用户指南

服务限额

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

服务限额: 用户指南

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其它商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 Service Quotas？ ... 1
- Service Quotas 的特点 ... 1
- Service Quotas 中的术语 ... 1
- 访问 Service Quotas ... 2

开始使用 ... 4
查看服务配额 ... 5
请求增加配额 ... 6
- 查看配额请求历史 ... 6

为资源添加标签 ... 8
- 支持的资源 ... 9
- 标签限制 ... 9
- 所需权限 ... 9
- 管理标签（控制台） ... 10
- 管理标签 (AWS CLI） ... 10
- 管理标签 (AWSAPI) ... 11
- 使用 标签控制访问 ... 11

使用请求模板 ... 13
安全性 ... 15
- 数据保护 ... 15
- 日志记录和监控 ... 16
  - 概览 ... 16
  - 使用 CloudTrail 记录 Service Quotas API ... 17
  - 使用 CloudWatch 警报 ... 20
- Identity and Access Management ... 21
  - 使用 IAM 策略授予权限 ... 21
  - Service Quotas 的 API 操作 ... 22
  - Service Quotas 资源 ... 23
  - Service Quotas 的资源级权限 ... 23
  - Service Quotas 的条件键 ... 23
  - 预定义AWSService Quotas 的托管策略 ... 24
- 合规性验证 ... 24
- 故障恢复能力 ... 24
- 基础设施安全性 ... 25

Service Quotas 的配额 ... 26

Service Quotas 文档记录 29
..... xxx

什么是 Service Quotas？

使用 Service Quotas，您可以查看和管理自己的配额AWS 服务从中心位置出发。中的配额，也称为中的限制。AWS 服务中资源、操作和项目的最大值。AWS 账户. EQUOAWS 服务定义其配额并为这些配额建立默认值。根据您的业务需求，您可能需要提高服务配额值。使用 Service Quotas，您可以查找服务配额并请求提高配额。支持可能会批准、拒绝或部分批准您的请求。

目录

- Service Quotas 的特点
- Service Quotas 中的术语
- 访问 Service Quotas

Service Quotas 的特点

“Service Quotas” 提供以下功能：

查看您的服务配额

“Service Quotas” 控制台提供快速访问AWS所有账户的默认配额值AWS 区域. 在 Service Quotas 控制台中选择服务时，您会看到配额以及配额是否可调。应用配额是覆盖或特定配额的增加，超过AWS默认值。

请求提高服务配额

对于任何可调整的 Service Quotas，您可以使用 “服务配额” 来请求提高配额。要请求提高配额，请在 “Service Quotas” 控制台中选择服务和特定配额，然后选择请求提高配额. 您还可以使用 “Service Quotas” API 操作或AWS CLI用于请求增加服务配额的工具。

查看资源的当前利用率

在账户处于活动状态一段时间后，您可以查看资源利用率图。

Service Quotas 中的术语

以下术语对了解 Service Quotas 及其工作原理来说很重要。

服务配额

适用于AWS 账户或者AWS 区域. 的数量AWS Identity and Access Management每个账户的 (IAM) 角色是基于账户的配额的示例。每个区域的虚拟私有云 (VPC) 数量就是基于区域的配额的示例。要确定服务配额是否特定于区域，请查看服务配额的描述。

可调的值

可以提高的配额值。

应用的配额

在配额增加后更新的配额值。

默认值

建立的初始配额值AWS.

全球配额

在账户级别应用的服务配额。全球配额都可用AWS 区域. 您可以从任何地区申请提高全球配额。您可以从请求提升的地区跟踪增加的状态。如果您请求提高全局配额的配额，则在第一个请求完成之前，您无法从其他地区申请增加同一配额。初始请求完成后，应用的配额值在可用的所有可用配额的区域中都可见。

使用率

服务配额中正在使用的资源或操作的数量。

利用率

正在使用的服务配额的百分比。例如，如果配额值为 200 个资源，正在使用 150 个资源，则利用率为 75%。

访问 Service Quotas

您可以通过以下方式使用 “Service Quotas”：

AWS Management Console

“Service Quotas” 控制台是一个基于浏览器的界面，您可以用它来查看和管理您的服务配额。您几乎可以使用控制台执行与服务配额相关的任何任务。您可以从任何位置访问 Service QuotasAWS Management Console通过在顶部导航栏上选择该页面，或者在AWS Management Console.

AWS Command Line Interface工具

通过使用AWS Command Line Interface工具，您可以在系统的命令行中发出命令来执行 Service Quotas 和其他AWS任务。与使用控制台相比，这可能是一种更快、更方便的方法。如果要构建执行 AWS 任务的脚本，命令行工具也会十分有用。

AWS 提供两组命令行工具：AWS Command Line Interface 和 AWS Tools for Windows PowerShell。有关安装和使用 AWS CLI 的更多信息，请参阅 AWS Command Line Interface 用户指南。有关安装和使用 Tools for Windows PowerShell 的信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

AWS 开发工具包

这些区域有：AWS开发工具包包含各种编程语言和平台的库和示例代码（例如，Java、Python、红宝石、.NET、iOS 和 Android, 和其他的)。开发工具包包括多个任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求。有关 AWS 开发工具包的更多信息（包括如何下载和安装这些工具包），请参阅适用于 Amazon Web Services 的工具。

Service Quotas 入门

打开 Service Quotas 控制台时，仪表板会显示最多 9 项服务的卡片。每张卡都列出了AWS 服务. 选择卡片将打开一个显示服务配额的页面。您可以选择在仪表板上显示哪些服务。

修改仪表板服务卡

1. 登录到AWS Management Console然后在打开 Service Quotas 控制台https://console.aws.amazon.com/servicequotas/home.
2. 在控制面板上，选择修改控制面板卡.
3. 当前选择的服务显示在右侧。如果选择了九项服务，则必须先删除服务，然后才能添加其他服务。对于控制面板上不需要的每项服务，请选择Remove.
4. 要将服务添加到仪表板，请从选择服务.
5. 添加和删除完服务后，选择Save（保存）.

后续步骤

- 查看服务配额
- 请求增加配额

查看服务配额

使用 Service Quotas，您可以查找特定配额的值。配额，也称为限制. 您还可以查找特定配额的所有配额AWS 服务.

要查看服务的配额

1. 登录到AWS Management Console然后在打开 Service Quotas 控制台：https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择 AWS services（AWS 服务）。
3. SELECTAWS 服务从列表中选择，或在搜索字段中键入服务名称。对于每个配额，控制台将显示名称、应用的配额、默认配额以及配额是否可调。如果应用的值不可用，则会显示控制台不可用.
4. 要查看有关配额的其他信息（如配额描述和 Amazon 资源名称 (ARN)，请选择配额名称。

请求增加配额

对于可调 配额，您可以请求增加配额。自动批准较小的增加，更大的请求会被提交至支持. 您可以在支持 控制台中跟踪您的请求案例。要提高服务配额的请求没有得到优先支持。如果您有紧急请求，请联系支持.

支持可能会批准、拒绝或部分批准您的请求。

要请求提高服务配额

1. 登录到AWS Management Console然后在打开 Service Quotas 控制台https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择 AWS services（AWS 服务）。
3. 选择AWS 服务从列表中，或在搜索框中键入服务名称。
4. 如果配额是可调整的，您可以选择按钮或名称，然后选择请求增加配额.
5. 对于 Change quota value (更改配额值)，输入新值。新值必须大于当前值。
6. 选择 Request (请求)。

要查看任何待处理或最近解决的请求，请从导航窗格选择 Dashboard (控制面板)。对于待处理的请求，请选择请求状态以打开收到的请求。请求的初始状态为Pending. 在状态变为后请求配额，您将看到案例编号支持. 选择案例编号以打开请求服务单。

解决请求后，配额的 Applied quota value (应用的配额值) 设置为新值。

查看配额请求历史

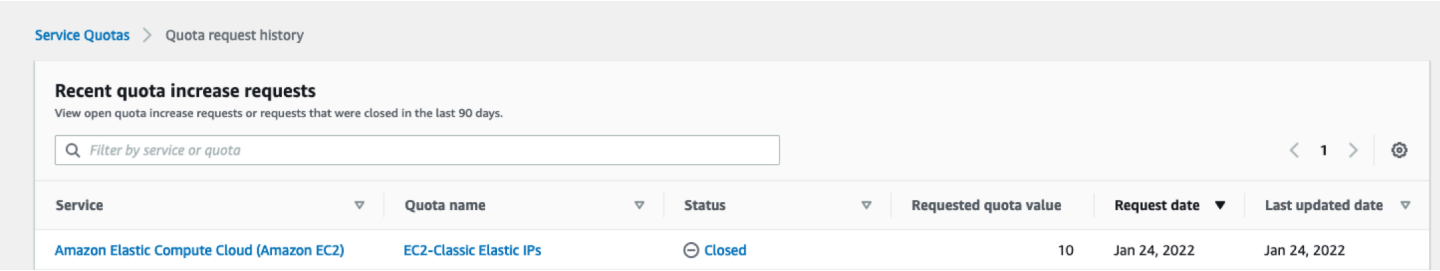
在 Service Quotas 控制台中查看配额请求历史记录。控制台会显示过去 90 天内所有未完成的增加配额请求以及关闭的配额请求。

> **Note**
>
> 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的AWS 服务（如 IAM）可能仅在某些地区提供。如果您在不同地区有增加配额的请求，请务必先选择适当的区域。

要查看配额请求历史记录，请执行以下步骤：

1. 登录到AWS Management Console然后在打开 Service Quotas 控制台https://console.aws.amazon.com/servicequotas/home.
2. 要查看任何待处理或最近解决的请求，请选择请求历史从导航窗格中。

这些区域有：最近增加配额请求面板显示有关您最近打开的配额增加请求以及在 90 天内关闭的任何请求的信息。



- 服务— 显示为请求选择的服务名称。
- 配额名称— 显示为增加配额选择的配额名称。
- 状态— 显示增加配额请求的状态。

  您可能会看到以下类型的状态：

  - Closed— 批准增加配额并关闭请求。
  - 已批准配额请求— 自动批准增加配额。
  - 请求配额— 配额增加请求待处理支持审批。
- 请求配额值— 您为配额请求的增加配额值。
- 请求日期— 您请求增加配额的日期。
- 上次更新日期— 请求最后收到更新的日期。

查看有关服务、配额名称和状态的详细信息请求历史通过选择其中一个条目来表。

在 Service Quotas 中标记资源

标签 是自定义的属性标签，您将其添加到 AWS 资源以便更轻松地确定、组织和搜索资源。每个标签具有两个部分：

- 一个标签键之外的压缩算法（例如`CostCenter`、`Environment`，或者`Project`. 标签键区分大小写。
- 一个标签值之外的压缩算法（例如`111122223333`要么`Production`. 您可以将标签的值设为空的字符串，但是不能将其设为空值。省略标签值与使用空字符串相同。与标签键一样，标签值区分大小写。

您可使用标签，按用途、所有者、环境或其他标准对资源进行分类。

标签可帮助您：

- 标识和整理您的 AWS 资源。许多 Amazon Web Services 支持标记，因此，您可以将同一标签分配给来不同服务的资源，以指示这些资源是相关的。
- 跟踪您的 AWS 成本。您可以在 AWS 账单与成本管理 控制面板上激活这些标签。AWS 使用标签对您的成本进行分类，并向您提供每月成本分配报告。有关更多信息，请参阅《AWS Billing 用户指南》https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/中的使用成本分配标签。
- 控制对 AWS 资源的访问。有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/中的使用标签控制访问。

主题

- 支持在 Service Quotas 中标记的资源
- 标签限制
- 标记 Service Quotas 资源所需的权限
- 管理 Service Quotas 标签（控制台）
- 管理 Service Quotas 标签 (AWS CLI）
- 管理 Service Quotas 标签 (AWSAPI)
- 使用 Service Quotas 标签控制访问

支持在 Service Quotas 中标记的资源

用于标记支持的 Service Quotas 资源应用配额，之前申请的增加配额获得批准支持.

> **Important**
>
> 只有当配额具有应用的配额值时，才能对配额进行标记。无法标记具有默认配额值的配额。请勿在标签中存储个人身份信息 (PII) 或其他机密或敏感信息。标签不适合用于私有或敏感数据。

标签限制

以下限制应用到 Service Quotas 资源的标签：

- 您可以分配给资源的最大标签数量 - 50
- 最大密钥长度 – 128 个 Unicode 字符
- 最大值长度 – 256 个 Unicode 字符
- 键和值的有效字符 - a-z、A-Z、0-9、空格和以下字符：_ . : / = + - 和 @
- 键和值区分大小写。
- 请勿使用`aws:`作为键的前缀，因为它保留为AWS使用。

标记 Service Quotas 资源所需的权限

您必须配置权限以允许用户或角色管理 Service Quotas 中的标签。管理标签所需的权限通常与该任务的 API 操作相对应。

为确保用户和角色可以使用 Service Quotas 控制台进行标记操作，请附加`ServiceQuotasReadOnlyAccess` AWS托管策略到实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限。

- 要将标签添加到应用的配额，您必须拥有以下权限：

  `servicequotas:ListTagsForResource`

  `servicequotas:TagResource`
- 要查看应用配额的标签，您必须拥有以下权限：

```
servicequotas:ListTagsForResource
```

- 要从应用配额中删除现有标签，您必须拥有以下权限：

```
servicequotas:UntagResource
```

- 要编辑应用配额的现有标签值，您必须拥有以下权限：

```
servicequotas:ListTagsForResource

servicequotas:TagResource

servicequotas:UntagResource
```

管理 Service Quotas 标签（控制台）

您可 Service Quotas 过使用AWS Management Console.

1. 登录到AWS Management Console然后在打开 Service Quotas 控制台https://console.aws.amazon.com/servicequotas/home.
2. 在导航页面中，选择AWS服务.
3. 选择一个AWS 服务从列表中输入，或在搜索框中键入服务名称。
4. 选择一项在应用配额值column.
5. 在 Tags (标签) 部分中，选择 Manage tags (管理标签)。此选项不适用于没有应用配额值的配额。
6. 您可以添加或删除标签，也可以编辑现有标签的标签值。在中输入标签的名称密钥. 您可以在 Value (值) 中添加可选的标签值。
7. 对标签进行所有更改后，选择保存更改.

如果操作成功，您将返回配额详细信息页面，您可以在其中验证更改。如果操作失败，请按照错误消息中的说明解决。

管理 Service Quotas 标签 (AWS CLI）

您可 Service Quotas 过使用AWS Command Line Interface(AWS CLI)。

- 向应用的配额添加标签

```
aws service-quotas tag-resource
```

- 查看已应用配额的标签

  `aws service-quotas list-tags-for-resource`
- 删除已应用配额的现有标签值

  `aws service-quotas untag-resource`

管理 Service Quotas 标签 (AWSAPI)

您可以使用 Service Quotas API 管理 Service Quotas 标签。

- 向应用的配额添加标签

  `TagResource`
- 查看已应用配额的标签

  `ListTagsForResource`
- 删除已应用配额的现有标签值

  `UntagResource`

使用 Service Quotas 标签控制访问

要根据标签控制对 Service Quotas 资源的访问，您需要在条件元素使用策略`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`，或者`aws:TagKeys`条件键。有关这些条件键的更多信息，请参阅控制对 的访问AWS使用资源标签的资源中的IAM 用户指南.

例如，将以下策略附加到AWS Identity and Access Management(IAM) 用户或角色，该实体可以请求增加Amazon Athena使用标签键标记的已应用配额**Owner**和标记值**admin**.

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

```
            }
        }
    ]
}
```

您还可以将标签附加到 IAM 实体（用户或角色）以使用基于属性的访问控制 (ABAC)。ABAC 是一种授权策略，该策略基于属性来定义权限。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看包含设置 ABAC 步骤的教程，请参阅IAM 教程：定义访问权限AWS根据标签资源中的IAM 用户指南.

使用 Service Quotas 请求模板

一个配额请求模板在为新的自定义配额时有助于节省时间AWS 账户在组织中。要使用模板，请为新账户配置所需的服务配额增加。然后，启用模板关联。这将模板与您的组织相关联AWS Organizations. 无论何时在组织中创建新账户，模板都会自动为您请求增加配额。

要使用请求模板，您必须使用AWS Organizations并且必须在同一组织中创建新账户。您的组织必须已启用所有功能，所有功能. 如果仅使用整合账单功能，则无法使用配额请求模板。

您可以通过添加或删除服务配额来更新请求模板。您还可以增加可调配额的值。一旦您调整模板，就会为新账户请求这些服务配额值。更新请求模板不会更新现有账户的配额值。

启用模板

1. 登录到AWS Management Console并在打开 Service Quotas 控制台：https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择。配额请求模板. 如果配额请求模板不可见，选择组织以打开它。
3. 在模板关联部分中，选择。启用.

向请求模板添加配额

1. 登录到AWS Management Console并在打开 Service Quotas 控制台：https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择。配额请求模板. 如果配额请求模板不可见，选择组织以打开它。
3. 在添加配额部分中，选择。添加配额.

> **Note**
>
> 您将最多 10 个配额添加到请求模板中。

4. 在存储库的添加配额页面上，选择区域、服务、配额, 和所需配额值，然后选择。Add.

从请求模板中删除配额

无论模板是否与组织关联，您都可以从模板中删除服务配额请求。如果您达到服务配额请求的最大数量，则可能需要从请求模板中删除一些配额。

1. 登录到AWS Management Console并在打开 Service Quotas 控制台：https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择。配额请求模板. 如果配额请求模板不可见，选择组织以打开它。
3. 在添加配额部分中，选择您希望移除的配额的选项按钮。
4. 选择 Remove。

禁用模板关联

如果禁用配额，新账户将收到AWS所有配额的默认配额值。禁用组织的模板关联不会从模板中删除服务配额请求。您可以继续在模板中编辑服务配额。

1. 登录到AWS Management Console并在打开 Service Quotas 控制台：https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择。配额请求模板. 如果配额请求模板不可见，选择组织以打开它。
3. 在模板关联部分中，选择。禁用.

Service Quotas 安全性

AWS 十分重视云安全性。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 客户，您也将从这些数据中心和网络架构受益。

安全性是 AWS 和您的共同责任。shared responsibility model（责任共担模式）（责任共担模式）（责任共担模式）将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS 合规性计划的一部分。要了解适用于 Service Quotas 的合规性计划，请参阅AWS合规性计划范围内的服务.
- 云中的安全性 – 您的责任由您使用的 AWS 服务 决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Service Quotas 时应用责任共担模型。以下主题说明如何配置 Service Quotas 以实现您的安全性和合规性目标。您还将了解如何使用其他AWS 服务这将帮助您监控和保护您的 Service Quotas 资源。

目录

- Service Quotas 中的数据保护
- 日志记录和监控 Service Quotas
- Service Quotas 的身份和访问管理
- Service Quotas 的合规性验证
- 中的 Service Quotas
- 中的基础设施安全性

Service Quotas 中的数据保护

这些区域有：AWS 责任共担模式适用于 “Service Quotas” 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Simple Storage Service（Amazon S3）中的个人数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用 Service Quotas 或其他时间AWS使用控制台、API、AWS CLI，或者AWS开发工具包。您在用于名称的标签或自由格式字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

日志记录和监控 Service Quotas

概览

监控是保持和您的其他 Service Quotas 的可靠性、可用性和性能的重要方面AWS解决方案。AWS提供以下监控工具来监控 Service Quotas、在出现错误时进行报告并在适当的时候采取自动化措施：

- AWS CloudTrail 捕获由您的 AWS 账户 或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。
- Amazon CloudWatch 实时监控您的 AWS 资源以及在 AWS 上运行的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以具有 CloudWatch 跟踪 Amazon EC2 实例的 CPU 使用率或其他指标并且在需要时自动启动新实例。有关更多信息，请参阅 。亚马逊 CloudWatch 用户指南.

使用记录 Service Quotas API 调用AWS CloudTrail

Service Quotas 与AWS CloudTrail，提供用户、角色或执行操作的记录的服务AWS 服务中的 Service Quotas。 CloudTrail 将 Service Quotas 的 API 调用作为事件捕获。捕获的调用包含来自 Service Quotas 控制台的调用和对 Service Quotas API 操作的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Service Quotas 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 中的控制台事件记录. 使用 CloudTrail 收集的信息，您可以确定向 Service Quotas 发出了什么请求、发出请求的 IP 地址、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 中的 Service Quotas 信息

在您创建 AWS 账户 时，将在该账户上启用 CloudTrail。当活动发生在 Service Quotas 中时，该活动将记录在 CloudTrail 活动以及其他AWS 服务中的事件事件记录. 您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅 。使用查看事件 CloudTrail 事件记录.

要持续记录在您的事件AWS 账户（包括 Service Quotas 的事件），请创建跟踪。一个踪迹启用 CloudTrail 将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您还可以配置其他AWS 服务进一步分析在中收集的事件数据并采取措施 CloudTrail 日志。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 接收 CloudTrail 来自多个区域的日志文件和接收 CloudTrail 来自多个账户的日志文件

所有 Service Quotas 操作均由记录 CloudTrail 并记录在Service Quotas API 参考. 例如，对`GetServiceQuota`、`RequestServiceQuotaIncrease`和`ListAWSDefaultServiceQuotas`中的操作会生成条目 CloudTrail 日志文件。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Service Quotas 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例显示了 CloudTrail 说明`RequestQuotaIncrease`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA123456789012Example",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "ASIA123456789012Example",
        "userName": " admin",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-01-24T16:57:04Z",
                "mfaAuthenticated": "true"
            }
        }
    },
    "eventTime": "2022-01-24T17:00:15Z",
    "eventSource": "servicequotas.amazonaws.com",
    "eventName": "RequestServiceQuotaIncrease",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.21.16.1",
    "userAgent": "aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.147-83.259.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
    "requestParameters": {
        "serviceCode": "ec2",
        "quotaCode": "L-CEED54BB",
        "desiredValue": 10
    },
    "responseElements": {
```

```
        "requestedQuota": {
            "id": "cd3ad3d9-2776-4ef1-a904-4c229d1642ee",
            "serviceCode": "ec2",
            "serviceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
            "quotaCode": "L-CEED54BB",
            "quotaName": "EC2-Classic Elastic IPs",
            "desiredValue": 10,
            "status": "PENDING",
            "created": "Jan 24, 2022 5:00:15 PM",
            "requester": "{\"accountId\":\"111122223333\",\"callerArn\":
\"arn:aws:iam::111122223333:user/admin\"}",
            "quotaArn": "arn:aws:servicequotas:us-east-1:111122223333:ec2/L-CEED54BB",
            "globalQuota": false,
            "unit": "None"
        }
    },
    "requestID": "3d3f5cdc-af30-4121-b69a-84b2f5c33be5",
    "eventID": "0cb51588-e460-4e00-bc48-a9d4820cad83",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

此示例显示，用户（管理员）于 2022 年 1 月 24 日生成了额外 Amazon Elastic Compute Cloud 弹性 IP 地址的请求。请求的增加额为 10 个，比默认配额 5 增加了 5 个。

以下是批准增加 Service Quotas 的示例：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "servicequotas.amazonaws.com"
    },
    "eventTime": "2022-01-24T17:02:17Z",
    "eventSource": "servicequotas.amazonaws.com",
    "eventName": "UpdateServiceQuotaIncreaseRequestStatus",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "servicequotas.amazonaws.com",
    "userAgent": "servicequotas.amazonaws.com",
    "requestParameters": null,
```

```
    "responseElements": null,
    "eventID": "e331b0a0-9395-4895-aeba-73cbab9ebcb0",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "requestId": "cdc5f1f78739459e6642407bb2bZKO8GKUM",
        "newStatus": "CASE_CLOSED",
        "createTime": "2022-01-24T17:00:15.363Z",
        "newQuotaValue": "10.0",
        "serviceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
        "quotaName": "EC2-Classic Elastic IPs",
        "unit": "None"
    },
    "eventCategory": "Management"
}
```

从`serviceEventDetails`部分，你可以确定支持批准了将配额增加到 10 个弹性 IP 地址的请求，并关闭了该请求。这些区域有：`newQuotaValue`显示 10 作为新配额。

SService Quotas a 和亚马逊 CloudWatch 警报

你可以创建亚马逊 CloudWatch 警报以在接近配额值阈值时通知您。在您需要请求提高配额时，设置警报可以帮助您提醒。

创建 CloudWatch 警报配额

1. 登录到AWS Management Console在打开 Service Quotas 控制台https://console.aws.amazon.com/servicequotas/home.
2. 在导航窗格中，选择AWS服务然后选择一项服务。
3. 选择支持的配额 CloudWatch 警报。

   如果您主动使用配额，则利用率将显示在配额描述下方。CloudWatch 告警部分将显示在页面底部。
4. In亚马逊 CloudWatch 警报，选择Create.
5. 适用于警报阈值，选择一个阈值。
6. 对于 Alarm name (警报名称)，输入警报的名称。此名称在AWS 账户.
7. 选择 Create（创建）。

8. 将通知添加到 CloudWatch 警报，请参阅创建 CloudWatch 根据 CloudWatch 公制中的亚马逊 CloudWatch 用户指南.

删除 CloudWatch 警报

1. 使用警报选择服务配额。
2. 选择警报。
3. 选择 Delete（删除）。

Service Quotas 的身份和访问管理

AWS 使用安全凭证来识别您的身份并向您授予对 AWS 资源的访问权限。你可以使用AWS Identity and Access Management(IAM) 可允许其他用户、服务和应用程序使用您的AWS资源完全或以有限的方式。您可以在不共享安全凭证的情况下执行此操作。

默认情况下，IAM 用户没有创建、查看或修改 AWS 资源的权限。要允许 IAM 用户访问资源（如负载均衡器）并执行任务，请执行以下步骤：

1. 创建授予 IAM 用户使用所需特定资源和 API 操作的权限的 IAM 策略。
2. 将该策略附加到 IAM 用户或 IAM 用户所属的组。

在将策略附加到一个用户或一组用户时，它会授权或拒绝用户使用指定资源执行指定任务。

例如，您可以使用 IAM 在您的AWS 账户. IAM 用户可以是人员、系统或应用程序。然后，使用 IAM 策略向用户和组授予对指定资源执行特定操作的权限。

使用 IAM 策略授予权限

在将策略附加到一个用户或一组用户时，它会授权或拒绝用户使用指定资源执行指定任务。

IAM 策略是包含一个或多个语句的 JSON 文档。每个语句的结构如下例所示。

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect": "effect",
    "Action": "action",
    "Resource": "resource-arn",
```

```
    "Condition": {
      "condition": {
        "key":"value"
      }
    }
  }]
}
```

- **`Effect`**— 的价值**`effect`**可以是`Allow`要么`Deny`. 在默认情况下，IAM 用户没有使用资源和 API 操作的许可，因此，所有请求均会被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。
- **`Action`**— 的价值**`action`**是对其授予或拒绝权限的特定 API 操作。有关指定的更多信息`Action`请参阅Service Quotas 的 API 操作.
- `Resource`Resource 受操作影响的资源。利用某些 Service Quotas API 操作，您可以限制对特定配额授予或拒绝的权限。为此，请在此语句中指定其 Amazon Resource Name (ARN)。否则，您可以使用通配符 (*) 来指定所有 Service Quotas 资源。有关更多信息，请参阅 Service Quotas 资源。
- `Condition`Condition — 您可以选择性地使用条件来控制策略的生效时间。有关更多信息，请参阅 Service Quotas 的条件键。

有关更多信息，请参阅 IAM 用户指南。

Service Quotas 的 API 操作

在`Action`IAM 策略语句的元素中，您可以指定 Service Quotas 所提供的任意 API 操作。如以下示例所示，您必须使用小写形式的字符串 `servicequotas:` 作为操作名称的前缀。

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

要在单个语句中指定多项操作，请使用方括号将操作括起来并以逗号分隔，如以下示例所示。

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

您也可以使用通配符指定多项操作。*)。以下示例指定以开头的 Service Quotas 的所有 API 操作名称：`Get`.

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

要指定 Service Quotas 的所有 API 操作，请使用通配符 (*) ，如以下示例所示。

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

有关 Service Quotas 的 API 操作列表，请参阅Service Quotas 操作.

Service Quotas 资源

资源级权限指的是能够指定允许用户对哪些资源执行操作的能力。对于支持资源级权限的 API 操作，您可以控制用户可与操作结合使用的资源。要在策略中指定资源，您必须使用其 Amazon Resource Name (ARN)。

配额的 ARN 具有以下示例中显示的格式。

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

对于不支持资源级权限的 API 操作，必须指定以下示例中显示的资源语句。

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

Service Quotas 的资源级权限

以下 Service Quotas 操作支持资源级权限：

- 将 Service QuoequtainCrease 请求放入模板
- RequestServiceQuotaIncrease

有关更多信息，请参阅 。Service Quotas 定义的操作中的服务授权参考.

Service Quotas 的条件键

在创建策略时，您可指定控制策略生效时间的条件。每个条件都包含一个或多个键值对。有全局条件键和特定于服务的条件键。

这些区域有：`servicequotas:servicekey` 特定于 Service Quotas。以下 Service Quotas API 操作支持此密钥：

- 将 Service QuoequtainCrease 请求放入模板
- RequestServiceQuotaIncrease

有关全局条件键的更多信息，请参阅AWS全局条件上下文键中的IAM 用户指南.

预定义AWSService Quotas 的托管策略

AWS 创建的托管策略将授予针对常用案例的必要权限。您可以根据您的 IAM 用户对 Service Quotas 所需的访问权限将这些策略附加到这些用户：

- `ServiceQuotasFullAccess`授予使用 Service Quotas 功能所需的完整访问权限。
- `ServiceQuotasReadOnlyAccess`授予对 Service Quotas 功能的只读访问权限。

Service Quotas 的合规性验证

作为多个项目的一部分，第三方审计员将评估的安全性和合 Service QuotasAWS合规性计划。其中包括 SOC、PCI、FedRAMP、HIPAA 及其它。

列表AWS 服务在特定的合规性计划范围内，请参阅AWS合规性计划范围内的服务. 有关常规信息，请参阅AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅下载 AWS Artifact 中的报告。

您在使用 Service Quotas 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。AWS提供以下资源来帮助实现合规性：

- 安全性与合规性 Quick Start 指南 - 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 – 此白皮书介绍公司如何使用AWS创建符合 HIPAA 标准的应用程序。
- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config 开发人员指南中的使用规则评估资源 – 此 AWS Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub：此 AWS 服务 提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。

中的 Service Quotas

AWS 全球基础设施围绕 AWS 区域 和可用区构建。AWS 区域 提供多个在物理上独立且隔离的可用区，这些可用区与延迟率低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作

在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

中的基础设施安全性

作为托管AWS 服务，Service Quotas 受AWS中描述的全局网络安全程序Amazon Web Services：安全过程概述白皮书。

你使用AWS发布的 API 调用通过网络访问 Service Quotas。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

Service Quotas 的服务配额

下表列出了您的 Service Quotas 资源的默认最大值AWS 账户. 所有这些配额值都是按AWS 区域，除非另有说明。你无法调整这些配额值。

增加请求

配额	默认值
每个 账户的活动服务配额增加请求	20
每个地区活动服务配额增加请求	2
每个配额活动服务配额增加请求	1

API 请求速率

配额	默认值
`GetAWSDefaultServiceQuota` 每秒请求数	5
其他`GetAWSDefaultServiceQuota` 在一次突发中每秒发送的请求	5
`GetRequestedServiceQuotaChange` 每秒请求数	5
其他`GetRequestedServiceQuotaChange` 在一次突发中每秒发送的请求	5
`GetServiceQuota` 每秒请求数	5
其他`GetServiceQuota` 在一次突发中每秒发送的请求	5
`ListAWSDefaultServiceQuotas` 每秒请求数	10
其他`ListAWSDefaultServiceQuotas` 在一次突发中每秒发送的请求	10
`ListRequestedServiceQuotaChangeHistory` 每秒请求数	5

配额	默认值
其他ListRequestedServiceQuotaChangeHistory 在一次突发中每秒发送的请求	5
ListRequestedServiceQuotaChangeHistoryByQuota 每秒请求数	5
其他ListRequestedServiceQuotaChangeHistoryByQuota 在一次突发中每秒发送的请求	5
ListServiceQuotas 每秒请求数	10
其他ListServiceQuotas 在一次突发中每秒发送的请求	10
ListServices 每秒请求数	10
其他ListServices 在一次突发中每秒发送的请求	10
ListTagsForResource 每秒请求数	10
ListTagsForResource 在一次突发中每秒发送的请求	10
RequestServiceQuotaIncrease 每秒请求数	3
其他RequestServiceQuotaIncrease 在一次突发中每秒发送的请求	3
TagResource 每秒请求数	10
TagResource 在一次突发中每秒发送的请求	10
UntagResource 每秒请求数	10
UntagResource 在一次突发中每秒发送的请求	10

配额请求模板 API 请求费率

配额	默认值
AssociateQuotaTemplate 每秒请求数	1
其他AssociateQuotaTemplate 在一次突发中每秒发送的请求	1
DeleteServiceQuotaIncreaseRequestFromTemplate 每秒请求数	2
其他DeleteServiceQuotaIncreaseRequestFromTemplate 在一次突发中每秒发送的请求	1
DisassociateQuotaTemplate 每秒请求数	1
其他DisassociateQuotaTemplate 在一次突发中每秒发送的请求	1
GetAssociationForQuotaTemplate 每秒请求数	2
其他GetAssociationForQuotaTemplate 在一次突发中每秒发送的请求	2
GetServiceQuotaIncreaseRequestFromTemplate 每秒请求数	2
其他GetServiceQuotaIncreaseRequestFromTemplate 在一次突发中每秒发送的请求	1
ListServiceQuotaIncreaseRequestsInTemplate 每秒请求数	2
其他ListServiceQuotaIncreaseRequestsInTemplate 在一次突发中每秒发送的请求	1
PutServiceQuotaIncreaseRequestIntoTemplate 每秒请求数	1
其他PutServiceQuotaIncreaseRequestIntoTemplate 在一次突发中每秒发送	1

Service Quotas 文档记录

下表描述了自 Service Quotas 上一次发布以来对文档所做的重要更改。

更改	说明	日期
GitHub 上发布的指南	现在，您可 Service Quotas 通过在我们的 GitHub 位于存储库https://github.com/awsdocs/service-quotas-user-guide.	2021 年 3 月 23 日
标记 Service Quotas 资源	现在，您可以将标签附加到应用的配额并编写策略来控制对这些配额的访问。	2020 年 12 月 21 日
首次发布	此版本引入了 Service Quotas。	2019 年 6 月 24 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。