Service Quotas: User Guide
Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
Table of Contents

What is Service Quotas? ................................................................. 1
  Features of Service Quotas .......................................................... 1
  Terminology in Service Quotas ................................................. 1
  Accessing Service Quotas .......................................................... 2
Getting started ........................................................................... 3
Viewing service quotas ............................................................... 4
Requesting a quota increase ....................................................... 5
  View quota request history ...................................................... 5
Tagging resources ....................................................................... 7
  Supported resources .............................................................. 7
  Tag restrictions ................................................................... 7
  Permissions required ............................................................ 8
  Managing tags (console) ........................................................ 8
  Managing tags (AWS CLI) ........................................................ 9
  Managing tags (AWS API) ....................................................... 9
Controlling access using tags ..................................................... 9
Using request templates .......................................................... 11
Security ..................................................................................... 13
  Data protection .................................................................... 13
  Logging and monitoring ........................................................ 14
    Overview ........................................................................... 14
    Logging Service Quotas APIs with CloudTrail ................... 14
    Using CloudWatch alarms .................................................. 17
  Identity and access management .......................................... 17
    Grant permissions using IAM policies ............................... 18
    API actions for Service Quotas ........................................... 18
    Service Quotas resources .................................................. 19
    Resource-level permissions for Service Quotas .................. 19
    Condition keys for Service Quotas ..................................... 19
    Predefined AWS managed policies for Service Quotas .......... 20
Compliance validation ............................................................... 20
Resilience ................................................................................ 20
Infrastructure security .............................................................. 21
Quotas for Service Quotas ....................................................... 22
Service Quotas Document history ............................................ 24
What is Service Quotas?

With Service Quotas, you can view and manage your quotas for AWS services from a central location. Quotas, also referred to as limits in AWS services, are the maximum values for the resources, actions, and items in your AWS account. Each AWS service defines its quotas and establishes default values for those quotas. Depending on your business needs, you might need to increase your service quota values. Service Quotas enables you to look up your service quotas and to request increases. AWS Support might approve, deny, or partially approve your requests.

Contents
- Features of Service Quotas (p. 1)
- Terminology in Service Quotas (p. 1)
- Accessing Service Quotas (p. 2)

Features of Service Quotas

Service Quotas provides the following features:

**View your service quotas**

The Service Quotas console provides quick access to the AWS default quota values for your account, across all AWS Regions. When you select a service in the Service Quotas console, you see the quotas and whether the quota is adjustable. *Applied quotas are overrides, or increases for a specific quota, over the AWS default value.*

**Request a service quota increase**

For any adjustable service quotas, you can use Service Quotas to request a quota increase. To request a quota increase, in the Service Quotas console, select the service and the specific quota, and then choose **Request quota increase**. You can also use Service Quotas API operations or the AWS CLI tools to request service quota increases.

**View current utilization of resources**

After your account becomes active for a period of time, you can view a graph of your resource utilization.

Terminology in Service Quotas

The following terms are important for understanding Service Quotas and how it works.

**service quota**

The maximum number of service resources or operations that apply to an AWS account or an AWS Region. The number of AWS Identity and Access Management (IAM) roles per account is an example of an account-based quota. The number of virtual private clouds (VPCs) per Region is an example of a Region-based quota. To determine whether a service quota is Region-specific, check the description of the service quota.

**adjustable value**

A quota value that can be increased.
**applied quota**

The updated quota value after a quota increase.

**default value**

The initial quota value established by AWS.

**global quota**

A service quota applied at an account level. Global quotas are available in all AWS Regions. You can request an increase to a global quota from any Region. You can track the status of the increase from the Region where you requested the increase. If you request a quota increase for a global quota, you can't request an increase for the same quota from a different Region until the first request is complete. After the initial request is completed, the applied quota value is visible in all Regions where applied quotas are available.

**usage**

The number of resources or operations in use for a service quota.

**utilization**

The percentage of a service quota in use. For example, if the quota value is 200 resources and 150 resources are in use, then the utilization is 75 percent.

---

**Accessing Service Quotas**

You can work with Service Quotas in the following ways:

**AWS Management Console**

The Service Quotas console is a browser-based interface that you can use to view and manage your service quotas. You can perform almost any task that's related to your service quotas by using the console. You can access Service Quotas from any AWS Management Console page by choosing it on the top navigation bar, or by searching for Service Quotas in the AWS Management Console.

**AWS Command Line Interface tools**

By using the AWS Command Line Interface tools, you can issue commands at your system's command line to perform Service Quotas and other AWS tasks. This can be a faster and more convenient approach than using the console. The command line tools also are useful if you want to build scripts that perform AWS tasks.


**AWS SDKs**

The AWS SDKs consist of libraries and sample code for various programming languages and platforms (for example, Java, Python, Ruby, .NET, iOS and Android, and others). The SDKs include tasks such as cryptographically signing requests, managing errors, and retrying requests automatically. For more information about the AWS SDKs, including how to download and install them, see Tools for Amazon Web Services.
Getting started with Service Quotas

When you open the Service Quotas console, the dashboard displays cards for up to nine services. Each card lists the number of service quotas for the AWS service. Choosing a card opens a page that displays the quotas for the service. You can choose which services appear on the dashboard.

To modify the dashboard service cards

2. On the dashboard, choose Modify dashboard cards.
3. The services that are currently selected appear on the right. If you have selected nine services, you must remove a service before you can add a different service. For each service that you don't need on the dashboard, choose Remove.
4. To add a service to the dashboard, select it from Choose services.
5. When you have finished adding and removing services, choose Save.

Next steps

- Viewing service quotas (p. 4)
- Requesting a quota increase (p. 5)
Viewing service quotas

Service Quotas enables you to look up the value of a particular *quota*, also referred to as a *limit*. You can also look up all quotas for a particular AWS service.

**To view the quotas for a service**

2. In the navigation pane, choose **AWS services**.
3. Select an AWS service from the list, or type the name of the service in the search field. For each quota, the console displays the name, applied quota, default quota, and whether the quota is adjustable. If the applied value is not available, the console displays **Not available**.
4. To view additional information about a quota, such as its description and Amazon Resource Name (ARN), choose the quota name.
Requesting a quota increase

For adjustable quotas, you can request a quota increase. Smaller increases are automatically approved, and larger requests are submitted to AWS Support. You can track your request case in the AWS Support console. Requests to increase service quotas don't receive priority support. If you have an urgent request, contact AWS Support.

AWS Support might approve, deny, or partially approve your requests.

**To request a service quota increase**

2. In the navigation pane, choose **AWS services**.
3. Choose an AWS service from the list, or type the name of the service in the search box.
4. If the quota is adjustable, you can choose the button or the name, and then choose **Request quota increase**.
5. For **Change quota value**, enter the new value. The new value must be greater than the current value.
6. Choose **Request**.

To view any pending or recently resolved requests, choose **Dashboard** from the navigation pane. For pending requests, choose the status of the request to open the request receipt. The initial status of a request is **Pending**. After the status changes to **Quota requested**, you'll see the case number with AWS Support. Choose the case number to open the ticket for your request.

After the request is resolved, the **Applied quota value** for the quota is set to the new value.

View quota request history

View your quota request history in the Service Quotas console. The console displays all open quota increase requests as well as quota requests closed in the last 90 days.

**Note**

An AWS service, such as IAM, may be available only in certain regions. If you have quota increase requests in different regions, be sure to select the appropriate region first.

To view the quota request history, use the following steps:

2. To view any pending or recently resolved requests, choose **Quota request history** from the navigation pane.

The **Recent quota increase requests** panel displays information about your open recent quota increase requests and any requests closed within 90 days.
**Service Quotas User Guide**

**View quota request history**

- **Service** – Displays the service name selected for the request.
- **Quota name** – Displays the quota name selected for the quota increase.
- **Status** – Displays the status of a request for a quota increase.

  You may see the following types of status:
  - **Closed** – Quota increase approved and request closed.
  - **Quota request approved** – Quota increase approved automatically.
  - **Quota requested** – Quota increase request pending AWS Support approval.
- **Requested quota value** – The increased quota value you requested for the quota.
- **Request date** – The date you requested the quota increase.
- **Last updated date** – The last date the request received an update.

View details about a service, quota name, and status in the **Quota request history** table by choosing one of the entries.
Tagging resources in Service Quotas

A tag is a custom attribute label that you add to an AWS resource to make it easier to identify, organize, and search for resources. Each tag has two parts:

- A tag key, such as CostCenter, Environment, or Project. Tag keys are case sensitive.
- A tag value, such as 111122223333 or Production. You can set the value of a tag to an empty string, but you can’t set the value of a tag to null. Omitting the tag value is the same as using an empty string. Like tag keys, tag values are case sensitive.

You can use tags to categorize resources by purpose, owner, environment, or other criteria.

Tags help you do the following:

- Identify and organize your AWS resources. Many Amazon Web Services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related.
- Track your AWS costs. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Use cost allocation tags in the AWS Billing User Guide.
- Control access to your AWS resources. For more information, see Controlling access using tags in the IAM User Guide.

Topics

- Resources that support tagging in Service Quotas (p. 7)
- Tag restrictions (p. 7)
- Permissions required for tagging Service Quotas resources (p. 8)
- Managing Service Quotas tags (console) (p. 8)
- Managing Service Quotas tags (AWS CLI) (p. 9)
- Managing Service Quotas tags (AWS API) (p. 9)
- Controlling access using Service Quotas tags (p. 9)

Resources that support tagging in Service Quotas

The Service Quotas resources for tagging support Applied quotas, previously requested quota increases approved by AWS Support.

Important

You can tag quotas only if they have an applied quota value. Quotas with default quota values can’t be tagged.

Don’t store personally identifiable information (PII) or other confidential or sensitive information in tags. Tags aren’t intended to be used for private or sensitive data.

Tag restrictions

The following restrictions apply to tags on Service Quotas resources:

- Maximum number of tags that you can assign to a resource – 50
• Maximum key length – 128 Unicode characters
• Maximum value length – 256 Unicode characters
• Valid characters for key and value – a-z, A-Z, 0-9, space, and the following characters: _ . : / = + - and @
• Keys and values are case sensitive.
• Don’t use aws: as a prefix for keys because it’s reserved for AWS use.

Permissions required for tagging Service Quotas resources

You must configure permissions to allow your users or roles to manage tags in Service Quotas. The permissions that are required to administer tags usually correspond to the API operations for the task.

To ensure that users and roles can use the Service Quotas console for tagging operations, attach the ServiceQuotasReadOnlyAccess AWS managed policy to the entities. For more information, see Adding permissions to a user in the IAM User Guide.

• To add tags to applied quotas, you must have the following permissions:
  servicequotas:ListTagsForResource
  servicequotas:TagResource

• To view tags for an applied quota, you must have the following permissions:
  servicequotas:ListTagsForResource

• To remove existing tags from an applied quota, you must have the following permissions:
  servicequotas:UntagResource

• To edit existing tag values for applied quotas, you must have the following permissions:
  servicequotas:ListTagsForResource
  servicequotas:TagResource
  servicequotas:UntagResource

Managing Service Quotas tags (console)

You can manage Service Quotas tags by using the AWS Management Console.

2. In the navigation page, choose AWS services.
3. Choose an AWS service from the list, or type the name of the service in the search box.
4. Choose a service with a value in the Applied quota value column.
5. In the Tags section, choose Manage tags. This option is not available for quotas without an applied quota value.
6. You can add or remove tags, or you can edit tag values for existing tags. Enter a name for the tag in Key. You can add an optional value for the tag in Value.
7. After making all of your changes to tags, choose Save changes.
If the operation is successful, you are returned to the quota details page where you can verify your changes. If the operation fails, please follow the instructions in the error message to resolve it.

Managing Service Quotas tags (AWS CLI)

You can manage Service Quotas tags by using the AWS Command Line Interface (AWS CLI).

- To add tags to applied quotas
  
  `aws service-quotas tag-resource`

- To view tags for an applied quota
  
  `aws service-quotas list-tags-for-resource`

- To delete existing tag values for applied quotas
  
  `aws service-quotas untag-resource`

Managing Service Quotas tags (AWS API)

You can manage Service Quotas tags by using the Service Quotas API.

- To add tags to applied quotas
  
  `TagResource`

- To view tags for an applied quota
  
  `ListTagsForResource`

- To delete existing tag values for applied quotas
  
  `UntagResource`

Controlling access using Service Quotas tags

To control access to Service Quotas resources based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys. For more information about these condition keys, see Controlling access to AWS resources using resource tags in the IAM User Guide.

For example, when you attach the following policy to an AWS Identity and Access Management (IAM) user or role, that entity can request an increase to Amazon Athena applied quotas that are tagged with the tag key `Owner` and tag value `admin`.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["servicequotas:RequestServiceQuotaIncrease"],
            "Resource": "arn:aws:servicequotas:*:*:athena/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "admin"}
            }
        }
    ]
}
```
You can also attach tags to IAM entities (users or roles) to use attribute-based access control (ABAC). ABAC is an authorization strategy that defines permissions based on attributes. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they're trying to access. ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

For more information about ABAC, see What is ABAC? in the IAM User Guide. To view a tutorial with steps for setting up ABAC, see IAM tutorial: Define permissions to access AWS resources based on tags in the IAM User Guide.
Using Service Quotas request templates

A quota request template helps you save time when customizing quotas for new AWS accounts in your organization. To use a template, configure the desired service quota increases for new accounts. Then, enable template association. This associates the template with your organization in AWS Organizations. Whenever new accounts are created in your organization, the template automatically requests quota increases for you.

To use a request template, you must use AWS Organizations and the new accounts must be created in the same organization. Your organization must have all features enabled, all features. If you use consolidated billing features only, you can't use quota request templates.

You can update the request template by adding or removing service quotas. You can also increase the values for adjustable quotas. As soon as you adjust the template, those service quota values are requested for new accounts. Updating a request template doesn't update quota values for existing accounts.

To enable template

2. In the navigation pane, choose Quota request template. If the Quota request template isn't visible, choose Organization to open it.
3. In the Template association section, choose Enable.

To add a quota to your request template

2. In the navigation pane, choose Quota request template. If the Quota request template isn't visible, choose Organization to open it.
3. In the Added quotas section, choose Add quota.

   Note
   You add up to 10 quotas to your request template.
4. On the Add quota page, choose a Region, Service, Quota, and Desired quota value, and then choose Add.

To remove a quota from your request template

You can remove service quota requests from the template regardless of whether the template is associated with an organization. If you reach the maximum number of service quota requests, you might need to remove some quotas from your request template.

2. In the navigation pane, choose Quota request template. If the Quota request template isn't visible, choose Organization to open it.
3. In the Added quotas section, select the option button for the quota that you want to remove.
4. Choose Remove.

To disable the template association

If you disable the quota, new accounts receive the AWS default quota values for all quotas. Disabling the template association from the organization doesn't delete the service quota requests from the template. You can continue to edit the service quotas in the template.

2. In the navigation pane, choose Quota request template. If the Quota request template isn't visible, choose Organization to open it.
3. In the Template association section, choose Disable.
Security in Service Quotas

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Service Quotas, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Service Quotas. The following topics show you how to configure Service Quotas to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Service Quotas resources.

Contents
- Data protection in Service Quotas (p. 13)
- Logging and monitoring Service Quotas (p. 14)
- Identity and access management for Service Quotas (p. 17)
- Compliance validation for Service Quotas (p. 20)
- Resilience in Service Quotas (p. 20)
- Infrastructure security in Service Quotas (p. 21)

Data protection in Service Quotas

The AWS shared responsibility model applies to data protection in Service Quotas. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
• Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
• If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a Name field. This includes when you work with Service Quotas or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Logging and monitoring Service Quotas

Overview

Monitoring is an important part of maintaining the reliability, availability, and performance of Service Quotas and your other AWS solutions. AWS provides the following monitoring tools to watch Service Quotas, report when something is wrong, and take automatic actions when appropriate:

• AWS CloudTrail captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.
• Amazon CloudWatch monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the Amazon CloudWatch User Guide.

Logging Service Quotas API calls using AWS CloudTrail

Service Quotas is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Service Quotas. CloudTrail captures all API calls for Service Quotas as events. The calls captured include calls from the Service Quotas console and code calls to the Service Quotas API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Service Quotas. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to Service Quotas, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Service Quotas information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Service Quotas, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history.
For an ongoing record of events in your AWS account, including events for Service Quotas, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions

All Service Quotas actions are logged by CloudTrail and are documented in the Service Quotas API Reference. For example, calls to the GetServiceQuota, RequestServiceQuotaIncrease and ListAWSDefaultServiceQuotas actions generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

### Understanding Service Quotas log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the RequestQuotaIncrease action.

```json
{
  "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",
...}
```
This example shows that the user, admin, generated a request for additional Amazon Elastic Compute Cloud Elastic IP addresses on January 24, 2022. The requested increase was 10, an increase of 5 from the default quota of 5.

The following is an example of an approved quota increase in Service Quotas:
From the serviceEventDetails section, you can determine that AWS Support approved the request for a quota increase to 10 Elastic IP addresses, and closed the request. The newQuotaValue displays 10 as the new quota.

**Service Quotas and Amazon CloudWatch alarms**

You can create Amazon CloudWatch alarms to notify you when you're close to a quota value threshold. Setting an alarm can help alert you if you need to request a quota increase.

**To create a CloudWatch alarm for a quota**

2. In the navigation pane, choose AWS services and then select a service.
3. Select a quota that supports CloudWatch alarms.
   
   If you actively use the quota, utilization appears beneath the quota description. The CloudWatch alarms section appears at the bottom of the page.
4. In Amazon CloudWatch alarms, choose Create.
5. For Alarm threshold, choose a threshold.
6. For Alarm name, enter a name for the alarm. This name must be unique within the AWS account.
7. Choose Create.
8. To add a notification to the CloudWatch alarm, see Creating a CloudWatch alarm based on a CloudWatch metric in the Amazon CloudWatch User Guide.

**To delete a CloudWatch alarm**

1. Choose the service quota with the alarm.
2. Select the alarm.
3. Choose Delete.

**Identity and access management for Service Quotas**

AWS uses security credentials to identify you and to grant you access to your AWS resources. You can use features of AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your AWS resources fully or in a limited way. You can do this without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources such as a load balancer, and to perform tasks, perform the following steps:
1. Create an IAM policy that grants the IAM user permission to use the specific resources and API actions they need.

2. Attach the policy to the IAM user or the group that the IAM user belongs to.

When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

For example, you can use IAM to create users and groups under your AWS account. An IAM user can be a person, a system, or an application. Then you grant permissions to the users and groups to perform specific actions on the specified resources using an IAM policy.

## Grant permissions using IAM policies

When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

An IAM policy is a JSON document that consists of one or more statements. Each statement is structured as shown in the following example.

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

- **Effect** – The value for effect can be either Allow or Deny. By default, IAM users don’t have permission to use resources and API actions, so all requests are denied. An explicit allow overrides the default. An explicit deny overrides any allows.

- **Action** – The value for action is the specific API action for which you are granting or denying permission. For more information about specifying Action, see API actions for Service Quotas (p. 18).

- **Resource** – The resource that’s affected by the action. With some Service Quotas API actions, you can restrict the permissions granted or denied to a specific quota. To do so, specify its Amazon Resource Name (ARN) in this statement. Otherwise, you can use the wildcard character (*) to specify all Service Quotas resources. For more information, see Service Quotas resources (p. 19).

- **Condition** – You can optionally use conditions to control when your policy is in effect. For more information, see Condition keys for Service Quotas (p. 19).

For more information, see the IAM User Guide.

## API actions for Service Quotas

In the Action element of your IAM policy statement, you can specify any API action that Service Quotas offers. You must prefix the action name with the lowercase string servicequotas:, as shown in the following example.

```
"Action": "servicequotas:GetServiceQuota"
```
To specify multiple actions in a single statement, enclose them in square brackets and separate them with a comma, as shown in the following example.

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

You can also specify multiple actions using the wildcard character (*). The following example specifies all API action names for Service Quotas that start with Get.

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

To specify all API actions for Service Quotas, use the wildcard character (*), as shown in the following example.

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

For the list of API actions for Service Quotas, see Service Quotas Actions.

## Service Quotas resources

*Resource-level permissions* refers to the ability to specify which resources users are allowed to perform actions on. For API actions that support resource-level permissions, you can control the resources that users are allowed to use with the action. To specify a resource in a policy statement, you must use its Amazon Resource Name (ARN).

The ARN for a quota has the format shown in the following example.

```
```

For API actions that don't support resource-level permissions, you must specify the resource statement shown in the following example.

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

### Resource-level permissions for Service Quotas

The following Service Quotas actions support resource-level permissions:

- `PutServiceQuotaIncreaseRequestIntoTemplate`
- `RequestServiceQuotaIncrease`

For more information, see Actions defined by Service Quotas in the *Service Authorization Reference*.

## Condition keys for Service Quotas

When you create a policy, you can specify the conditions that control when the policy is in effect. Each condition contains one or more key-value pairs. There are global condition keys and service-specific condition keys.

The `servicequotas:service` key is specific to Service Quotas. The following Service Quotas API actions support this key:
Predefined AWS managed policies for Service Quotas

The managed policies created by AWS grant the required permissions for common use cases. You can attach these policies to your IAM users, based on the access to Service Quotas that they require:

- **ServiceQuotasFullAccess** – Grants full access required to use Service Quotas features.
- **ServiceQuotasReadOnlyAccess** – Grants read-only access to Service Quotas features.

Compliance validation for Service Quotas

Third-party auditors assess the security and compliance of Service Quotas as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using Service Quotas is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **Architecting for HIPAA Security and Compliance Whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **Evaluating Resources with Rules** in the AWS Config Developer Guide – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Service Quotas

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.
Infrastructure security in Service Quotas

As a managed AWS service, Service Quotas is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Service Quotas through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.
Service quotas for Service Quotas

The following tables list the default maximum values for Service Quotas resources for your AWS account. All of these quota values are per AWS Region, unless noted otherwise. You can’t adjust these quota values.

### Increase requests

<table>
<thead>
<tr>
<th>Quota</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active service quota increase requests per account</td>
<td>20</td>
</tr>
<tr>
<td>Active service quota increase requests per Region</td>
<td>2</td>
</tr>
<tr>
<td>Active service quota increase requests per quota</td>
<td>1</td>
</tr>
</tbody>
</table>

### API request rates

<table>
<thead>
<tr>
<th>Quota</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetAWSDefaultServiceQuota requests per second</td>
<td>5</td>
</tr>
<tr>
<td>Additional GetAWSDefaultServiceQuota requests per second sent in one burst</td>
<td>5</td>
</tr>
<tr>
<td>GetRequestedServiceQuotaChange requests per second</td>
<td>5</td>
</tr>
<tr>
<td>Additional GetRequestedServiceQuotaChange requests per second sent in one burst</td>
<td>5</td>
</tr>
<tr>
<td>GetServiceQuota requests per second</td>
<td>5</td>
</tr>
<tr>
<td>Additional GetServiceQuota requests per second sent in one burst</td>
<td>5</td>
</tr>
<tr>
<td>ListAWSDefaultServiceQuotas requests per second</td>
<td>10</td>
</tr>
<tr>
<td>Additional ListAWSDefaultServiceQuotas requests per second sent in one burst</td>
<td>10</td>
</tr>
<tr>
<td>ListRequestedServiceQuotaChangeHistory requests per second</td>
<td>5</td>
</tr>
<tr>
<td>Additional ListRequestedServiceQuotaChangeHistory requests per second sent in one burst</td>
<td>5</td>
</tr>
<tr>
<td>ListRequestedServiceQuotaChangeHistoryByQuota requests per second</td>
<td>5</td>
</tr>
<tr>
<td>Additional ListRequestedServiceQuotaChangeHistoryByQuota requests per second sent in one burst</td>
<td>5</td>
</tr>
<tr>
<td>ListServiceQuotas requests per second</td>
<td>10</td>
</tr>
<tr>
<td>Additional ListServiceQuotas requests per second sent in one burst</td>
<td>10</td>
</tr>
<tr>
<td>ListServices requests per second</td>
<td>10</td>
</tr>
<tr>
<td>Additional ListServices requests per second sent in one burst</td>
<td>10</td>
</tr>
</tbody>
</table>
### Service Quotas User Guide

#### Quota

<table>
<thead>
<tr>
<th>Quota</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListTagsForResource requests per second</td>
<td>10</td>
</tr>
<tr>
<td>ListTagsForResource requests per second sent in one burst</td>
<td>10</td>
</tr>
<tr>
<td>RequestServiceQuotaIncrease requests per second</td>
<td>3</td>
</tr>
<tr>
<td>Additional RequestServiceQuotaIncrease requests per second sent in one burst</td>
<td>3</td>
</tr>
<tr>
<td>TagResource requests per second</td>
<td>10</td>
</tr>
<tr>
<td>TagResource requests per second sent in one burst</td>
<td>10</td>
</tr>
<tr>
<td>UntagResource requests per second</td>
<td>10</td>
</tr>
<tr>
<td>UntagResource requests per second sent in one burst</td>
<td>10</td>
</tr>
</tbody>
</table>

#### Quota request template API request rates

<table>
<thead>
<tr>
<th>Quota</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssociateQuotaTemplate requests per second</td>
<td>1</td>
</tr>
<tr>
<td>Additional AssociateQuotaTemplate requests per second sent in one burst</td>
<td>1</td>
</tr>
<tr>
<td>DeleteServiceQuotaIncreaseRequestFromTemplate requests per second</td>
<td>2</td>
</tr>
<tr>
<td>Additional DeleteServiceQuotaIncreaseRequestFromTemplate requests per second sent in one burst</td>
<td>1</td>
</tr>
<tr>
<td>DisassociateQuotaTemplate requests per second</td>
<td>1</td>
</tr>
<tr>
<td>Additional DisassociateQuotaTemplate requests per second sent in one burst</td>
<td>1</td>
</tr>
<tr>
<td>GetAssociationForQuotaTemplate requests per second</td>
<td>2</td>
</tr>
<tr>
<td>Additional GetAssociationForQuotaTemplate requests per second sent in one burst</td>
<td>2</td>
</tr>
<tr>
<td>GetServiceQuotaIncreaseRequestFromTemplate requests per second</td>
<td>2</td>
</tr>
<tr>
<td>Additional GetServiceQuotaIncreaseRequestFromTemplate requests per second sent in one burst</td>
<td>1</td>
</tr>
<tr>
<td>ListServiceQuotaIncreaseRequestsInTemplate requests per second</td>
<td>2</td>
</tr>
<tr>
<td>Additional ListServiceQuotaIncreaseRequestsInTemplate requests per second sent in one burst</td>
<td>1</td>
</tr>
<tr>
<td>PutServiceQuotaIncreaseRequestIntoTemplate requests per second</td>
<td>1</td>
</tr>
<tr>
<td>Additional PutServiceQuotaIncreaseRequestIntoTemplate per second sent in one burst</td>
<td>1</td>
</tr>
</tbody>
</table>
## Service Quotas Document history

The following table describes the important changes to the documentation since the last release of Service Quotas.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published guide on GitHub</td>
<td>You can now request updates to the Service Quotas User Guide by submitting pull requests on our GitHub repository at <a href="https://github.com/awsdocs/service-quotas-user-guide">https://github.com/awsdocs/service-quotas-user-guide</a>.</td>
<td>March 23, 2021</td>
</tr>
<tr>
<td>Tagging Service Quotas resources</td>
<td>You can now attach tags to applied quotas and write policies to control access to those quotas.</td>
<td>December 21, 2020</td>
</tr>
<tr>
<td>Initial release</td>
<td>This release introduces Service Quotas.</td>
<td>June 24, 2019</td>
</tr>
</tbody>
</table>