien auf der JSON Registerkarte erstellen im IAMBenutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Application Cost Profiler-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugreifen auf einen Amazon-S3-Bucket

Bewährte Methoden für Richtlinien

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

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle 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 AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Um festzulegen, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der Application Cost Profiler-Konsole

Um auf die AWS Application Cost Profiler-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Application Cost Profiler-Ressourcen in Ihrem AWS Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Entitäten (IAMBenutzer oder Rollen) mit dieser Richtlinie nicht wie vorgesehen.

Um sicherzustellen, dass diese Entitäten die Application Cost Profiler-Konsole verwenden können, um die Application Cost Profiler-Berichtsdefinition für Ihr AWS Konto anzuzeigen, fügen Sie den Entitäten die folgenden Berechtigungen zu.

```
application-cost-profiler:ListReportDefinitions
application-cost-profiler:GetReportDefinition
```

Sie könnten beispielsweise die folgende Richtlinie für Ihre schreibgeschützten Benutzer erstellen.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "application-cost-profiler:ListReportDefinitions",
            "application-cost-profiler:GetReportDefinition"
         ],
         "Resource":"*"
      }
   ]
}
```

Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

Sie müssen Benutzern, die nur Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline- und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

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

```
        }
    ]
}
```

Zugreifen auf einen Amazon-S3-Bucket

In diesem Beispiel möchten Sie einem IAM Benutzer in Ihrem AWS Konto Zugriff auf einen Ihrer Amazon S3 S3-Buckets gewähren. `examplebucket` Sie möchten dem Benutzer außerdem Berechtigungen zum Hinzufügen, Aktualisieren und Löschen von Objekten gewähren.

Zusätzlich zum Erteilen der Berechtigungen `s3:PutObject`, `s3:GetObject` und `s3:DeleteObject` für den Benutzer, gewährt die Richtlinie die Berechtigungen `s3:ListAllMyBuckets`, `s3:GetBucketLocation` und `s3:ListBucket`. Dies sind die zusätzlichen Berechtigungen, die von der Konsole benötigt werden. Außerdem sind die Aktionen `s3:PutObjectAcl` und `s3:GetObjectAcl` erforderlich, um Objekte in der Konsole kopieren, ausschneiden und einfügen zu können. Eine detaillierte Anleitung für das Gewähren von Berechtigungen für Benutzer und das Testen dieser Berechtigungen unter Verwendung der Konsole finden Sie unter Eine Beispielanleitung: Verwendung von Benutzerrichtlinien für die Steuerung des Zugriffs auf Ihren Bucket.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
```

```
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

Fehlerbehebung bei AWS Application Cost Profiler: Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Application Cost Profiler und AWS Identity and Access Management () IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Application Cost Profiler durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf die Ressourcen meines Antrags ermöglichen. Cost Profiler

Ich bin nicht berechtigt, eine Aktion in Application Cost Profiler durchzuführen

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 `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zum Application Cost Profiler-Bericht anzuzeigen, aber nicht `application-cost-profiler:ListReportDefinitions` dazu berechtigt ist.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er mithilfe der Aktion auf die Berichtsdefinitionsressource zugreifen kann. `application-cost-profiler:ListReportDefinitions`

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Application Cost Profiler übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Application Cost Profiler auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf die Ressourcen meines Antrags ermöglichen. Cost Profiler

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Application Cost Profiler diese Funktionen unterstützt, finden Sie unter. Wie funktioniert AWS Application Cost Profiler mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Gewähren des Zugriffs auf einen anderen IAMBenutzer AWS-Konto , dessen Eigentümer Sie sind.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Konformitätsprüfung für AWS Application Cost Profiler

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 Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

> **Note**
>
> Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- 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 für 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)) zusammengefasst.
- 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.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- 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.

Ausfallsicherheit inAWSApplication Cost Profiler

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und -Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen 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 AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS Application Cost Profiler

Als verwalteter Dienst ist AWS Application Cost Profiler 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, um über das Netzwerk auf Application Cost Profiler zuzugreifen. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

ApplicCost Profilerereignisse in EventBridge

Sie können Amazon verwenden EventBridge um IhreAWS-Services und reagieren automatisch auf Systemereignisse, z. B. bei Problemen mit der Anwendungsverfügbarkeit oder Ressourcenänderungen. Veranstaltungen vonAWSDienstleistungen werden geliefert an EventBridge nahezu in Echtzeit. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie unterAmazon EventBridge - Benutzerhandbuchaus.

Sie können überwachenAWSApplicCost Profiler-Events in EventBridgeaus. EventBridge leitet diese Daten an Ziele wieAWS Lambdaund Amazon Simple Notification Service (Amazon SNS). Diese Ereignisse sind mit den bei Amazon auftretenden Ereignissen identisch CloudWatch Ereignisse, die eine near-real-time Stream von Systemereignissen, der Änderungen in beschreibtAWSRessourcen schätzen.

Überwachen Sie die Berichterstellung mit EventBridge

mit EventBridgekönnen Sie Regeln erstellen, die zu ergreifende Aktionen definieren, wenn ApplicCost Profiler Service Cost Profiler Service Cost Profiler Service Sie können beispielsweise eine Regel erstellen, die Ihnen bei jeder Generierung eines Berichts eine E-Mail-Nachricht sendet.

So überwachen Sie die Generierung von Berichten

1. Loggen Sie sich einAWSmit einem Konto, das die Berechtigung zur Verwendung von beiden hat EventBridge ApplicCost Profiler Service
2. Öffnen des Amazonas EventBridge -Konsole beihttps://console.aws.amazon.com/events/aus.
3. Erstellen Sie mit den folgenden Werten eine EventBridge Regel, die Ereignisse überwacht, die beim Generieren eines Berichts erstellt wurden:

   - Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
   - FürEreignisquelle, wählenSonstigeaus.
   - In derEreignismuster-Bereich, wählen SieBenutzerdefinierte Muster (JSON-Editor)und fügen Sie anschließend das folgende Ereignismuster in das Textfeld ein:

     ```
     {
     ```

```
  "source": ["aws.application-cost-profiler"],
  "detail-type": ["Application Cost Profiler Report Generated"]
}
```

- FürZieltypen, wählenAWSBedienungund fürWählen Sie ein Ziel aus, wähle dasAWSService, bei dem Sie handeln möchten, wenn EventBridge erkennt ein Ereignis des ausgewählten Typs. Das Ziel wird ausgelöst, wenn ein Ereignis empfangen wird, das dem in der Regel definierten Ereignismuster entspricht.

Einzelheiten zum Erstellen von Regeln finden Sie unterAmazon erstellen EventBridge Regeln, die auf Ereignisse reagierenimAmazon EventBridge -Benutzerhandbuchaus.

Beispiel für ein Ereignis „Bericht generiert“

Dieses Ereignis informiert Sie, wenn ein Bericht generiert wurde und zum Abrufen bereitsteht. Die`message`gibt Ihnen den Amazon Simple Storage Service (Amazon S3) -Bucket und -Schlüssel für das Amazon-S3 -Objekt, in dem der Bericht gespeichert ist.

```
{
   "version": "0",
   "id": "01234567-EXAMPLE",
   "detail-type": "Application Cost Profiler Report Generated",
   "source": "aws.application-cost-profiler",
   "account": "123456789012",
   "time": "2021-03-31T10:23:43Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
     "message": "Application Cost Profiler report delivered in bucket: SampleBucket,
 key: SampleReport-112233445566"
   }
}
```

Dokumentverlauf

In der folgenden Tabelle werden die Dokumentationsversionen für beschriebenAWSCost Profiler für Anwendungen.

Änderung	Beschreibung	Datum
Benachrichtigung über die Einstellung des Dienstes	AWSApplication Cost Profiler wird bis zum 30. September 2024 eingestellt und akzeptiert keine Neukunden mehr.	11. August 2023
Ereignisse überwachen	Aufgrund von Änderunge n an derEventBridgeIn der Konsole wurde die Art und Weise, wie Sie Regeln zur Überwachung von Applicati on Cost Profiler-Ereignissen erstellen, geändert. Weitere Informationen finden Sie unterÜberwachung von Application Cost Profiler-Ereignissen inEventBridge.	5. Juli 2022
Aktualisierungen von Beispiele n für S3-Bucket-Richtlinien	Aktualisierung der Beispiele für S3-Bucket-Richtlinien, die nur in der Dokumenta tion verfügbar sind. Weitere Informationen finden Sie unterAmazon S3-Buckets für Application Cost Profiler einrichten.	6. Dezember 2021
Allgemeine Verfügbarkeit	Die erste öffentliche Version von Application Cost Profiler.	13. Mai 2021