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 neuen Kunden 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, Kosteninformationen zu Ihren AWS Ressourcen zu erhalten, indem die Ressourcennutzung nach Mandanten und nicht für die Ressource als Ganzes gemeldet wird. Ein Mandant kann ein Benutzer, eine Gruppe von Benutzern oder ein Projekt sein. Stellen Sie sicher, dass Sie Ihre Ressourcennutzung nach dem von Ihnen ausgewählten Mandanten identifizieren können. Um Kostenberichte über die 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.

Themen

So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein 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 ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. 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 eines Administratorbenutzers

Wenn Sie sich für ein AWS-Konto registriert haben, erstellen Sie einen Administratorbenutzer, damit Sie nicht den Root-Benutzer für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console als Kontobesitzer 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-AnmeldungBenutzerhandbuch zu .
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

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

Erstellen eines Administratorbenutzers

- Weisen Sie einem Administratorbenutzer in Administratorzugriff für Ihre täglichen administrativen Aufgaben zu AWS IAM Identity Center.

  Anleitungen dazu finden Sie unter Erste Schritte im AWS IAM Identity Center Benutzerhandbuch.

Anmelden als Administratorbenutzer

- 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 unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmgesteuerten Zugriff, wenn sie außerhalb der AWS Management Console mit AWS interagieren möchten. Die Vorgehensweise, um programmgesteuerten Zugriff zu gewähren, hängt davon ab, welcher Benutzertyp auf 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 programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Konfigurieren der AWS CLI für die Verwendung von AWS IAM Identity Center im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs, Tools und AWS-APIs finden Sie unter IAM-Identity-Center-Authentifizierung im Referenzhandbuch zu AWS-SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS-Ressourcen im IAM-Benutzerhandbuch.

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

Spezifische Voraussetzungen für Application Cost Profiler

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

- Cost Explorer aktivieren

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

Weitere Informationen finden Sie unter Aktivieren von Cost Explorer im AWS Billing and Cost Management -Benutzerhandbuch.

- Erstellen von S3-Buckets

  Erstellen Sie mindestens zwei Amazon Simple Storage Service (Amazon S3)-Buckets. Application Cost Profiler verwendet einen S3-Bucket, um Ihnen Berichte bereitzustellen. 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, damit Sie die Nutzung für verschiedene Services in separaten S3-Buckets mit unterschiedlichen Berechtigungen beibehalten können, wenn dies für Ihre Sicherheit erforderlich ist. Sie müssen Application-Cost-Profiler-Berechtigungen für diese S3-Buckets erteilen.

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

- Tags aktivieren

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

  Weitere Informationen zum Aktivieren von AWS generierten Tags finden Sie unter Aktivieren der von generierten KostenzuordnungsAWS-Tags im AWS Billing and Cost Management -Benutzerhandbuch. Weitere Informationen zum Aktivieren benutzerdefinierter Tags finden Sie unter Aktivieren benutzerdefinierter Kostenzuordnungs-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	Die`ApplicationId`angegeben in den Nutzungsdaten, die an Application Cost Profiler gesendet werden.
TenantIdentifier	Die`TenanID`angegeben 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	Die`AWS`Produkt, 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 StundeTenant1für die Hälfte der Zeit. Eine halbe Stunde bleibt wieunattributedaus. 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 imTenantCostcolumn.

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 geteilten gilt für den Datenschutz in AWS Application Cost Profiler. https://aws.amazon.com/compliance/shared-responsibility-model/ Wie in diesem Modell beschrieben, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt enthält die Sicherheitskonfigurations- und Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

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

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Application Cost Profiler oder anderen unter AWS-Services Verwendung der Konsole, APIAWS CLI, oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

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

Verschlüsselung im Ruhezustand

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

Für Amazon S3-Buckets, die Sie bereitstellen, müssen Sie den Berichts-Bucket verschlüsseln, und kann 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 während der Übertragung. Die Kommunikation mit Application Cost Profiler erfolgt immer über HTTPS, sodass Ihre Daten während der Übertragung immer verschlüsselt werden. Diese Verschlüsselung ist standardmäßig konfiguriert, wenn Sie Application Cost Profiler verwenden.

Identity and Access Management für AWS Application Cost Profiler

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer für die Nutzung von Application-Cost-Profiler-Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Fehlerbehebung für AWS Application-Cost-Profiler-Identität und -Zugriff

Zielgruppe

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

Service-Benutzer – Wenn Sie den Application-Cost-Profiler-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie zur Ausführung von Aufgaben weitere Funktionen von Application Cost Profiler verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf ein Feature in Application Cost Profiler zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung für AWS Application-Cost-Profiler-Identität und -Zugriff.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für die Ressourcen von Application Cost Profiler verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Application Cost Profiler. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Funktionen und Ressourcen von Application Cost Profiler Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Application Cost Profiler verwenden kann, finden Sie unter Funktionsweise von AWS Application Cost Profiler mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Application Cost Profiler verfassen können. Beispiele für identitätsbasierte Richtlinien von Application Cost Profiler, die Sie in IAM verwenden können, finden Sie unter AWS Beispiele für identitätsbasierte Richtlinien für Application Cost Profiler.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center),

die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

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

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

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

AWS-Konto-Root-Benutzer

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

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir,

temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

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

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

IAM-Rollen

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

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

- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff: Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Service kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Prinzipalberechtigungen – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Richtlinien gewähren einem Prinzipal Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Informationen dazu, ob eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erfordert, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für -AWSServices in der Service-Autorisierungs-Referenz.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und – AWS CLIoder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil,

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

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

Verwalten des Zugriffs mit Richtlinien

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

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

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

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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

Ressourcenbasierte Richtlinien

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

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

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

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

- Berechtigungsgrenzen:Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien:Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

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

Funktionsweise von AWS Application Cost Profiler mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Application Cost Profiler zu verwalten, sollten Sie verstehen, welche IAM-Funktionen Sie mit Application Cost Profiler verwenden können. Einen Überblick über das Zusammenwirken von Application Cost Profiler und anderen -AWSServices mit IAM finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien für Application Cost Profiler
- Ressourcenbasierte Richtlinien für Application Cost Profiler
- Autorisierung basierend auf Application-Cost-Profiler-Tags
- IAM-Rollen für Application Cost Profiler

Identitätsbasierte Richtlinien für Application Cost Profiler

Mit identitätsbasierten IAM-Richtlinien können Sie zusätzlich zu den Bedingungen, unter denen Aktionen erlaubt oder verweigert werden, auch erlaubte oder verweigerte Aktionen und Ressourcen angeben. Application Cost Profiler unterstützt bestimmte Aktionen. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

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

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

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

Richtlinienaktionen in Application Cost Profiler verwenden das folgende Präfix vor der Aktion: `application-cost-profiler:`. Um beispielsweise jemandem die Berechtigung zum Anzeigen der Details Ihrer Application-Cost-Profiler-Berichtsdefinition zu erteilen, fügen Sie die `application-cost-profiler:GetReportDefinition` Aktion in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Application Cost Profiler definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen 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 Aktionen aufgeführt, die in Application Cost Profiler verfügbar sind. Jede erlaubt die gleichnamige API-Aktion. Weitere Informationen zur Application-Cost-Profiler-API finden Sie unter AWS Application-Cost-Profiler-API-Referenz.

- `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 das Aktualisieren einer Berichtsdefinition.
- `application-cost-profiler:DeleteReportDefinition` – Ermöglicht das Löschen eines Berichts (nur über die Application-Cost-Profiler-API verfügbar).
- `application-cost-profiler:ImportApplicationUsage` – Ermöglicht das Anfordern von Application-Cost-Profiler-Importnutzungsdaten aus einem angegebenen Amazon S3-Bucket.

Ressourcen

Application Cost Profiler unterstützt nicht die Angabe von Amazon-Ressourcennamen (ARNs) in einer Richtlinie.

Bedingungsschlüssel

Application Cost Profiler stellt keine servicespezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Beispiele

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

Ressourcenbasierte Richtlinien für Application Cost Profiler

Application Cost Profiler unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung basierend auf Application-Cost-Profiler-Tags

Application Cost Profiler unterstützt nicht das Markieren von Ressourcen oder das Steuern des Zugriffs auf der Grundlage von Tags.

IAM-Rollen für Application Cost Profiler

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen.

Verwenden temporärer Anmeldeinformationen mit Application Cost Profiler

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldeinformationen, indem Sie AWS STS -API-Operationen wie AssumeRole oder aufrufenGetFederationToken.

Application Cost Profiler unterstützt die Verwendung temporärer Anmeldeinformationen.

Serviceverknüpfte Rollen

Serviceverknüpfte Rollen erlauben AWS-Services den Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Auftrag auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein -Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Application Cost Profiler unterstützt keine serviceverknüpften 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 zum 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 für Application Cost Profiler

Standardmäßig haben IAM-Benutzer und -Rollen keine Berechtigungen zum Erstellen oder Ändern von AWS Application-Cost-Profiler-Ressourcen. Sie können auch keine Aufgaben mit der AWS Management Console, der AWS Command Line Interface (AWS CLI) oder der AWS API ausführen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen der spezifischen API-Operationen gewähren, die sie benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

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

Themen

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

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

Verwenden der Application-Cost-Profiler-Konsole

Um auf die AWS Application-Cost-Profiler-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Ressourcen von Application Cost Profiler in Ihrem AWS Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

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

```
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 unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

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

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

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

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

Zugreifen auf einen Amazon-S3-Bucket

In diesem Beispiel möchten Sie einem IAM-Benutzer in Ihrem AWS Konto Zugriff auf einen Ihrer Amazon 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 für AWS Application-Cost-Profiler-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige 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 autorisiert, eine Aktion im Application Cost Profiler auszuführen
- Ich bin nicht autorisiert, iam durchzuführen:PassRole
- Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine Ressourcen von Application Cost Profiler gewähren

Ich bin nicht autorisiert, eine Aktion im Application Cost Profiler auszuführen

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

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zum Application-Cost-Profiler-Bericht anzuzeigen, aber nicht über `application-cost-profiler:ListReportDefinitions` die Berechtigung verfügt.

```
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 mit der `application-cost-profiler:ListReportDefinitions` Aktion auf die Berichtsdefinitionsressource zugreifen kann.

Ich bin nicht autorisiert, iam durchzuführen:PassRole

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

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. 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.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine Ressourcen von Application Cost Profiler gewähren

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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Application Cost Profiler diese Funktionen unterstützt, finden Sie unter Funktionsweise von AWS Application Cost Profiler mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.

- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Compliance-Validierung für AWS Application Cost Profiler

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

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

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

- Kurzanleitungen für Sicherheit und Compliance: In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

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

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub: Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager: Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards 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 inAWSCost Profiler für Anwendungen

Als verwalteter ServiceAWSApplication Cost Profiler ist geschützt durchAWSglobale Netzwerksicherheit. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Du verwendestAWSveröffentlichte API-Aufrufe für den Zugriff auf Application Cost Profiler über das Netzwerk. Kunden müssen Folgendes unterstützen:

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

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

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