
AWS Support

User Guide

API Version 2013-04-15



AWS Support: 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

Getting started with AWS Support	1
Features of AWS Support plans	1
Creating support cases and case management	2
Creating a support case	2
Example: Create a case for an Amazon EC2 instance	3
Describing your problem	6
Choosing a severity	6
Monitoring, resolving, and reopening cases	7
Resolving a support case	7
Reopening a resolved case	8
Creating a related case	9
Case history	10
Access permissions for AWS Support	10
AWS account	11
IAM	11
Access to AWS Trusted Advisor	12
Changing your AWS Support plan	12
Using AWS Support with an AWS SDK	12
About the AWS Support API	14
Support case management	14
Trusted Advisor	14
Endpoint	15
Support in AWS SDKs	15
Programming an AWS Support case	16
Overview	16
Using IAM with the AWS Support API	16
Create an AWS Support client	16
Discover Amazon Web Services and issue severity levels	17
Create an attachment set	18
Create a support case	19
Retrieve and update support case communications	21
Retrieve all support case information	23
Resolve a support case	24
Service quotas for the AWS Support API	24
AWS Trusted Advisor	25
Get started with AWS Trusted Advisor	25
Sign in to the Trusted Advisor console	25
View check categories	27
View specific checks	28
Filter your checks	29
Refresh check results	30
Download check results	30
Organizational view	30
Preferences	31
Organizational view for AWS Trusted Advisor	31
Prerequisites	32
Enable organizational view	32
Refresh Trusted Advisor checks	33
Create organizational view reports	33
View the report summary	35
Download an organizational view report	36
Disable organizational view	40
Using IAM policies to allow access to organizational view	41
Using other AWS services to view Trusted Advisor reports	42

Change log for AWS Trusted Advisor checks	49
Updated check name for Amazon OpenSearch Service	50
Added checks for Amazon Elastic Block Store volume storage	50
Added checks for AWS Lambda	50
Trusted Advisor check removal	51
Updated checks for Amazon Elastic Block Store	51
Trusted Advisor check removal	51
Trusted Advisor check removal	52
Using Trusted Advisor as a web service	52
Get the list of available Trusted Advisor checks	52
Refresh the list of available Trusted Advisor checks	53
Poll a Trusted Advisor check for status changes	53
Request a Trusted Advisor check result	54
Print details of a Trusted Advisor check	55
Trusted Advisor check reference	56
Cost optimization	56
Amazon Comprehend Underutilized Endpoints	57
Amazon EC2 Reserved Instance Lease Expiration	57
Amazon EC2 Reserved Instance Optimization	57
Amazon ElastiCache Reserved Node Optimization	58
Amazon OpenSearch Service Reserved Instance Optimization	58
Amazon RDS Idle DB Instances	59
Amazon Redshift Reserved Node Optimization	59
Amazon Relational Database Service (RDS) Reserved Instance Optimization	59
Amazon Route 53 Latency Resource Record Sets	60
AWS Lambda Functions with Excessive Timeouts	60
AWS Lambda Functions with High Error Rates	60
Idle Load Balancers	60
Low Utilization Amazon EC2 Instances	61
Savings Plan	61
Unassociated Elastic IP Addresses	61
Underutilized Amazon EBS Volumes	62
Underutilized Amazon Redshift Clusters	62
Performance	62
Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration	63
Amazon EC2 to EBS Throughput Optimization	63
Amazon Route 53 Alias Resource Record Sets	63
CloudFront Alternate Domain Names	64
CloudFront Content Delivery Optimization	64
CloudFront Header Forwarding and Cache Hit Ratio	64
High Utilization Amazon EC2 Instances	64
Large Number of EC2 Security Group Rules Applied to an Instance	65
Large Number of Rules in an EC2 Security Group	65
Overutilized Amazon EBS Magnetic Volumes	65
Security	65
Amazon EBS Public Snapshots	66
Amazon RDS Public Snapshots	66
Amazon RDS Security Group Access Risk	67
Amazon Route 53 MX Resource Record Sets and Sender Policy Framework	67
Amazon S3 Bucket Permissions	67
AWS CloudTrail Logging	67
AWS Lambda Functions Using Deprecated Runtimes	68
CloudFront Custom SSL Certificates in the IAM Certificate Store	68
CloudFront SSL Certificate on the Origin Server	68
ELB Listener Security	69
ELB Security Groups	69
Exposed Access Keys	69

IAM Access Key Rotation	70
IAM Password Policy	70
IAM Use	70
MFA on Root Account	70
Security Groups – Specific Ports Unrestricted	71
Security Groups – Unrestricted Access	71
Fault tolerance	71
Amazon Aurora DB Instance Accessibility	72
Amazon Comprehend Endpoint Access Risk	72
Amazon EBS Snapshots	72
Amazon EC2 Availability Zone Balance	73
Amazon RDS Backups	73
Amazon RDS Multi-AZ	73
Amazon Route 53 Deleted Health Checks	73
Amazon Route 53 Failover Resource Record Sets	74
Amazon Route 53 High TTL Resource Record Sets	74
Amazon Route 53 Name Server Delegations	74
Amazon S3 Bucket Logging	75
Amazon S3 Bucket Versioning	75
Auto Scaling Group Health Check	75
Auto Scaling Group Resources	76
AWS Direct Connect Connection Redundancy	76
AWS Direct Connect Location Redundancy	76
AWS Direct Connect Virtual Interface Redundancy	77
AWS Lambda VPC-enabled Functions without Multi-AZ Redundancy	77
ELB Connection Draining	77
ELB Cross-Zone Load Balancing	77
Load Balancer Optimization	78
VPN Tunnel Redundancy	78
Service limits	78
Auto Scaling Groups	80
Auto Scaling Launch Configurations	80
CloudFormation Stacks	80
DynamoDB Read Capacity	80
DynamoDB Write Capacity	80
EBS Active Snapshots	81
EBS Cold HDD (sc1) Volume Storage	81
EBS General Purpose SSD (gp2) Volume Storage	81
EBS General Purpose SSD (gp3) Volume Storage	81
EBS Magnetic (standard) Volume Storage	81
EBS Provisioned IOPS (SSD) Volume Aggregate IOPS	82
EBS Provisioned IOPS SSD (io1) Volume Storage	82
EBS Provisioned IOPS SSD (io2) Volume Storage	82
EBS Throughput Optimized HDD (st1) Volume Storage	82
EC2 On-Demand Instances	82
EC2 Reserved Instance Leases	83
EC2-Classic Elastic IP Addresses	83
EC2-VPC Elastic IP Address	83
ELB Application Load Balancers	83
ELB Classic Load Balancers	83
ELB Network Load Balancers	83
IAM Group	84
IAM Instance Profiles	84
IAM Policies	84
IAM Roles	84
IAM Server Certificates	84
IAM Users	85

Kinesis Shards per Region	85
RDS Cluster Parameter Groups	85
RDS Cluster Roles	85
RDS Clusters	85
RDS DB Instances	85
RDS DB Manual Snapshots	86
RDS DB Parameter Groups	86
RDS DB Security Groups	86
RDS Event Subscriptions	86
RDS Max Auths per Security Group	86
RDS Option Groups	87
RDS Read Replicas per Master	87
RDS Reserved Instances	87
RDS Subnet Groups	87
RDS Subnets per Subnet Group	87
RDS Total Storage Quota	87
Route 53 Hosted Zones	88
Route 53 Max Health Checks	88
Route 53 Reusable Delegation Sets	88
Route 53 Traffic Policies	88
Route 53 Traffic Policy Instances	88
SES Daily Sending Quota	89
VPC	89
VPC Internet Gateways	89
Security	90
Data protection	90
Identity and access management	91
Audience	91
Authenticating with identities	92
Managing access using policies	93
How AWS Support works with IAM	95
Identity-based policy examples	96
Using service-linked roles	98
AWS managed policies	102
Manage access for AWS Trusted Advisor	107
Troubleshooting	111
Incident response	113
Monitoring AWS Support	113
Logging AWS Support API calls with AWS CloudTrail	113
Logging AWS Trusted Advisor console actions with AWS CloudTrail	118
Monitoring Trusted Advisor checks	122
Compliance validation	133
Resilience	134
Infrastructure security	134
Configuration and vulnerability analysis	134
Troubleshooting resources	135
Service-specific troubleshooting	135
Document history	137
Earlier updates	138
AWS glossary	141

Getting started with AWS Support

AWS Support offers a range of plans that provide access to tools and expertise that support the success and operational health of your AWS solutions. All support plans provide 24/7 access to customer service, AWS documentation, technical papers, and support forums. For technical support and more resources to plan, deploy, and improve your AWS environment, you can choose a support plan that best aligns with your AWS use case.

Notes

- For more information about the different AWS Support plans, see [Compare AWS Support plans](#).
- To create a support case in the AWS Management Console, see [Creating a support case \(p. 2\)](#).

Topics

- [Features of AWS Support plans \(p. 1\)](#)
- [Creating support cases and case management \(p. 2\)](#)
- [Monitoring, resolving, and reopening your case \(p. 7\)](#)
- [Access permissions for AWS Support \(p. 10\)](#)
- [Changing your AWS Support plan \(p. 12\)](#)
- [Using AWS Support with an AWS SDK \(p. 12\)](#)

Features of AWS Support plans

AWS Support offers four support plans: Basic, Developer, Business, and Enterprise.

Basic Support offers support for account and billing questions and service quota increases. The other plans offer a number of technical support cases with pay-by-the-month pricing and no long-term contracts.

All AWS customers automatically have 24/7 access to these features of Basic Support:

- One-on-one responses to account and billing questions
- Support forums
- Service health checks
- Documentation, technical papers, and best practice guides

Customers with a Developer Support plan have access to these additional features:

- Best practice guidance
- Building-block architecture support: guidance on how to use AWS products, features, and services together
- Supports an unlimited number of support cases that can be opened by one primary contact, which is the [AWS account root user](#).

In addition, customers with a Business Support or Enterprise Support plan have access to these features:

- Use-case guidance – What AWS products, features, and services to use to best support your specific needs.

- [AWS Trusted Advisor \(p. 25\)](#) – A feature of AWS Support, which inspects customer environments and identifies opportunities to save money, close security gaps, and improve system reliability and performance. You can access all Trusted Advisor checks.
- The AWS Support API to interact with Support Center and Trusted Advisor. You can use the AWS Support API to automate support case management and Trusted Advisor operations.
- Third-party software support – Help with Amazon Elastic Compute Cloud (Amazon EC2) instance operating systems and configuration. Also, help with the performance of the most popular third-party software components on AWS. Third-party software support isn't available for customers on Basic or Developer Support plans.
- Supports an unlimited number of AWS Identity and Access Management (IAM) users who can open technical support cases.

In addition, customers with an Enterprise Support plan have access to these features:

- Application architecture guidance – Contextual guidance on how services fit together to meet your specific use case, workload, or application.
- Infrastructure event management – Short-term engagement with AWS Support to get a deep understanding of your use case. After analysis, provide architectural and scaling guidance for an event.
- Technical account manager – Work with a technical account manager (TAM) for your specific use cases and applications.
- White-glove case routing.
- Management business reviews.

For more information about features and pricing for each support plan, see [AWS Support](#) and [Compare AWS Support plans](#). Some features, such as 24/7 phone and chat support, aren't available in all languages.

Creating support cases and case management

In the AWS Management Console, you can create three types of customer cases in AWS Support:

- **Account and billing support** cases are available to all AWS customers. You can get help with billing and account questions.
- **Service limit increase** requests are available to all AWS customers. For more information about the default service quotas, formerly referred to as limits, see [AWS service quotas](#) in the *AWS General Reference*.
- **Technical support** cases connect you to technical support for help with service-related technical issues and, in some cases, third-party applications. If you have a Developer Support plan, you can communicate by using email and the Support Center. If you have a Business or Enterprise Support plan, you can also communicate by phone or live chat.

Note

- If you have Basic Support, you can't create a technical support case.
- To change your support plan, see [Changing your AWS Support plan \(p. 12\)](#).
- To close your account, see [Closing an Account](#) in the *AWS Billing and Cost Management User Guide*.

Creating a support case

You can create a support case in the Support Center of the AWS Management Console.

Notes

- You can sign in to Support Center as the *root user* of your AWS account or as an AWS Identity and Access Management (IAM) user. For more information, see [Access permissions for AWS Support \(p. 10\)](#).
- If you can't sign in to Support Center and create a support case, you can use the [Contact Us](#) page instead. You can use this page to get help with billing and account issues.

To create a support case

1. Sign in to the [AWS Management Console](#).
2. In the upper-right corner, choose **Support**, and then choose **Support Center**.
3. Choose **Create case**.
4. Choose one of the following options:
 - **Account and billing support**
 - **Service limit increase**
 - **Technical support**
5. Follow the prompts to describe your case, such as the following:
 - Error messages that you received
 - Troubleshooting steps that you followed
 - How you're accessing the service:
 - AWS Management Console
 - AWS Command Line Interface (AWS CLI)
 - API operations
6. Choose **Submit**. Your case ID number and summary appear.

Example: Create a case for an Amazon EC2 instance

As shown in the following screenshot, this example is a technical support case for an Amazon Elastic Compute Cloud (Amazon EC2) instance.

Support Center > Create case

Create case [Info](#)

1
Account and billing support ☐
Assistance with account and billing-related enquiries

Service limit increase ☐
Requests to increase the service limit of your AWS resources

Technical support ☒
Service-related technical issues and third-party applications

Case classification

2
Service
Elastic Compute Cloud (EC2 - Linux) ▼

3
Category
Instance Issue ▼

4
Severity [Info](#)
General guidance ▼

Instance ID(s) - optional
i-xxxxxxx

1. **Create case** – Choose the type of case to create from the three boxes at the top of the page. In this example, the case type is **Technical support**.

Note

If you have the Basic Support plan, you can't create a technical support case.

2. **Service** – If your question affects multiple services, choose the service that's most applicable. In this example, the service is **Elastic Compute Cloud (EC2 - Linux)**.
3. **Category** – Choose the category that best fits your use case. In this example, there's trouble connecting to an instance, so **Instance Issue** is chosen. When you choose a category, links to information that might resolve your problem appear below the **Case classification** section.
4. **Severity** – Customers with a paid support plan can choose the **General guidance** (1-day response time) or **System impaired** (12-hour response time) severity level. Customers with a Business Support plan can also choose **Production system impaired** (4-hour response) or **Production system down** (1-hour response). Customers with Enterprise Support can choose **Business-critical system down** (15-minute response).


Response times are for first response from AWS Support. These response times don't apply to subsequent responses. For third-party issues, response times can be longer, depending on the availability of skilled personnel. For more information, see [Choosing a severity \(p. 6\)](#).

Note

Based on your category choice, you might be prompted for more information. In this example, you're prompted to enter the **Instance ID**. As a best practice, enter resource IDs, even when not prompted.

After you specify the case type and classification, you can specify the description and how you want to be contacted.

Case description

**Assistance**
For troubleshooting ideas, see [Troubleshooting Instances](#).

If you are receiving an error, provide the detailed error message and a description of any changes that you may have made recently. Include the date, time, and time zone that you first observed the issue.

1 Subject

Failed status checks

Maximum 250 characters (230 remaining)

2 Description

One of my instances (i-xxxxxxx) is uncontactable and began failing status checks as of 2019-01-06 1540 UTC. See my attached screenshot.


I performed several software updates this week, and also implemented some network adapter and firewall changes to this instance. My application automatically replaced this instance when it failed, but I would like to analyze the failure to make sure that I don't repeat it.

Would my recent changes have caused this?

Maximum 5000 characters (4546 remaining)

3 Attachments

Provide more details with text, image or PDFs

 Choose files

failedStatus.png

Up to 3 attachments, each less than 5MB

▼ Contact options

4 Preferred contact language

English

5 Contact methods [Info](#)

Web

Via email and Support Center

We will get back to you within 24 hours

Chat

Chat online with a representative

Phone

We call you back at your number

6 Additional contacts - optional [Info](#)

When we contact you via email, we will copy the correspondence to the following email addresses

Email addresses

Use commas or semicolons to separate email addresses - Maximum 200 characters (200 remaining)

7

Cancel Submit

1. **Subject** – Enter a title that briefly describes your issue. In this example, the subject is **Failed status checks**.
2. **Description** – This is the most important information that you provide to AWS Support. For most service and category combinations, a prompt suggests information that's most helpful for the fastest resolution. For more information, see [Describing your problem \(p. 6\)](#).
3. **Attachments** – Screenshots and other attachments (less than 5 MB each) can be helpful. In this example, the attached image is a failed status check.
4. **Preferred contact language** – Currently, you can choose English or Japanese.
5. **Contact methods** – Choose a contact method. The options depend on the type of case and your support plan. If you choose **Web**, you can read and respond to the case progress in Support Center.

API Version 2013-04-15

5

If you have a Business or Enterprise Support plan, you can also choose **Chat** or **Phone**. If you choose **Phone**, you're prompted for a callback number.

6. **Additional contacts** – Enter the email addresses of people to be notified when the status of the case changes. If you're signed in as an IAM user, include your email address. If you're signed in with your email address and password, you don't need to include your email address.

Note

If you have the Basic Support plan, the **Additional contacts** box isn't available. However, the **Operations** contact specified in the **Alternate Contacts** section of the [My Account](#) page receives copies of the case correspondence, but only for the specific case types of account and billing, and technical.

7. Choose **Submit** when your information is complete and you're ready to create the case.

Describing your problem

Make your description as detailed as possible. Include relevant resource information, along with anything else that might help us understand your issue. For example, to troubleshoot performance, include timestamps and logs. For feature requests or general guidance questions, include a description of your environment and purpose. In all cases, follow the **Description Guidance** that appears on your case submission form.

When you provide as much detail as possible, you increase the chances that your case can be resolved quickly.

Choosing a severity

You might be inclined to always create a support case at the highest severity that your support plan allows. However, we recommend that you choose the highest severities for cases that can't be worked around or that directly affect production applications. For information about building your services so that losing single resources doesn't affect your applications, see the [Building Fault-Tolerant Applications on AWS](#) technical paper.

The following table lists the severity levels, response times, and example problems.

Note

You can't change the severity code for a support case after you create one. If your situation changes, work with the AWS Support associate for your support case.

Severity	First-response time	Description and support plan
General guidance	24 hours	You have a general development question, or you want to request a feature. (Developer*, Business, and Enterprise Support plans)
System impaired	12 hours	Non-critical functions of your application are behaving abnormally, or you have a time-sensitive development question. (Developer*, Business, and Enterprise Support plans)
Production system impaired	4 hours	Important functions of your application are impaired or degraded. (Business and Enterprise Support plans)
Production system down	1 hour	Your business is significantly impacted. Important functions of your application aren't available. (Business and Enterprise Support plans)

Severity	First-response time	Description and support plan
Business-critical system down	15 minutes	Your business is at risk. Critical functions of your application aren't available. (Enterprise Support plan)

* For Developer Support, response targets are calculated in business hours. Business hours are defined as 08:00 AM to 6:00 PM in the customer country, excluding holidays and weekends. This information appears in the **Contact Information** section of the [My Account](#) page in the AWS Management Console. These times can vary in countries with multiple time zones. Japanese support is available from 9:00 AM to 6:00 PM.

Note

We make every reasonable effort to respond to your initial request within the indicated timeframe. For more information about the scope of support for each AWS Support plan, see [AWS Support features](#).

Monitoring, resolving, and reopening your case

After you create your support case, you can monitor the status of your case in Support Center. A new case begins in the **Unassigned** state. When a support agent begins work on a case, the status changes to **Work in Progress**. The support agent might respond to your case to ask for more information (**Pending Customer Action**) or to let you know that the case is being investigated (**Pending Amazon Action**).

When your case is updated, you receive email with the correspondence and a link to the case in Support Center. Use the link in the email message to navigate to the support case. You can't respond to case correspondences by email.

Notes

- You must sign in to the AWS account that submitted the support case. If you sign in as an AWS Identity and Access Management (IAM) user, you must have the required permissions to view support cases. For more information, see [Access permissions for AWS Support \(p. 10\)](#).
- If you don't respond to the case within a few days, AWS Support resolves the case automatically.
- Support cases that have been in the resolved state for more than 14 days can't be reopened. If you have a similar issue that is related to the resolved case, you can create a related case. For more information, see [Creating a related case \(p. 9\)](#).

Topics

- [Resolving a support case \(p. 7\)](#)
- [Reopening a resolved case \(p. 8\)](#)
- [Creating a related case \(p. 9\)](#)
- [Case history \(p. 10\)](#)

Resolving a support case

When you're satisfied with the response or your problem is solved, you can resolve the case in Support Center.

To resolve a support case

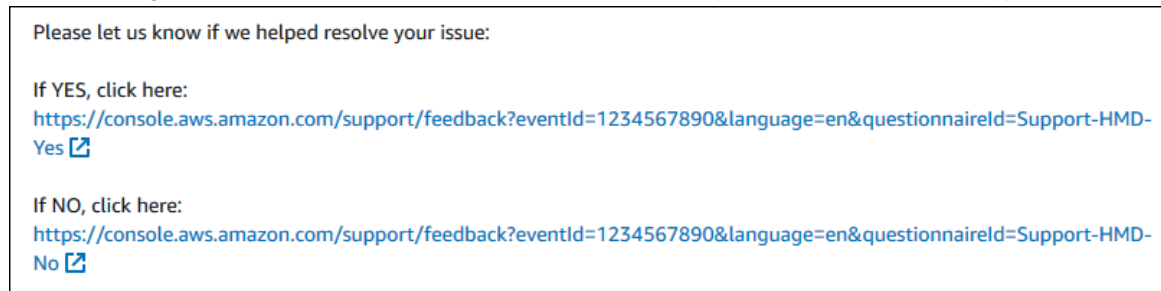
1. Sign in to the [AWS Management Console](#).
2. In the upper-right corner, choose **Support**, and then choose **Support Center**.
3. Under **Open support cases**, choose the **Subject** of the support case that you want to resolve.
4. (Optional) Choose **Reply** and in the **Correspondence** section, enter why you're resolving the case, and then choose **Submit**. For example, you can enter information about how you fixed the issue yourself in case you need this information for future reference.
5. Choose **Resolve case**.
6. In the dialog box, choose **Ok** to resolve the case.

Note

If AWS Support resolved your case for you, you can use the feedback link to provide more information about your experience with AWS Support.

Example : Feedback links

The following screenshot shows the feedback links in the correspondence of a case in Support Center.



Reopening a resolved case

If you're experiencing the same issue again, you can reopen the original case. Provide details about when the issue occurred again and what troubleshooting steps that you tried. Include any related case numbers so that the support agent can refer to previous correspondences.

Notes

- You can reopen your support case up to 14 days from when your issue was resolved. However, you can't reopen a case that has been inactive for more than 14 days. You can create a new case or a related case. For more information, see [Creating a related case \(p. 9\)](#).
- If you reopen an existing case that has different information than your current issue, the support agent might ask you to create a new case.

To reopen a resolved case

1. Sign in to the [AWS Management Console](#).
2. In the upper-right corner, choose **Support**, and then choose **Support Center**.
3. Choose **View all cases** and then choose the **Subject** or the **Case ID** of the support case that you want to reopen.
4. Choose **Reopen case**.
5. Under **Correspondence**, for **Reply**, enter the case details.
6. (Optional) Choose **Choose files** to attach files to your case. You can attach up to 3 files.
7. For **Contact methods**, choose one of the following options:

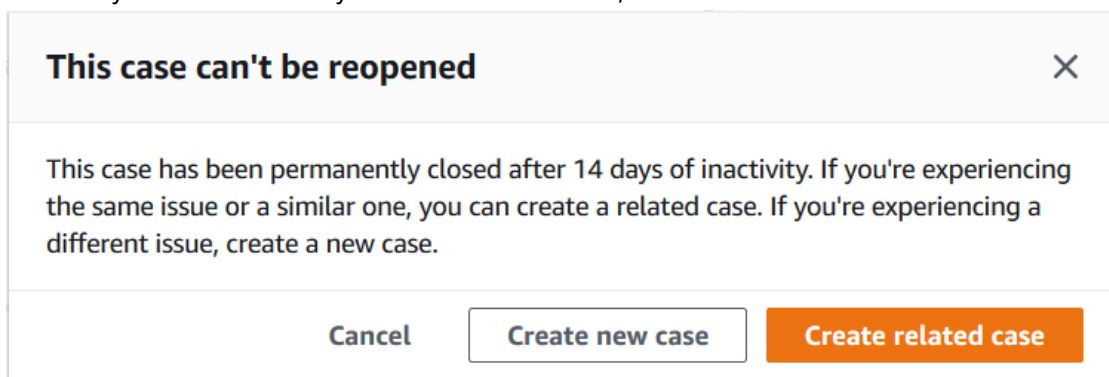
- **Web** – Get notified by email and the Support Center.
 - **Chat** – Chat online with a support agent.
 - **Phone** – Receive a phone call from a support agent.
8. (Optional) For **Additional contacts**, enter email addresses for other people that you want to receive case correspondences.
 9. Review your case details and choose **Submit**.

Creating a related case

After 14 days of inactivity, you can't reopen a resolved case. If you have a similar issue that is related to the resolved case, you can create a related case. This related case will include a link to the previously resolved case, so that the support agent can review the previous case details and correspondences. If you're experiencing a different issue, we recommend that you create a new case.

To create a related case

1. Sign in to the [AWS Management Console](#).
2. In the upper-right corner, choose **Support** and then choose **Support Center**.
3. Choose **View all cases** and then choose the **Subject** or the **Case ID** of the support case that you want to reopen.
4. Choose **Reopen case**.
5. In the dialog box, choose **Create related case**. The previous case information will be automatically added to your related case. If you have a different issue, choose **Create new case**.



This case can't be reopened ✕

This case has been permanently closed after 14 days of inactivity. If you're experiencing the same issue or a similar one, you can create a related case. If you're experiencing a different issue, create a new case.

Cancel Create new case Create related case

6. Follow the same steps to create your case. See [Creating a support case \(p. 2\)](#).

Note

By default, your related case has the same **Type**, **Category**, and **Severity** of the previous case. You can update the case details as needed.

7. Review your case details and choose **Submit**.

After you create your case, the previous case appears in the **Related cases** section, such as in the following example.

Case ID 234567891

Info

Resolve case

Case details

Subject

Same issue is happening for my Amazon EC2 instances

Case ID

234567891

Created

2021-04-21T20:30:23.945Z

Case type

Account

Opened by

janedoe@example.com

Status

Unassigned

Severity

General question

Category

General Info and Getting Started

Additional contacts

john.doe@example.com

Related cases

Subject

Case ID

Problem with EC2 instances

1234567890

Correspondence

Reply

Jane Doe

Wed Apr 21 2021
13:30:23 GMT-0700
(Pacific Daylight Time)

I keep getting an error for my EC2 instances. What do you recommend that I do to fix it?

Case history

You can view case history information up to 12 months after you create a case.

Access permissions for AWS Support

You must have permissions to access Support Center and to [create a support case \(p. 2\)](#).

You can use one of the following options to access Support Center:

- Use the email address and password associated with your AWS account. This identity is called the AWS account *root user*.
- Use AWS Identity and Access Management (IAM).

If you have a Business or Enterprise Support plan, you can also use the [AWS Support API \(p. 14\)](#) to access AWS Support and Trusted Advisor operations programmatically. For more information, see the [AWS Support API Reference](#).

Note

If you can't sign in to Support Center, you can use the [Contact Us](#) page instead. You can use this page to get help with billing and account issues.

AWS account

You can sign in to the AWS Management Console and access the Support Center by using your AWS account email address and password. This identity is called the AWS account *root user*. However, we strongly recommend that you don't use the root user for your everyday tasks, even the administrative ones. Instead, we recommend that you use IAM, which lets you control who can perform certain tasks in your account.

IAM

By default, IAM users can't access the Support Center. You can use IAM to create individual users or groups. Then, you attach IAM policies to these entities, so that they have permission to perform actions and access resources, such as to open Support Center cases and use the AWS Support API.

After you create IAM users, you can give those users individual passwords and an account-specific sign-in page. They can then sign in to your AWS account and work in the Support Center. IAM users who have AWS Support access can see all cases that are created for the account.

For more information, see [How IAM users sign in to your AWS account](#) in the *IAM User Guide*.

The easiest way to grant permissions is to attach the AWS managed policy [AWSSupportAccess](#) to the user, group, or role. AWS Support allows action-level permissions to control access to specific AWS Support operations. AWS Support doesn't provide resource-level access, so the *Resource* element is always set to *. You can't allow or deny access to specific support cases.

Example : Allow access to all AWS Support actions

The AWS managed policy [AWSSupportAccess](#) grants an IAM user access to AWS Support. An IAM user with this policy can access all AWS Support operations and resources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["support:*"],
      "Resource": "*"
    }
  ]
}
```

For more information about how to attach the `AWSSupportAccess` policy to your entities, see [Adding IAM identity permissions \(console\)](#) in the *IAM User Guide*.

Example : Allow access to all actions except the `ResolveCase` action

You can also create *customer managed policies* in IAM to specify what actions to allow or deny. The following policy statement allows an IAM user to perform all actions in AWS Support except resolve a case.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
    "Action": "support:*",
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": "support:ResolveCase",
    "Resource": "*"
  }
]
```

For more information about how to create a customer managed IAM policy, see [Creating IAM policies \(console\)](#) in the *IAM User Guide*.

If the user or group already has a policy, you can add the AWS Support-specific policy statement to that policy.

Important

- If you can't view cases in the Support Center, make sure that you have the required permissions. You might need to contact your IAM administrator. For more information, see [Identity and access management for AWS Support \(p. 91\)](#).

Access to AWS Trusted Advisor

In the AWS Management Console, a separate `trustedadvisor` IAM namespace controls access to Trusted Advisor. In the AWS Support API, the `support` IAM namespace controls access to Trusted Advisor. For more information, see [Manage access for AWS Trusted Advisor \(p. 107\)](#).

Changing your AWS Support plan

You can change your support plan in the AWS Management Console.

To change your support plan

1. Sign in to the AWS Management Console with your root account credentials at <https://console.aws.amazon.com/support/plans/home>.
2. On the **Support plans** page, choose **Change plan**.
3. On the **Change support plan** page, choose your **New plan**, review the plan information, and then choose **Change plan**.

For an example video of how to change your support plan, see [How do I change my AWS Support plan?](#)

Notes

If you have Enterprise Support, use the link on the **Change support plan** page to contact AWS Support.

- To close your account, see [Closing an Account](#) in the *AWS Billing and Cost Management User Guide*.

Using AWS Support with an AWS SDK

AWS software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language.

SDK documentation	Code examples
AWS SDK for C++	AWS SDK for C++ code examples
AWS SDK for Go	AWS SDK for Go code examples
AWS SDK for Java	AWS SDK for Java code examples
AWS SDK for JavaScript	AWS SDK for JavaScript code examples
AWS SDK for .NET	AWS SDK for .NET code examples
AWS SDK for PHP	AWS SDK for PHP code examples
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) code examples
AWS SDK for Ruby	AWS SDK for Ruby code examples

Example availability

Can't find what you need? Request a code example with the feedback link.

About the AWS Support API

The AWS Support API provides access to some of the features in the [AWS Support Center](#).

The API provides two different groups of operations:

- [Support case management \(p. 14\)](#) operations to manage the entire life cycle of your AWS support cases, from creating a case to resolving it
- [Trusted Advisor \(p. 14\)](#) operations to access [AWS Trusted Advisor \(p. 25\)](#) checks

Note

You must have a Business or Enterprise Support plan to use the AWS Support API. For more information, see [AWS Support](#).

For more information about the operations and data types provided by AWS Support, see the [AWS Support API Reference](#).

Topics

- [Support case management \(p. 14\)](#)
- [Trusted Advisor \(p. 14\)](#)
- [Endpoint \(p. 15\)](#)
- [Support in AWS SDKs \(p. 15\)](#)

Support case management

You can use the API to perform the following tasks:

- Open a support case
- Get a list and detailed information about recent support cases
- Filter your search for support cases by dates and case identifiers, including resolved cases
- Add communications and file attachments to your cases, and add the email recipients for case correspondences
- Resolve your cases

The AWS Support API supports CloudTrail logging for support case management operations. For more information, see [Logging AWS Support API calls with AWS CloudTrail \(p. 113\)](#).

For example Java code that demonstrates how to manage the entire life cycle of a support case, see [Programming an AWS Support case \(p. 16\)](#).

Trusted Advisor

You can use the Trusted Advisor operations to perform the following tasks:

- Get the names and identifiers for the Trusted Advisor checks
- Request that a Trusted Advisor check be run against your AWS account and resources
- Get summaries and detailed information for your Trusted Advisor check results

- Refresh your Trusted Advisor checks
- Get the status of each Trusted Advisor check

The AWS Support API supports CloudTrail logging for Trusted Advisor operations. For more information, see [AWS Trusted Advisor information in CloudTrail logging \(p. 114\)](#).

You can use Amazon CloudWatch Events to monitor for changes to your check results for Trusted Advisor. For more information, see [Monitoring Trusted Advisor check results with Amazon CloudWatch Events \(p. 123\)](#).

For example Java code that demonstrates how to use the Trusted Advisor operations, see [Using Trusted Advisor as a web service \(p. 52\)](#).

Endpoint

You can use the following endpoint to access the AWS Support API:

- <https://support.us-east-1.amazonaws.com>

Important

The AWS Support endpoint creates cases in the production database. If you're creating test support cases, we recommend that you include a subject line, such as **TEST CASE-Please ignore**, when you call the [CreateCase](#) operation. After you're done testing, call the [ResolveCase](#) operation to resolve the case.

For more information about using AWS endpoints, see [Regions and endpoints](#) in the *Amazon Web Services General Reference*.

Support in AWS SDKs

The AWS Command Line Interface (AWS CLI), and the AWS Software Development Kits (SDKs) include support for the AWS Support API.

For a list of languages that support the AWS Support API, choose an operation name, such as [CreateCase](#), and in the [See Also](#) section, choose your preferred language.

Programming an AWS Support case

You can use the AWS Support API to create support cases programmatically instead of using the AWS Support Center in the AWS Management Console. You can add correspondences and attach files to your case, so that support agents can investigate and help resolve your issue. This topic provides examples of how to use the AWS Support API operations.

Notes

- For a list of API operations, parameters, and data types that you can use for AWS Support, see the [AWS Support API Reference](#).
- For a list of languages that support the AWS Support API, choose an operation name, such as [CreateCase](#), and in the [See Also](#) section, choose your preferred language.

Topics

- [Overview \(p. 16\)](#)
- [Create an AWS Support client \(p. 16\)](#)
- [Discover Amazon Web Services and issue severity levels \(p. 17\)](#)
- [Create an attachment set \(p. 18\)](#)
- [Create a support case \(p. 19\)](#)
- [Retrieve and update support case communications \(p. 21\)](#)
- [Retrieve all support case information \(p. 23\)](#)
- [Resolve a support case \(p. 24\)](#)
- [Service quotas for the AWS Support API \(p. 24\)](#)

Overview

This topic uses Java code examples to demonstrate the use of AWS Support. For more information about SDK support, see [Sample code & libraries](#).

Note

If you exceed service quotas for your calls to AWS Support, see the following information:

- [Service quotas for the AWS Support API \(p. 24\)](#)
- [Error retries and exponential backoff in AWS](#) in the *AWS General Reference*

Using IAM with the AWS Support API

AWS Identity and Access Management (IAM) is supported by the AWS Support API. For more information, see [Access permissions for AWS Support \(p. 10\)](#).

Create an AWS Support client

The following Java code snippet shows how to create an `AWSSupportClient`, which is used to call the `AWSSupportService`. The `createClient` method gets AWS credentials by calling the

`AWSSupportClient()` constructor with no parameters, which retrieves credentials from the credentials provider chain. For more information about this process, see [Tutorial: Grant access using an IAM role and the AWS SDK for Java](#) in the *AWS SDK for Java*.

For more information about AWS credentials, see [AWS security credentials](#) in the *AWS General Reference*.

```
private static AWSSupportClient createClient()
{
    AWSSupportClient client = new AWSSupportClient();
    client.setEndpoint("https://support.us-east-1.amazonaws.com");
    return client;
}
```

Discover Amazon Web Services and issue severity levels

The AWS Support Java client provides a `CreateCaseRequest` type to submit a case programmatically to AWS Support. The `CreateCaseRequest` structure is populated with the request parameters and then passed to the `createClient` method on the `AWSSupportClient` instance. These parameters include codes that specify the AWS service and case severity.

The following Java code snippet demonstrates calls to the AWS Support [DescribeServices](#) and [DescribeSeverityLevel](#) operations.

```
// DescribeServices example

public static void getServiceCodes(AWSSupportClient client)
{
    DescribeServicesResult result = client.describeServices();
    for (Service service : result.getServices())
    {
        System.out.println("Service code (name): " +
            service.getCode() + "(" + service.getName() + ")");
        for (Category category : service.getCategories())
        {
            System.out.println("    Category code (name): " +
                category.getCode() + "(" + category.getName() + ")");
        }
    }
}

// DescribeSeverityLevels example

public static void getSeverityLevels(AWSSupportClient client)
{
    DescribeSeverityLevelsResult result = client.describeSeverityLevels();
    for (SeverityLevel level : result.getSeverityLevelsList())
    {
        System.out.println("Severity level (name): " +
            level.getCode() + level.getName() + ");");
    }
}
```

Each call returns a list of JSON-formatted objects. `DescribeServices` returns service codes and their corresponding names, and `DescribeSeverityLevels` returns severity levels and their corresponding names. In addition, `DescribeServices` also returns a list of AWS Support categories that apply to each AWS service. These categories are also used to open a support case by using the [CreateCase](#) operation.

Although these values can also be obtained from the AWS Support site, the AWS Support service always returns the most recent version of this information.

Create an attachment set

To attach files to the case, you must add the attachments to an attachment set before creating the case. You can add up to three attachments to an attachment set, and the maximum size of any attachment in the set is 5 MB. For more information, see [AddAttachmentsToSet](#).

The following Java code snippet creates a text file attachment, adds it to an attachment set, and then gets the ID of the attachment set for adding to the case.

```
public static String createAttachmentSet() throws IOException
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));

    // Get content and file name for an attachment.
    System.out.println("Enter text content for an attachment to the case: ");
    String attachmentcontent = null;
    try
    {
        attachmentcontent = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    System.out.println("Enter the file name for the attachment: ");
    String attachmentfilename = null;
    try
    {
        attachmentfilename = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    // Create the attachment.
    Attachment attachment1 = new Attachment();
    attachment1.setData(ByteBuffer.wrap(attachmentcontent.getBytes()));
    attachment1.setFileName("attachmentfilename");

    // Add the attachment to an array list.
    List<Attachment> attachments = new ArrayList<Attachment>();
    attachments.add(attachment1);

    // Create an attachment set and add the attachment array list to it.
    AddAttachmentsToSetRequest addAttachmentsToSetRequest =
        new AddAttachmentsToSetRequest();
    addAttachmentsToSetRequest.setAttachments(attachments);

    AddAttachmentsToSetResult addAttachmentsToSetResult =
        client.addAttachmentsToSet(addAttachmentsToSetRequest);

    // Get the ID of the attachment set.
    String attachmentsetid = addAttachmentsToSetResult.getAttachmentSetId();
    System.out.println("Attachment ID: " + attachmentsetid);
}
```



```
    return attachmentsetid;  
}
```

Create a support case

To create an AWS Support case using the AWS Support service, populate a `CreateCaseRequest` instance with the following information:

- `ServiceCode` – The AWS Support service code that you obtained by calling the `DescribeServices` operation, as described in the previous section.
- `CategoryCode` – The category code that describes the type of issue the support case concerns.
- `Language` – A code for the language that AWS Support provides support in. Currently, AWS supports English (en) and Japanese (ja).
- `CcEmailAddresses` – A list of email addresses to receive copies of subsequent communications.
- `CommunicationBody` – Text for the body of the initial case submission.
- `Subject` – A title for the support case.
- `SeverityCode` – One of the values returned by the call to `DescribeSeverityLevels`.
- `AttachmentSetId` – (Optional) The ID of a set of file attachments to include with the case. The `AddAttachmentsToSet` operation returns the ID.

The following Java code snippet collects values for each of the case creation parameters from the command line. It then populates a `CreateCaseRequest` instance and passes them to AWS Support by calling the `createCase` method on an `AWSSupportClient` instance. If the call is successful, it returns an AWS Support `CaseId` value in the following format.

```
case-123456789012-muen-2012-74a757cd8cf7558a
```

Note

AWS Support provides both `CaseId` and `DisplayId` fields. The `DisplayId` field corresponds to the case number that is displayed on the AWS Support site. The `CaseId` field is for use in programmatic interactions with the AWS Support service. Both fields are exposed on the `CaseDetails` data type.

```
public static void createCase(AWSSupportClient client) throws IOException  
{  
    BufferedReader reader =  
        new BufferedReader(new InputStreamReader(System.in));  
  
    System.out.println("Enter an AWS service code: ");  
    String servicecode = null;  
    try  
    {  
        servicecode = reader.readLine().trim();  
    }  
    catch (IOException e)  
    {  
        e.printStackTrace();  
        System.exit(1);  
    }  
  
    System.out.println("Enter a category code: ");  
    String categorycode = null;  
    try  
    {  
        categorycode = reader.readLine().trim();  
    }  
}
```

```
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter a language code, 'en' for English: ");
String language = null;
try
{
    language = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter an email address to copy on correspondence: ");
String ccemailaddress = null;
try
{
    ccemailaddress = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter body text for the case: ");
String communicationbody = null;
try
{
    communicationbody = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter a subject for the case: ");
String casesubject = null;
try
{
    casesubject = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter the severity code for the case: ");
String severitycode = null;
try
{
    severitycode = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}
```

```
System.out.println("Enter the attachment set ID for the case: ");
String attachmentsetid = null;
try
{
    attachmentsetid = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

CreateCaseRequest request = new CreateCaseRequest()
    .withServiceCode(servicecode)
    .withCategoryCode(categorycode)
    .withLanguage(language)
    .withCcEmailAddresses(ccemailaddress)
    .withCommunicationBody(communicationbody)
    .withSubject(casesubject)
    .withSeverityCode(severitycode)
    .withAttachmentSetId(attachmentsetid);

CreateCaseResult result = client.createCase(request);
System.out.println("CreateCase() Example: Case created with ID "
    + result.getCaseId());
}
```

Retrieve and update support case communications

AWS Support cases usually result in communication between the customer and AWS Support professionals. AWS Support provides the [DescribeCommunications](#) and [DescribeAttachment](#) operations to retrieve this correspondence, and the [AddAttachmentsToSet](#) and [AddCommunicationToCase](#) operations to update the case. These operations use the [Communication](#) data type to pass updates to the service and return them to your code.

The following Java code snippet adds communication to an AWS Support case. In the example, a private `printCommunicationsmethod` is provided for your convenience.

```
public static void addCommunication(AWSSupportClient client)
{
    System.out.println("Enter the CaseID for the case you want to update.");
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));
    String caseid = null;
    try
    {
        caseid = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    System.out.println("Enter text you want to add to this case.");
    String addcomm = null;
    try
    {
        addcomm = reader.readLine().trim();
    }
}
```

```
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

AddCommunicationToCaseRequest request =
    new AddCommunicationToCaseRequest().withCaseId(caseid)
                                       .withCommunicationBody(addcomm);
client.addCommunicationToCase(request);

System.out.println(
    "AddCommunication() Example: Call GetCommunications() " +
    "if you want to see if the communication was added.");
}

// DescribeCommunications example

public static void getCommunications(AWSSupportClient client)
    throws IOException
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));
    String caseNumber = null;

    System.out.println("Enter a CaseID");
    caseNumber = reader.readLine().trim();

    {
        DescribeCommunicationsRequest request =
            new DescribeCommunicationsRequest()
                .withCaseId(caseNumber.toString());

        DescribeCommunicationsResult result =
            client.describeCommunications(request);
        printCommunications(result.getCommunications());

        // Get more pages.
        while (result.getNextToken() != null)
        {
            request.setNextToken(result.getNextToken());
            result = client.describeCommunications(request);
            printCommunications(result.getCommunications());
            System.out.println(
                "GetCommunications() Example: Case communications retrieved"
                + " for case number " + request.getCaseId().toString());
        }
    }
}

private static void printCommunications(List<Communication> communications)
{
    for (Communication communication : communications)
    {
        System.out.println("SubmittedBy: " + communication.getSubmittedBy());
        System.out.println("  Body: " + communication.getBody());
    }
}
}
```

Note

DescribeCommunications returns the five most recent communications from a support case. Also, DescribeCommunications takes a list of CaseId values, which lets you retrieve communications for multiple cases in a single call.

Retrieve all support case information

You can retrieve all the information associated with your AWS Support cases by calling the [DescribeCases](#) operation. You populate a `DescribeCasesRequest` data type with a list of `ClientId` values, which are returned by each case when a successful `createCase` request returns.

The following Java code snippet accepts `CaseId` values from the console and populates a `DescribeCasesRequest` instance for use by the `DescribeCases` operation. A private `printCases` method is provided for your convenience.

```
public static void getCases(AWSSupportClient client)
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));

    System.out.println("Enter an AWS Support Case ID");
    String caseid = null;
    try
    {
        caseid = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    DescribeCasesRequest request = new DescribeCasesRequest();
    request.withCaseIdList(caseid);

    DescribeCasesResult result = client.describeCases(request);
    printCases(result.getCases());

    // Get more pages.
    while (result.getNextToken() != null)
    {
        request.setNextToken(result.getNextToken());
        result = client.describeCases(request);
        printCases(result.getCases());
    }
}

private static void printCases(List<CaseDetails> caseDetailsList)
{
    for (CaseDetails caseDetails : caseDetailsList)
    {
        System.out.println(
            "Case ID: " + caseDetails.getCaseId()); // This ID is for API use.
        System.out.println(
            "  Display ID: " + caseDetails.getDisplayId());
            // This ID is displayed on the AWS Support website.
        System.out.println("  Language: " + caseDetails.getLanguage());
        System.out.println("  Status: " + caseDetails.getStatus());
        System.out.println("  Subject: " + caseDetails.getSubject());
        System.out.println("Recent Communications: " +
            caseDetails.getRecentCommunications());
    }
}
```

Note

The `DescribeCases` operation takes parameters that let you control the number of cases, types of cases, and amount of detail to retrieve. For more information, see the [DescribeCases](#) operation.

Resolve a support case

AWS Support provides a [ResolveCase](#) operation to resolve your own support cases. The following Java code example demonstrates its use.

```
public static void resolveSupportCase(AWSSupportClient client)
{
    System.out.println(
        "Enter the AWS Support case ID for the case you want to resolve.");
    BufferedReader BR = new BufferedReader(new InputStreamReader(System.in));

    String caseid = null;
    try
    {
        caseid = BR.readLine().trim();
    }
    catch (IOException e)
    {
        // TODO Auto-generated catch block
        e.printStackTrace();
    }

    ResolveCaseResult rcr =
        client.resolveCase(new ResolveCaseRequest().withCaseId(caseid));
    System.out.println("Initial case status: " + rcr.getInitialCaseStatus());
    System.out.println("Final case status: " + rcr.getFinalCaseStatus());
}
```

Service quotas for the AWS Support API

The following table describes the current quotas for the AWS Support API.

Resource	Default value
The maximum number of AWS Support cases that you can create.	10 per hour
The maximum number of AWS Support API operations that you can perform per second.	5
The maximum number of AWS Trusted Advisor API operations that you can perform per second.	100

AWS Trusted Advisor

Trusted Advisor draws upon best practices learned from serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment, and then makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps.

If you have a Basic or Developer Support plan, you can use the Trusted Advisor console to access all checks in the Service Limits category and six checks in the Security category.

If you have a Business or Enterprise Support plan, you can use the Trusted Advisor console and the [AWS Support API \(p. 14\)](#) to access all Trusted Advisor checks. You also can use Amazon CloudWatch Events to monitor the status of Trusted Advisor checks. For more information, see [Monitoring Trusted Advisor check results with Amazon CloudWatch Events \(p. 123\)](#).

You can access Trusted Advisor in the AWS Management Console. For more information about controlling access to the Trusted Advisor console, see [Manage access for AWS Trusted Advisor \(p. 107\)](#).

For more information, see [Trusted Advisor](#).

Topics

- [Get started with AWS Trusted Advisor \(p. 25\)](#)
- [Organizational view for AWS Trusted Advisor \(p. 31\)](#)
- [Change log for AWS Trusted Advisor checks \(p. 49\)](#)
- [Using Trusted Advisor as a web service \(p. 52\)](#)

Get started with AWS Trusted Advisor

You can access Trusted Advisor from the AWS Management Console. Use the Trusted Advisor console to review check results for your AWS account and then follow the recommended steps to fix any issues. For example, Trusted Advisor might recommend that you delete unused resources to reduce your monthly bill, such as an Amazon Elastic Compute Cloud (Amazon EC2) instance.

You can also use the AWS Support API to perform operations on your Trusted Advisor checks. For more information, see the [AWS Support API Reference](#).

Topics

- [Sign in to the Trusted Advisor console \(p. 25\)](#)
- [View check categories \(p. 27\)](#)
- [View specific checks \(p. 28\)](#)
- [Filter your checks \(p. 29\)](#)
- [Refresh check results \(p. 30\)](#)
- [Download check results \(p. 30\)](#)
- [Organizational view \(p. 30\)](#)
- [Preferences \(p. 31\)](#)

Sign in to the Trusted Advisor console

You can view the checks and the status of each check in the Trusted Advisor console.

Note

You must have AWS Identity and Access Management (IAM) permissions to access the Trusted Advisor console. For more information, see [Manage access for AWS Trusted Advisor \(p. 107\)](#).

To sign in to the Trusted Advisor console

1. Sign in to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor/home>.
2. On the **Dashboard** page, view the summary for each check category:
 - **Action recommended (red)** – Trusted Advisor recommends an action for the check. For example, a check that detects a security issue for your IAM resources might recommend urgent steps.
 - **Investigation recommended (yellow)** – Trusted Advisor detects a possible issue for the check. For example, a check that reaches a quota for a resource might recommend ways to delete unused resources.
 - **Excluded items (gray)** – The number of checks that have excluded items, such as resources that you want a check to ignore. For example, this might be Amazon EC2 instances that you don't want the check to evaluate.
3. You can do the following on the **Dashboard** page:
 - To refresh all checks in your account, choose **Refresh all checks**.
 - To create an .xls file that includes all check results, choose **Download all checks**.
 - Under **Checks Summary**, choose a check category, such as **Security**, to view the results.
 - Under **Potential Monthly Savings**, you can view how much you can save for your account and the cost optimization checks for recommendations.
 - Under **Recent changes**, you can view changes to check statuses within the last 30 days. Choose a check name to view the latest results for that check or choose the arrow icon to view the next page.

Example : Trusted Advisor Dashboard

The following example shows a summary of the check results.

Dashboard

Refresh all checksDownload all checks

Use the Trusted Advisor dashboard to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. [Learn more](#)

Checks Summary

18

Action recommended

34

Investigation recommended

4

Excluded items

Security	13	Cost Optimization	13	Fault Tolerance	3
Fault Tolerance	5	Fault Tolerance	15	Performance	1
		Performance	4		
		Security	2		

Potential Monthly Savings

\$14,881.82

Trusted Advisor has identified 13 cost optimization checks that can save you money. For example, you might have unused resources in your AWS account that can be deleted. Choose a cost optimization check to view the recommendations.

[View all cost optimization checks](#)

Recent changes (49)

The following checks have new results or have changed status. Choose a check name to view the latest information.



Check	Date
EC2-VPC Elastic IP Address	06/22/2021
Amazon Relational Database Service (RDS) Reserved Instance Optimization	06/15/2021

View check categories

You can view the check descriptions and results for the following check categories:

- **Cost Optimization** – Recommendations that can potentially save you money. These checks highlight unused resources and opportunities to reduce your bill.
- **Performance** – Recommendations that can improve the speed and responsiveness of your applications.
- **Security** – Recommendations for security settings that can make your AWS solution more secure.
- **Fault Tolerance** – Recommendations that help increase the resiliency of your AWS solution. These checks highlight redundancy shortfalls, current service limits (also known as quotas), and overused resources.
- **Service Limits** – Checks the usage for your account and whether your account approaches or exceeds the limit (also known as quotas) for AWS services and resources.

To view check categories

1. Sign in to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor/home>.
2. In the navigation pane, choose the check category.
3. On the category page, view the summary for each check category:
 - **Action recommended (red)** – Trusted Advisor recommends an action for the check.
 - **Investigation recommended (yellow)** – Trusted Advisor detects a possible issue for the check.
 - **No problems detected (green)** – Trusted Advisor doesn't detect an issue for the check.
 - **Excluded items (gray)** – The number of checks that have excluded items, such as resources that you want a check to ignore.
4. For each check, choose the refresh icon () to refresh this check.
5. Choose the download icon () to create an .xls file that includes the results for this check.

Example : Cost Optimization category

The following example shows 13 (yellow) checks that need investigation and three (green) checks that don't have any issues.

Cost Optimization

[Refresh all checks](#)[Download all checks](#)

Choose a check name to see recommendations for ways to help save money for your AWS account. Trusted Advisor might recommend that you delete unused and idle resources, or use reserved capacity.

Cost Optimization Checks

Potential Monthly Savings
\$14,881.82

0

Info

13

Investigation recommended

3

No problems detected

0

Excluded items

Filter by tag [Learn more about using tags](#)

[Reset](#)[Apply filter](#)

View by
All checks

▶

⚠

Amazon EC2 Reserved Instances Optimization

Refreshed: a day ago

A significant part of using AWS involves balancing your Reserved Instance (RI) usage and your On-Demand instance usage.

Estimated monthly savings with one year RI term: \$329.91 (24.0%). Estimated monthly savings with three year RI term: \$530.07 (38.0%)

▶

⚠

Amazon RDS Idle DB Instances

Refreshed: a day ago

Checks the configuration of your Amazon Relational Database Service (Amazon RDS) for any DB instances that appear to be idle.

28 of 29 DB instances appear to be Idle. Monthly savings of up to \$3,744 are available by minimizing idle DB Instances.

▶

⚠

Amazon Redshift Reserved Node Optimization

Refreshed: a day ago

Checks your usage of Redshift and provides recommendations on purchase of Reserved Nodes to help reduce costs incurred from using Redshift On-Demand.

Estimated monthly savings with one year Reserved Node term: \$1,069.77 (32.0%). Estimated monthly savings with three year Reserved Node term: \$2,024.31 (60.0%).

View specific checks

Expand a check to view the full check description, your affected resources, any recommended steps, and links to more information.

To view a specific check

1. Sign in to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor/home>.
2. In the navigation pane, choose a check category.
3. Choose the check name to view the description and the following details:
 - **Alert Criteria** – Describes the threshold when a check will change status.
 - **Recommended Action** – Describes the recommended actions for this check.
 - **Additional Resources** – Lists related AWS documentation.
 - A table that lists the affected items in your account. You can include or exclude these items from check results.
4. (Optional) To exclude items so that they don't appear in check results:
 - a. Select an item and choose **Exclude & Refresh**.
 - b. To view all excluded items, choose **Excluded items**.
5. (Optional) To include items so that the check evaluates them again:
 - a. Choose **Excluded items**, select an item, and then choose **Include & Refresh**.
 - b. To view all included items, choose **Included items**.
6. Choose the settings icon (⚙) and in the **Preferences** dialog box, you can specify the number of items or the properties to display, and then choose **Confirm**.

API Version 2013-04-15
28

Example : Cost Optimization check

The following **Low Utilization Amazon EC2 Instances** check lists the affected instances in the account. This check identifies 41 Amazon EC2 instances that have low usage and recommends that you stop or terminate the resources.

Low Utilization Amazon EC2 Instances
Refreshed: a day ago

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria
Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action
Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

Additional Resources
[Monitoring Amazon EC2](#)
[Instance Metadata and User Data](#)
[Amazon CloudWatch Developer Guide](#)
[Auto Scaling Developer Guide](#)

Low Utilization Amazon EC2 Instances (41)
Exclude & Refresh
Included items

41 of 42 Amazon EC2 instances have low average daily utilization. Monthly savings of up to \$962.21 might be available by minimizing underutilized instances.

	Region/AZ	Instance ID	Instance Name	Instance Type	Estimated Monthly Savings	CPU Utilization 14-Day Average
<input type="checkbox"/>	eu-west-2a	i-0700a74207981234		t2.micro	0	7.667864087142718E-4
<input type="checkbox"/>	eu-west-2a	i-0e3f4b8ae22161234		t2.micro	0	0.0013923912552209253
<input type="checkbox"/>	us-east-1a	i-083bbd460741c1234	ec2WindowsCheck+c5.large+ami-085ea19726example	c5.large	60	0.003315245975413382

Filter your checks


On the check category pages, you can specify which check results that you want to view. For example, you might filter by checks that have detected errors in your account, so that you can investigate urgent issues first.

If you have checks that evaluate items in your account, such as AWS resources, you can use tag filters to only show items that have the specified tag.

To filter your checks

- Sign in to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor/home>.
- In the navigation pane or the **Dashboard** page, choose the check category.
- For the **View** list, specify which checks to view:
 - All checks** – List all checks for this category
 - Action recommended** – List checks that recommend that you take action. These checks are highlighted in red.
 - Investigation recommended** – List checks that recommend that you take possible action. These checks are highlighted in yellow.
 - No problems detected** – List checks that don't have any issues. These checks are highlighted in green.
 - Checks with excluded items** – List checks that you specified to exclude items from the check results.
- If you added tags to your AWS resources, such as Amazon EC2 instances or AWS CloudTrail trails, you can filter your results so that the checks only show items that have the specified tag.

For **Filter by tag**, enter a tag key and value, and then choose **Apply filter**.

Filter by tag [Learn more about using tags](#) 

Tag Key

Tag Value

Reset

Apply filter

5. In the table for the check, the check results only show items that have the specified key and value.
6. To clear the filter by tags, choose **Reset**.

Related information

For more information about tagging for Trusted Advisor, see the following topics:

- [AWS Support enables tagging capabilities for Trusted Advisor](#)
- [Tagging AWS resources](#) in the *AWS General Reference*

Refresh check results

You can refresh checks to get the latest results for your account.

To refresh Trusted Advisor checks

1. Navigate to the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. On the **Dashboard** or a check category page, choose **Refresh all checks**.


You can also refresh specific checks in the following ways:

- Choose the refresh icon () for an individual check.
- Use the [RefreshTrustedAdvisorCheck](#) API operation.

Download check results

You can download check results to get an overview of Trusted Advisor in your account. You can download results for all checks or a specific check.

To download Trusted Advisor checks results

1. Navigate to the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
 - To download all check results, in the **Dashboard** or a check category page, choose **Download all checks**.
 - To download a check result for a specific check, choose the check name, and then choose the download icon ()
2. Save or open the .xls file. The file contains the same summary information from the Trusted Advisor console, such as the check name, description, status, affected resources, and so on.

Organizational view

You can set up the organizational view feature to create a report for all member accounts in your AWS organization. For more information, see [Organizational view for AWS Trusted Advisor](#) (p. 31).

Preferences

On the **Preferences** page in the Trusted Advisor console, you can configure your weekly email messages for the check summary, enable the organizational view feature, or disable Trusted Advisor.

Set up notification preferences

Specify who can receive the weekly Trusted Advisor email messages for check results and the language.

To set up notification preferences

1. Sign in to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor/home>.
2. In the navigation pane, choose **Preferences**.
3. For **Weekly Email Notification**, select whom to notify for your check results. You can add and remove contacts from the [Account Settings](#) page in the AWS Billing and Cost Management console.
4. For **Language**, choose the language for the email message.
5. Choose **Save Email Preferences**.

Set up organizational view

If you set up your account with AWS Organizations, you can create reports for all member accounts in your organization. For more information, see [Organizational view for AWS Trusted Advisor \(p. 31\)](#).

Disable Trusted Advisor

When you disable this service, Trusted Advisor won't perform any checks on your account. Anyone who tries to access the Trusted Advisor console or use the API operations will receive an access denied error message.

To disable Trusted Advisor

1. Under **Trusted Advisor**, choose **Disable Trusted Advisor**. This action disables Trusted Advisor for all checks in your account.
2. You can then manually delete the [AWSServiceRoleForTrustedAdvisor](#) from your account. For more information, see [Deleting a service-linked role for Trusted Advisor \(p. 102\)](#).

Related information

For more information about Trusted Advisor, see the following topics:

- [How do I start using Trusted Advisor?](#)
- [AWS Trusted Advisor check reference \(p. 56\)](#)

Organizational view for AWS Trusted Advisor

Organizational view lets you view Trusted Advisor checks for all accounts in your [AWS Organizations](#). After you enable this feature, you can create reports to aggregate the check results for all member accounts in your organization. The report includes a summary of check results and information about

affected resources for each account. For example, you can use the reports to identify which accounts in your organization are using AWS Identity and Access Management (IAM) with the IAM Use check or whether you have recommended actions for Amazon Simple Storage Service (Amazon S3) buckets with the Amazon S3 Bucket Permissions check.

Topics

- [Prerequisites \(p. 32\)](#)
- [Enable organizational view \(p. 32\)](#)
- [Refresh Trusted Advisor checks \(p. 33\)](#)
- [Create organizational view reports \(p. 33\)](#)
- [View the report summary \(p. 35\)](#)
- [Download an organizational view report \(p. 36\)](#)
- [Disable organizational view \(p. 40\)](#)
- [Using IAM policies to allow access to organizational view \(p. 41\)](#)
- [Using other AWS services to view Trusted Advisor reports \(p. 42\)](#)

Prerequisites

You must meet the following requirements to enable organizational view:

- Your accounts must be members of an [AWS Organization](#).
- Your organization must have all features enabled for Organizations. For more information, see [Enabling all features in your organization](#) in the *AWS Organizations User Guide*.
- The management account in your organization must have a Business or Enterprise support plan. You can find your support plan from the AWS Support Center or from the [Support plans](#) page. See [Compare AWS Support plans](#).
- You must sign in as a user in the [management account](#) (or [assumed equivalent role](#)). Whether you sign in as an IAM user or an IAM role, you must have a policy with the required permissions. See [Using IAM policies to allow access to organizational view \(p. 41\)](#).

Enable organizational view

After you meet the prerequisites, follow these steps to enable organizational view. After you enable this feature, the following happens:

- Trusted Advisor is enabled as a *trusted service* in your organization. For more information, see [Enabling trusted access with other AWS services](#) in the *AWS Organizations User Guide*.
- The `AWSServiceRoleForTrustedAdvisorReporting` service-linked-role is created for you in the management account in your organization. This role includes the permissions that Trusted Advisor needs to call Organizations on your behalf. This service-linked role is locked, and you can't delete it manually. For more information, see [Using service-linked roles for Trusted Advisor \(p. 99\)](#).

You enable organizational view from the Trusted Advisor console.

To enable organizational view

1. Sign in as an administrator in the organization's management account and open the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. In the navigation pane, choose **Organizational View**.

3. Choose **Enable organizational view**.

Refresh Trusted Advisor checks

Before you create a report for your organization, we recommend that you refresh the statuses of your Trusted Advisor checks. You can download a report without refreshing your Trusted Advisor checks, but your report might not have the latest information.

If you have a Business or Enterprise account, Trusted Advisor automatically refreshes the checks in your account on a weekly basis.


Note

If you have accounts in your organization that have a Developer or Basic support plan, a user for those accounts must sign in to the Trusted Advisor console to refresh the checks. You can't refresh checks for all accounts from the organization's management account.

To refresh Trusted Advisor checks

1. Navigate to the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. On the **Dashboard** page, choose the **Refresh all checks**. This refreshes all checks in your account.

You can also refresh specific checks in the following ways:

- Use the [RefreshTrustedAdvisorCheck](#) API operation.
- Choose the refresh icon () for an individual check.

Create organizational view reports

After you enable organizational view, you can create reports so that you can view Trusted Advisor check results for your organization.

You can create up to 50 reports. If you create reports beyond this quota, Trusted Advisor deletes the earliest report. You can't recover deleted reports.

To create organizational view reports

1. Sign in to the organization's management account and open the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. In the navigation pane, choose **Organizational View**.
3. Choose **Create report**.
4. By default, the report includes all AWS Regions, check categories, checks, and resource statuses. On the **Create report** page, you can use the filter options to customize your report. For example, you can clear the **All** option for **Region**, and then specify the individual Regions to include in the report.
 - a. Enter a **Name** for the report.
 - b. For **Format**, choose **JSON** or **CSV**.
 - c. For **Region**, specify the AWS Regions or choose **All**.
 - d. For **Check category**, choose the check category or choose **All**.
 - e. For **Checks**, choose the specific checks for that category or choose **All**.

Note

The **Check category** filter overrides the **Checks** filter. For example, if you choose the **Security** category and then choose a specific check name, your report includes all check

results for that category. To create a report for only specific checks, keep the default **All** value for **Check category** and then choose your check names.

- f. For **Resource status**, choose the status to filter, such as **Warning**, or choose **All**.
5. For **AWS Organization**, select the organizational units (OUs) to include in your report. For more information about OUs, see [Managing organizational units](#) in the *AWS Organizations User Guide*.
6. Choose **Create report**.

Example : Create report filter options

The following example creates a JSON report for the following:

- Three AWS Regions
- All **Security** and **Performance** checks

Report filters

Choose the filter options for your report.

Report name

The report name can be up to 100 characters and can't start with a hyphen. Valid characters: A-Z, a-z, 0-9, and - (hyphen)

Format

Region

Check category

Checks

Resource status

In the following example, the report includes the **support-team** OU and one AWS account that are part of the organization.

AWS organization

You can select the organizational units (OUs) and individual AWS accounts to include in your report.

Organizational structure

▼

Root

r-xa9c

▶

instance-management

ou-xa9c-example1

▼

☒

support-team

ou-xa9c-example2

☒

Jane Doe

111122223333 | janedoe@example.com

☒

Mateo Jackson

444455556666 | mateojackson@example.com

▶

security-team

ou-xa9c-example3

☒

Ana Carolina Silva

777788889999 | anacarolinasilva@example.com

Notes

- The amount of time it takes to create the report depends on the number of accounts in the organization and the number of resources in each account.
- You can't create more than one report at a time unless the current report has been running for more than 6 hours.
- Refresh the page if you don't see the report appear on the page.

View the report summary

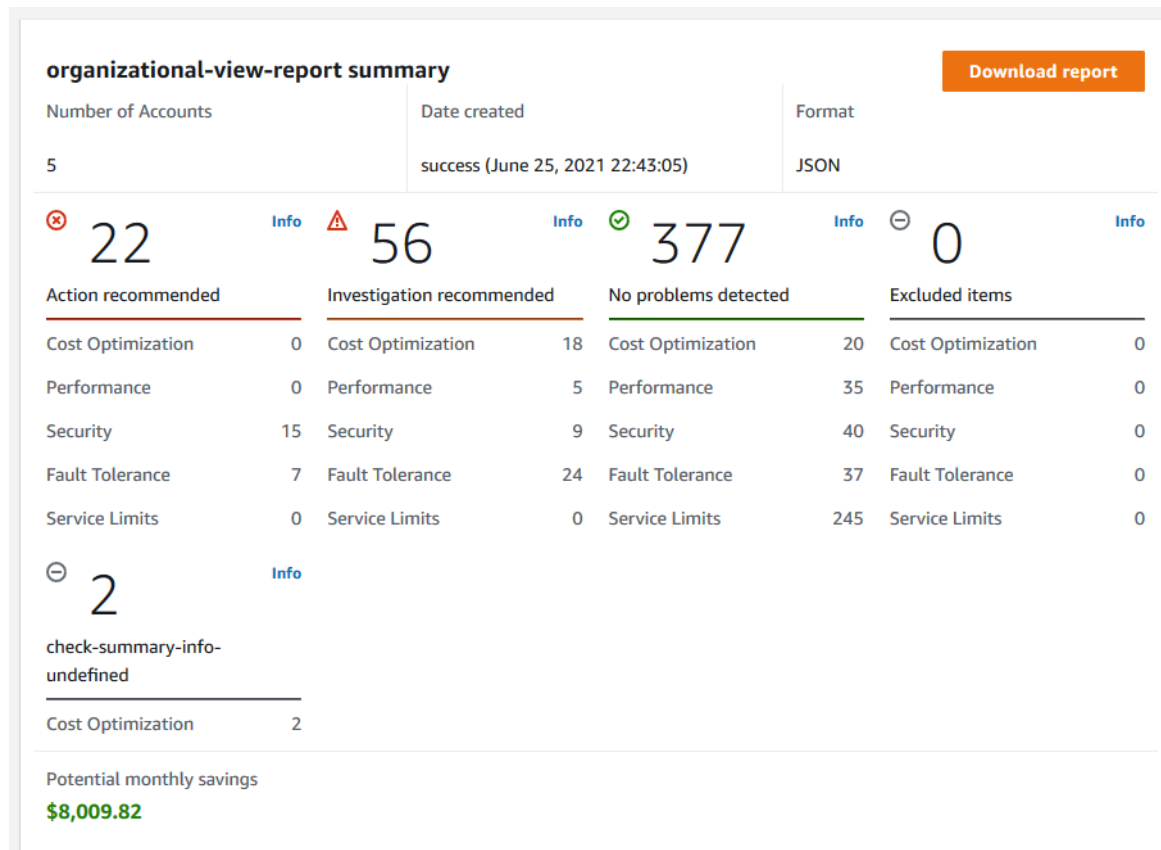
After the report is ready, you can view the report summary from the Trusted Advisor console. This lets you quickly view the summary of your check results across your organization.

To view the report summary

1. Sign in to the organization's management account and open the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.

2. In the navigation pane, choose **Organizational View**.
3. Choose the report name.
4. On the **Summary** page, view the check statuses for each category. You can also choose **Download report**.

Example : Report summary for an organization



Download an organizational view report

After your report is ready, download it from the Trusted Advisor console. The report is a .zip file that contains three files:

- `summary.json` – Contains a summary of the check results for each check category.
- `schema.json` – Contains the schema for the specified checks in the report.
- A resources file (.json or .csv) – Contains detailed information about the check statuses for resources in your organization.


To download an organizational view report

1. Sign in to the organization's management account and open the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. In the navigation pane, choose **Organizational View**.

The **Organizational View** page displays the available reports to download.

3. Select a report, choose **Download report**, and then save the file. You can only download one report at a time.

Organizational View

With AWS organizations, you can create reports for check results across all AWS accounts within an organization. This provides you a centralized view for all AWS Trusted Advisor checks. You can also view and download reports on this page. Use this report to identify issues and take action for accounts in your organization. [Learn more](#) .

Reports (50)

Create reportDownload report

	Report name	Date generated	Status	Format
<input type="radio"/>	all-regions-check-report	June 15, 2021 18:43:42	Success	JSON
<input type="radio"/>	json-us-east-1-region-only	June 14, 2021 20:54:29	Success	JSON
<input type="radio"/>	security-checks-only-all-accounts	June 10, 2021 03:33:59	Success	JSON

4. Unzip the file.
5. Use a text editor to open the .json file or a spreadsheet application to open the .csv file.

Note

You might receive multiple files if your report is 5 MB or larger.

Example : summary.json file

The `summary.json` file shows the number of accounts in the organization and the statuses of the checks in each category.

Trusted Advisor uses the following color code for check results:

- Green – Trusted Advisor doesn't detect an issue for the check.
- Yellow – Trusted Advisor detects a possible issue for the check.
- Red – Trusted Advisor detects an error and recommends an action for the check.
- Blue – Trusted Advisor can't determine the status of the check.

In the following example, two checks are Red, one is Green, and one is Yellow.

```
{
  "numAccounts": 3,
  "filtersApplied": {
    "accountIds": ["123456789012", "111122223333", "111111111111"],
    "checkIds": "All",
    "categories": [
      "security",
      "performance"
    ],
    "statuses": "All",
    "regions": [
      "us-west-1",
      "us-west-2",
      "us-east-1"
    ],
    "organizationalUnitIds": [
      "ou-xa9c-EXAMPLE1",
```

```
        "ou-xa9c-EXAMPLE2"
      ]
    },
    "categoryStatusMap": {
      "security": {
        "statusMap": {
          "ERROR": {
            "name": "Red",
            "count": 2
          },
          "OK": {
            "name": "Green",
            "count": 1
          },
          "WARN": {
            "name": "Yellow",
            "count": 1
          }
        }
      },
      "name": "Security"
    }
  },
  "accountStatusMap": {
    "123456789012": {
      "security": {
        "statusMap": {
          "ERROR": {
            "name": "Red",
            "count": 2
          },
          "OK": {
            "name": "Green",
            "count": 1
          },
          "WARN": {
            "name": "Yellow",
            "count": 1
          }
        }
      },
      "name": "Security"
    }
  }
}
```

Example : schema.json file

The `schema.json` file includes the schema for the checks in the report. The following example includes the IDs and properties for the IAM Password Policy (Yw2K9puPzl) and IAM Key Rotation (DqdJqYeRm5) checks.

```
{
  "Yw2K9puPzl": [
    "Password Policy",
    "Uppercase",
    "Lowercase",
    "Number",
    "Non-alphanumeric",
    "Status",
    "Reason"
  ],
  "DqdJqYeRm5": [
    "Status",
    "IAM User",
  ]
}
```

```

    "Access Key",
    "Key Last Rotated",
    "Reason"
  ],
  ...
}

```

Example : resources.csv file

The `resources.csv` file includes information about resources in the organization. This example shows some of the data columns that appear in the report, such as the following:

- Account ID of the affected account
- The Trusted Advisor check ID
- The resource ID
- Timestamp of the report
- The full name of the Trusted Advisor check
- The Trusted Advisor check category
- The account ID of the parent organizational unit (OU) or root

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUL	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUL	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWle_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3Y0wy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	Llc4zRaUSiIGRSImqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TlmW-5Jc	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7lgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbi	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-Mul6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

The resources file only contains entries if a check result exists at the resource level. You might not see checks in the report for the following reasons:

- Some checks, such as **MFA on Root Account**, don't have resources and won't appear in the report. Checks without resources appear in the `summary.json` file instead.
- Some checks only show resources if they are **Red** or **Yellow**. If all resources are **Green**, they might not appear in your report.
- If an account isn't enabled for a service that requires the check, the check might not appear in the report. For example, if you're not using Amazon Elastic Compute Cloud Reserved Instances in your organization, the Amazon EC2 Reserved Instance Lease Expiration check won't appear in your report.
- The account hasn't refreshed check results. This might happen when users with a Basic or Developer support plan sign in to the Trusted Advisor console for the first time. If you have a Business or Enterprise support plan, it can take up to one week from account sign up for users to see check results. For more information, see [Refresh Trusted Advisor checks \(p. 33\)](#).
- If only the organization's management account enabled recommendations for checks, the report won't include resources for other accounts in the organization.

For the resources file, you can use common software such as Microsoft Excel to open the .csv file format. You can use the .csv file for one-time analysis of all checks across all accounts in your organization. If you want to use your report with an application, you can download the report as a .json file instead.

The .json file format provides more flexibility than the .csv file format for advanced use cases such as aggregation and advanced analytics with multiple datasets. For example, you can use a SQL interface with an AWS service such as Amazon Athena to run queries on your reports. You can also use Amazon QuickSight to create dashboards and visualize your data. For more information, see [Using other AWS services to view Trusted Advisor reports \(p. 42\)](#).

Disable organizational view

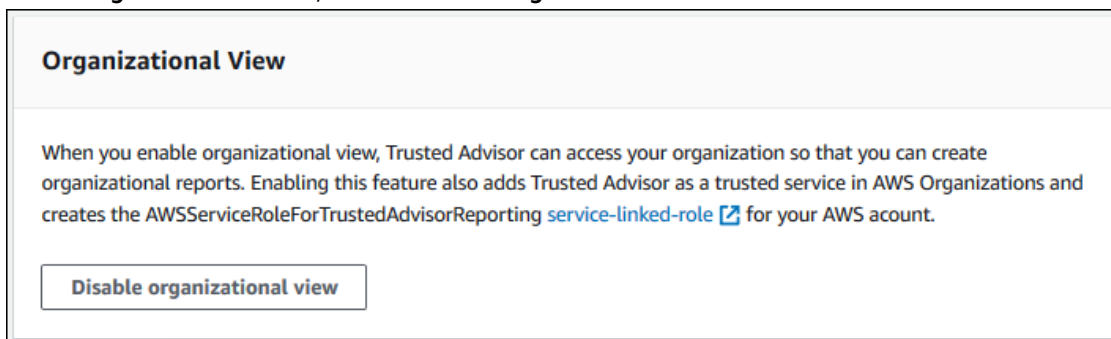
Follow this procedure to disable organizational view. You must sign in to the organization's management account or assume a role with the required permissions to disable this feature. You can't disable this feature from another account in the organization.

After you disable this feature, the following happens:

- Trusted Advisor is removed as a trusted service in Organizations.
- The `AWSServiceRoleForTrustedAdvisorReporting` service-linked role is unlocked in the organization's management account. This means you can delete it manually, if needed.
- You can't create, view, or download reports for your organization. To access previously created reports, you must reenble organizational view from the Trusted Advisor console. See [Enable organizational view \(p. 32\)](#).

To disable organizational view for Trusted Advisor

1. Sign in to the organization's management account and open the AWS Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. In the navigation pane, choose **Preferences**.
3. Under **Organizational View**, choose **Disable organizational view**.



After you disable organizational view, Trusted Advisor no longer aggregates checks from other AWS accounts in your organization. However, the `AWSServiceRoleForTrustedAdvisorReporting` service-linked role remains on the organization's management account until you delete it through the IAM console, IAM API, or AWS Command Line Interface (AWS CLI). For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Note

You can use other AWS services to query and visualize your data for organizational view reports. For more information, see the following resources:

- [View AWS Trusted Advisor recommendations at scale with AWS Organizations](#) in the *AWS Management & Governance Blog*
- [Using other AWS services to view Trusted Advisor reports \(p. 42\)](#)

Using IAM policies to allow access to organizational view

You can use the following AWS Identity and Access Management (IAM) policies to allow users or roles in your account access to organizational view in AWS Trusted Advisor.

Example : Full access to organizational view

The following policy allows full access to the organizational view feature. A user with these permissions can do the following:

- Enable organizational view.
- Create, view, and download reports.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadStatement",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "trustedadvisor:DescribeAccount",
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeAccountAccess",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeReports",
        "trustedadvisor:DescribeServiceMetadata",
        "trustedadvisor:DescribeOrganizationAccounts",
        "trustedadvisor:ListAccountsForParent",
        "trustedadvisor:ListRoots",
        "trustedadvisor:ListOrganizationalUnitsForParent"
      ],
      "Resource": "*"
    },
    {
      "Sid": "MutatingStatement",
      "Effect": "Allow",
      "Action": [
        "trustedadvisor:GenerateReport"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OnboardingStatement1",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OnboardingStatement2",
      "Effect": "Allow",

```

```
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
    }
  ]
}
```

Example : Read access to organizational view

The following policy allows read-only access to organizational view for Trusted Advisor. A user with these permissions can only view and download existing reports.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadStatement",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "trustedadvisor:DescribeAccount",
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeAccountAccess",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeReports",
        "trustedadvisor:ListAccountsForParent",
        "trustedadvisor:ListRoots",
        "trustedadvisor:ListOrganizationalUnitsForParent"
      ],
      "Resource": "*"
    }
  ]
}
```

You can also create your own IAM policy. For more information, see [Creating IAM Policies](#) in the *IAM User Guide*.

Note

If you enabled AWS CloudTrail in your account, the following roles can appear in your log entries:

- `AWSServiceRoleForTrustedAdvisorReporting` – The service-linked role that Trusted Advisor uses to access accounts in your organization.
- `AWSServiceRoleForTrustedAdvisor` – The service-linked role that Trusted Advisor uses to access services in your organization.

For more information about service-linked roles, see [Using service-linked roles for Trusted Advisor](#) (p. 99).

Using other AWS services to view Trusted Advisor reports

Follow this tutorial to upload and view your data by using other AWS services. In this topic, you create an Amazon Simple Storage Service (Amazon S3) bucket to store your report and an AWS CloudFormation

template to create resources in your account. Then, you can use Amazon Athena to analyze or run queries for your report or Amazon QuickSight to visualize that data in a dashboard.

For information and examples for visualizing your report data, see the [View AWS Trusted Advisor recommendations at scale with AWS Organizations](#) in the *AWS Management & Governance Blog*.

Prerequisites

Before you start this tutorial, you must meet the following requirements:

- Sign in as an AWS Identity and Access Management (IAM) user with administrator permissions.
- Use the US East (N. Virginia) AWS Region to quickly set up your AWS services and resources.
- Create an Amazon QuickSight account. For more information, see [Getting Started with Data Analysis in Amazon QuickSight](#) in the *Amazon QuickSight User Guide*.

Upload the report to Amazon S3

After you download your `resources.json` report, upload the file to Amazon S3. You must use a bucket in the US East (N. Virginia) Region.

To upload the report to an Amazon S3 bucket

1. Sign in to the AWS Management Console at <https://console.aws.amazon.com/>.
2. Use the **Region selector** and choose the US East (N. Virginia) Region.
3. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
4. From the list of buckets, choose an S3 bucket, and then copy the name. You use the name in the next procedure.
5. On the `bucket-name` page, choose **Create folder**, enter the name `folder1`, and then choose **Save**.
6. Choose the `folder1`.
7. In `folder1`, choose **Upload** and choose the `resources.json` file.
8. Choose **Next**, keep the default options, and then choose **Upload**.

Note

If you upload a new report to this bucket, rename the `.json` files each time you upload them so that you don't override the existing reports. For example, you can add the timestamp to each file, such as `resources-timestamp.json`, `resources-timestamp2.json`, and so on.

Create your resources using AWS CloudFormation

After you upload your report to Amazon S3, upload the following YAML template to AWS CloudFormation. This template tells AWS CloudFormation what resources to create for your account so that other services can use the report data in the S3 bucket. The template creates resources for IAM, AWS Lambda, and AWS Glue.

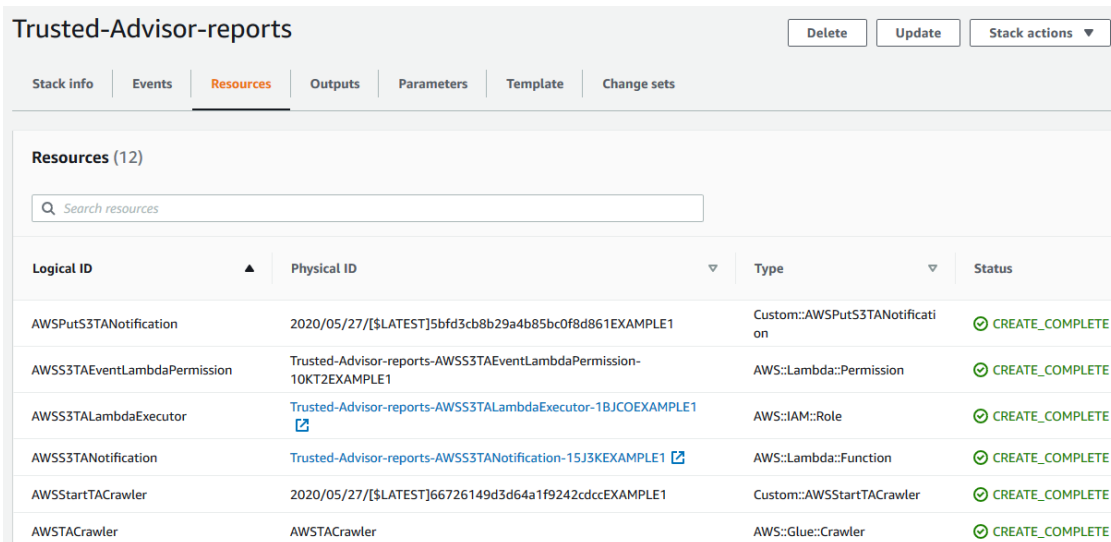
To create your resources with AWS CloudFormation

1. Download the [trusted-advisor-reports-template.zip](#) file.
2. Unzip the file.
3. Open the template file in a text editor.
4. For the `BucketName` and `FolderName` parameters, replace the values for `your-bucket-name-here` and `folder1` with the bucket name and folder name in your account.
5. Save the file.

6. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
7. If you haven't already, in the **Region selector**, choose the US East (N. Virginia) Region.
8. In the navigation pane, choose **Stacks**.
9. Choose **Create stack** and choose **With new resources (standard)**.
10. On the **Create stack** page, under **Specify template**, choose **Upload a template file**, and then choose **Choose file**.
11. Choose the YAML file and choose **Next**.
12. On the **Specify stack details** page, enter a stack name such as **Organizational-view-Trusted-Advisor-reports**, and choose **Next**.
13. On the **Configure stack options** page, keep the default options, and then choose **Next**.
14. On the **Review Organizational-view-Trusted-Advisor-reports** page, review your options. At the bottom of the page, select the check box for **I acknowledge that AWS CloudFormation might create IAM resources**.
15. Choose **Create stack**.

The stack takes about 5 minutes to create.

16. After the stack creates successfully, the **Resources** tab appears like the following example.



The screenshot shows the AWS CloudFormation console with the 'Resources' tab selected for a stack named 'Trusted-Advisor-reports'. The console displays a table of 12 resources, all of which are in the 'CREATE_COMPLETE' status. The resources include various AWS services like S3, Lambda, IAM, and Glue, used for generating and storing Trusted Advisor reports.

Logical ID	Physical ID	Type	Status
AWSPutS3Notification	2020/05/27/[\$LATEST]5b9d3cb8b29a4b85bc0f8d861EXAMPLE1	Custom::AWSPutS3Notification	CREATE_COMPLETE
AWSS3TAEventLambdaPermission	Trusted-Advisor-reports-AWSS3TAEventLambdaPermission-10KT2EXAMPLE1	AWS::Lambda::Permission	CREATE_COMPLETE
AWSS3TALambdaExecutor	Trusted-Advisor-reports-AWSS3TALambdaExecutor-1BJCOEXAMPLE1	AWS::IAM::Role	CREATE_COMPLETE
AWSS3TANotification	Trusted-Advisor-reports-AWSS3TANotification-15J3KEXAMPLE1	AWS::Lambda::Function	CREATE_COMPLETE
AWSSstartTACrawler	2020/05/27/[\$LATEST]66726149d3d64a1f9242cdccEXAMPLE1	Custom::AWSSstartTACrawler	CREATE_COMPLETE
AWSTACrawler	AWSTACrawler	AWS::Glue::Crawler	CREATE_COMPLETE

Query the data in Amazon Athena

After you have your resources, you can view the data in Athena. Use Athena to create queries and analyze the results of the report, such as looking up specific check results for accounts in the organization.

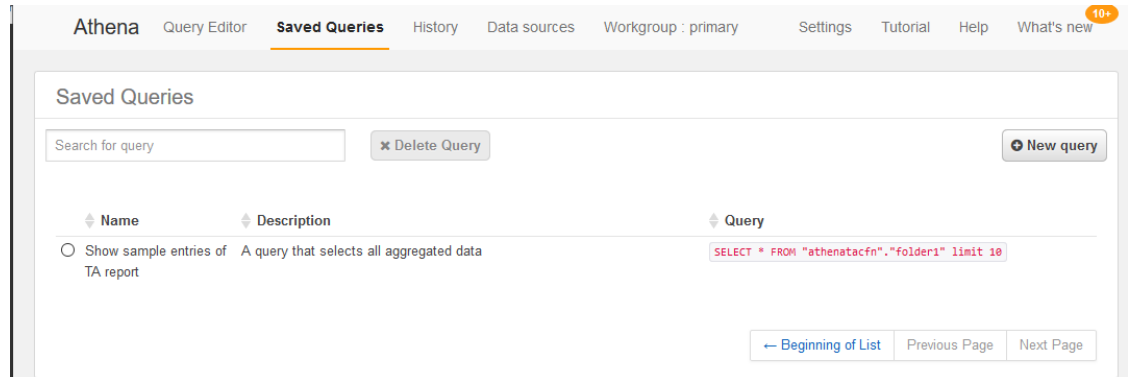
Notes

- Use the US East (N. Virginia) Region.
- If you're new to Athena, you must specify a query result location before you can run a query for your report. We recommend that you specify a different S3 bucket for this location. For more information, see [Specifying a query result location](#) in the *Amazon Athena User Guide*.

To query the data in Athena

1. Open the Athena console at <https://console.aws.amazon.com/athena/>.
2. If you haven't already, in the **Region selector**, choose the US East (N. Virginia) Region.

3. Choose **Saved Queries** and in search field, enter **Show sample**.
4. Choose the query that appears, such as **Show sample entries of TA report**.



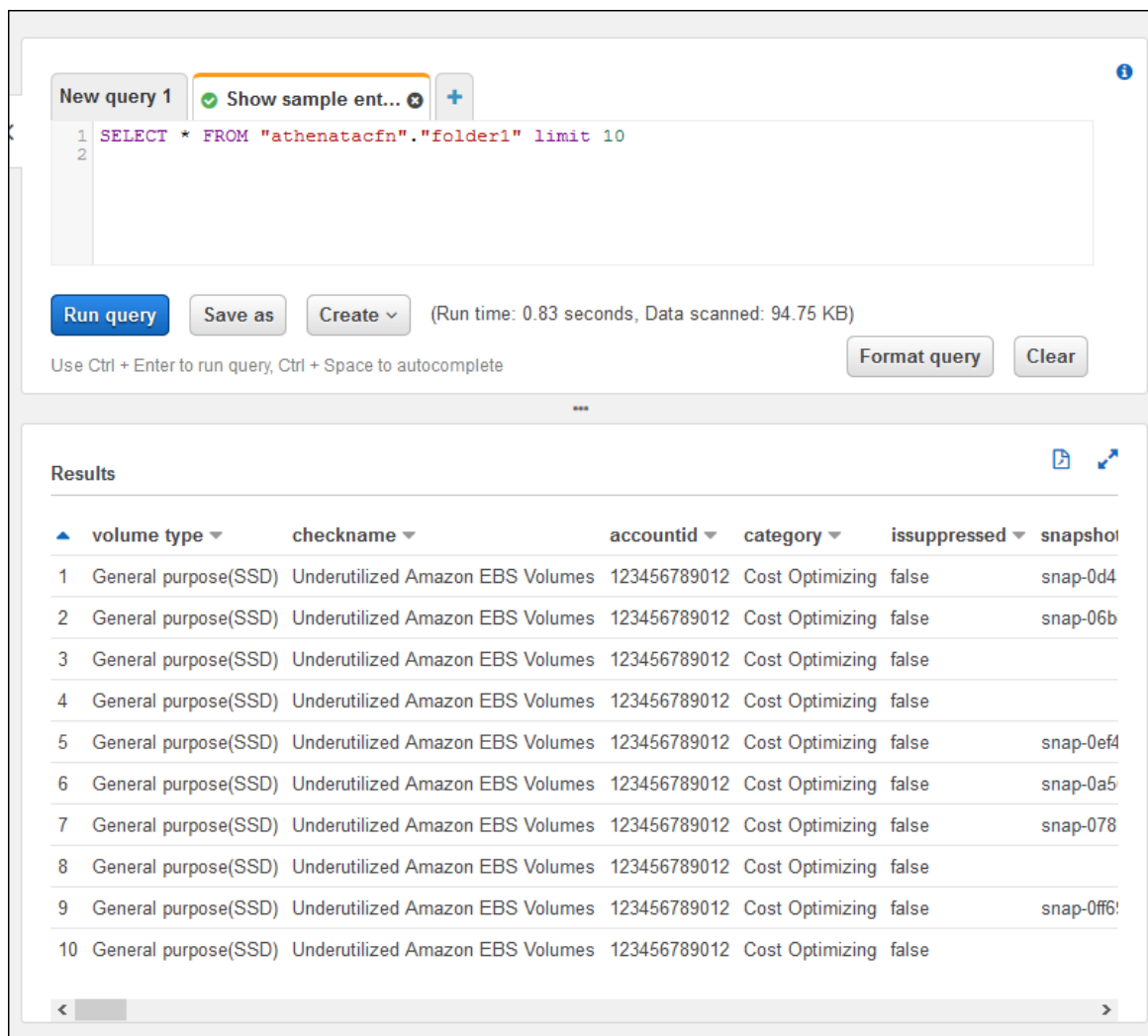
The query should look like the following.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. Choose **Run query**. Your query results appear.

Example : Athena query

The following example shows 10 sample entries from the report.



The screenshot shows the Amazon Athena console interface. At the top, there's a query editor with a text area containing a SQL query: `SELECT * FROM "athenatacfn"."folder1" limit 10`. Below the editor are buttons for "Run query", "Save as", and "Create", along with a status message: "(Run time: 0.83 seconds, Data scanned: 94.75 KB)". A hint says "Use Ctrl + Enter to run query, Ctrl + Space to autocomplete". To the right are "Format query" and "Clear" buttons. Below the editor is a "Results" section with a table of 10 rows. The table has columns: volume type, checkname, accountid, category, issuppressed, and snapshot. All rows show "General purpose(SSD)" for volume type, "Underutilized Amazon EBS Volumes" for checkname, and "Cost Optimizing" for category. The snapshot column shows various IDs like "snap-0d4", "snap-06b", etc.

	volume type	checkname	accountid	category	issuppressed	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

For more information, see [Running SQL Queries Using Amazon Athena](#) in the *Amazon Athena User Guide*.

Create a dashboard in Amazon QuickSight

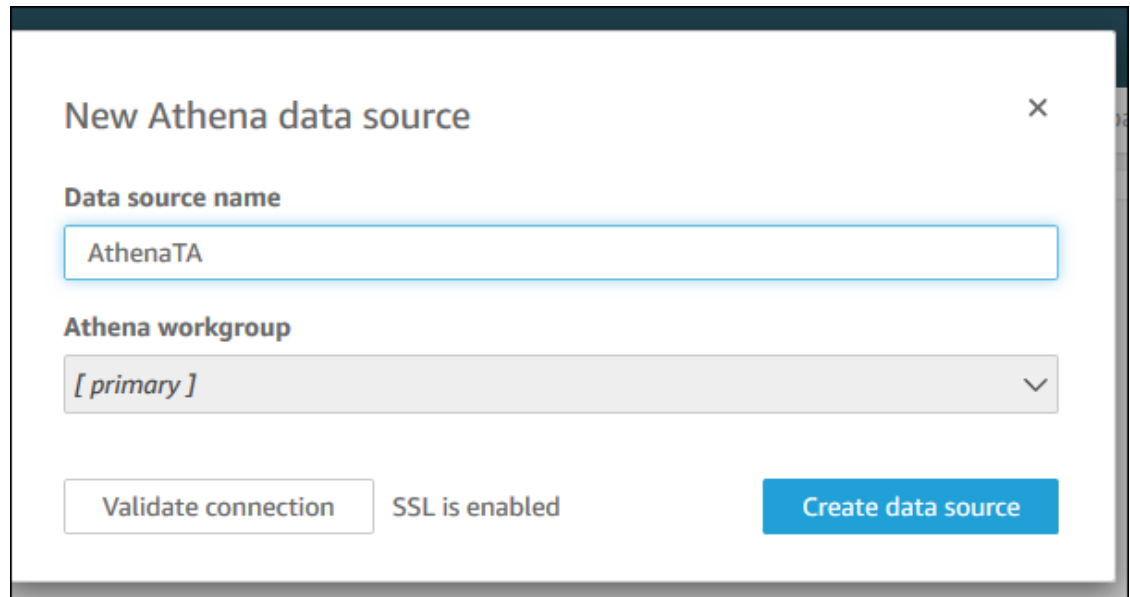
You can also set up Amazon QuickSight so that you can view your data in a dashboard and visualize your report information.

Note

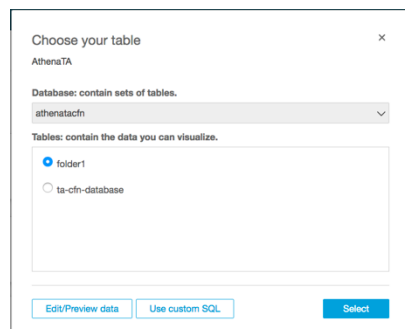
You must use the US East (N. Virginia) Region.

To create a dashboard in Amazon QuickSight

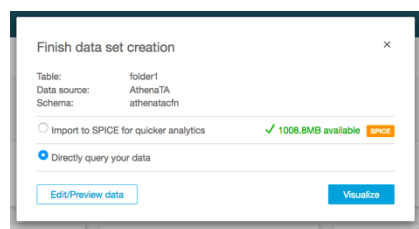
1. Navigate to the Amazon QuickSight console and sign in to your [account](#).
2. Choose **New analysis**, **New dataset**, and then choose **Athena**.
3. In the **New Athena data source** dialog box, enter a data source name such as **AthenaTA**, and then choose **Create data source**.



4. In the **Choose your table** dialog box, choose the **athenatacfn** table, choose **folder1**, and then choose **Select**.



5. In the **Finish data set creation** dialog box, choose **Directly query your data**, and then choose **Visualize**.



You can now create a dashboard in Amazon QuickSight. For more information, see [Working with Dashboards](#) in the *Amazon QuickSight User Guide*.

Example : Amazon QuickSight dashboard

The following example dashboard shows information about the Trusted Advisor checks, such as the following:

- Affected account IDs
- Summary by AWS Regions
- Check categories

- Check statuses
- Number of entries in the report for each account



Note

If you have permission errors while creating your dashboard, make sure that Amazon QuickSight can use Athena. For more information, see [I Can't Connect to Amazon Athena](#) in the *Amazon QuickSight User Guide*.

For more information and examples for visualizing your report data, see the [View AWS Trusted Advisor recommendations at scale with AWS Organizations](#) in the *AWS Management & Governance Blog*.

Troubleshooting

If you have issues with this tutorial, see the following troubleshooting tips.

I'm not seeing the latest data in my report

When you create a report, the organizational view feature doesn't automatically refresh the Trusted Advisor checks in your organization. To get the latest check results, refresh the checks for the management account and each member account in the organization. For more information, see [Refresh Trusted Advisor checks](#) (p. 33).

I have duplicate columns in the report

The Athena console might show the following error in your table if your report has duplicate columns.

HIVE_INVALID_METADATA: Hive metadata for table *folder1* is invalid: Table descriptor contains duplicate columns

For example, if you added a column in your report that already exists, this can cause issues when you try to view the report data in the Athena console. You can follow these steps to fix this issue.

Find duplicate columns

You can use the AWS Glue console to view the schema and quickly identify if you have duplicate columns in your report.

To find duplicate columns

1. Open the AWS Glue console at <https://console.aws.amazon.com/glue/>.
2. If you haven't already, in the **Region selector**, choose the US East (N. Virginia) Region.
3. In the navigation pane, choose **Tables**.
4. Choose your folder name, such as **folder1**, and then under **Schema**, view the values for **Column name**.

If you have a duplicate column, you must upload a new report to your Amazon S3 bucket. See the following [Upload a new report \(p. 49\)](#) section.

Upload a new report

After you identify the duplicate column, we recommend that you replace the existing report with a new one. This ensures that the resources created from this tutorial use the latest report data from your organization.

To upload a new report

1. If you haven't already, refresh your Trusted Advisor checks for the accounts in your organization. See [Refresh Trusted Advisor checks \(p. 33\)](#).
2. Create and download another JSON report in the Trusted Advisor console. See [Create organizational view reports \(p. 33\)](#). You must use a JSON file for this tutorial.
3. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
4. Choose your Amazon S3 bucket and choose the **folder1** folder.
5. Select the previous **resources.json** reports and choose **Delete**.
6. In the **Delete objects** page, under **Permanently delete objects?**, enter **permanently delete**, and then choose **Delete objects**.
7. In your S3 bucket, choose **Upload** and then specify the new report. This action automatically updates your Athena table and AWS Glue crawler resources with the latest report data. It can take a few minutes to refresh your resources.
8. Enter a new query in the Athena console. See [Query the data in Amazon Athena \(p. 44\)](#).

Note

If you still have issues with this tutorial, you can create a technical support case in the [AWS Support Center](#).

Change log for AWS Trusted Advisor checks

See the following topic for recent changes to Trusted Advisor checks.

Note

If you use the Trusted Advisor console or the AWS Support API, checks that were removed won't appear in check results. If you use any of the removed checks such as specifying the check ID in an AWS Support API operation or your code, you must remove these checks to avoid API call errors.

For more information about the available checks, see the [AWS Trusted Advisor check reference \(p. 56\)](#).

Updated check name for Amazon OpenSearch Service

Trusted Advisor updated the Amazon Elasticsearch Reserved Instance Optimization check name to Amazon OpenSearch Service Reserved Instance Optimization on September 8, 2021.

The Amazon OpenSearch Service is a successor to the Amazon Elasticsearch Service. The check recommendations, category, and ID are the same.

Check name	Check category	Check ID
Amazon OpenSearch Service Reserved Instance Optimization	Cost Optimization	7ujm6yhn5t

Note

If you use Trusted Advisor for Amazon CloudWatch metrics, the metric name for this check is also updated. For more information, see [Creating Amazon CloudWatch alarms to monitor AWS Trusted Advisor metrics](#) (p. 124).

Added checks for Amazon Elastic Block Store volume storage

Trusted Advisor added the following checks on June 8, 2021.

Check name	Check category	Check ID
EBS General Purpose SSD (gp3) Volume Storage	Service Limits	dH7RR0l6J3
EBS Provisioned IOPS SSD (io2) Volume Storage	Service Limits	gl7MM0l7J2

Added checks for AWS Lambda

Trusted Advisor added the following checks on March 8, 2021.

Check name	Check category	Check ID
AWS Lambda Functions with Excessive Timeouts	Cost Optimization	L4dfs2Q3C3
AWS Lambda Functions with High Error Rates	Cost Optimization	L4dfs2Q3C2
AWS Lambda Functions Using Deprecated Runtimes	Security	L4dfs2Q4C5
AWS Lambda VPC-enabled Functions without Multi-AZ Redundancy	Fault Tolerance	L4dfs2Q4C6

For more information about how to use these checks with Lambda, see [Example AWS Trusted Advisor workflow to view recommendations](#) in the *AWS Lambda Developer Guide*.

Trusted Advisor check removal

Trusted Advisor removed the following check for the AWS GovCloud (US) Region on March 8, 2021.

Check name	Check category	Check ID
EC2 Elastic IP Addresses	Service Limits	aW9HH0l8J6

Updated checks for Amazon Elastic Block Store

Trusted Advisor updated the unit of Amazon EBS volume from gibibyte (GiB) to tebibyte (TiB) for the following checks on March 5, 2021.

Note

If you use Trusted Advisor for Amazon CloudWatch metrics, the metric names for these five checks are also updated. For more information, see [Creating Amazon CloudWatch alarms to monitor AWS Trusted Advisor metrics](#) (p. 124).

Check name	Check category	Check ID	Updated CloudWatch metric for ServiceLimit
EBS Cold HDD (sc1) Volume Storage	Service Limits	gH5CC0e3J9	Cold HDD (sc1) volume storage (TiB)
EBS General Purpose SSD (gp2) Volume Storage	Service Limits	dH7RR0l6J9	General Purpose SSD (gp2) volume storage (TiB)
EBS Magnetic (standard) Volume Storage	Service Limits	cG7HH0l7J9	Magnetic (standard) volume storage (TiB)
EBS Provisioned IOPS SSD (io1) Volume Storage	Service Limits	gl7MM0l7J9	Provisioned IOPS (SSD) storage (TiB)
EBS Throughput Optimized HDD (st1) Volume Storage	Service Limits	wH7DD0l3J9	Throughput Optimized HDD (st1) volume storage (TiB)

Trusted Advisor check removal

Note

Trusted Advisor removed the following checks on November 18, 2020.

Checks removed on November 18, 2020	Check category	Check ID
EC2Config Service for EC2 Windows Instances	Fault Tolerance	V77iOLlBqz

Checks removed on November 18, 2020	Check category	Check ID
ENA Driver Version for EC2 Windows Instances	Fault Tolerance	TyfdMXG69d
NVMe Driver Version for EC2 Windows Instances	Fault Tolerance	yHAGQJV9K5
PV Driver Version for EC2 Windows Instances	Fault Tolerance	Wnwm9Il5bG
EBS Active Volumes	Service Limits	fH7LL0l7J9

Amazon Elastic Block Store no longer has a limit on the number of volumes that you can provision.

You can monitor your Amazon EC2 instances and verify they are up to date by using [AWS Systems Manager Distributor](#), other third-party tools, or write your own scripts to return driver information for Windows Management Instrumentation (WMI).

Trusted Advisor check removal

Trusted Advisor removed the following check on February 18, 2020.

Check name	Check category	Check ID
Service Limits	Performance	eW7HH0l7J9

Using Trusted Advisor as a web service

The AWS Support service enables you to write applications that interact with [AWS Trusted Advisor](#). This topic shows you how to get a list of Trusted Advisor checks, refresh one of them, and then get the detailed results from the check. These tasks are demonstrated in Java. For information about support for other languages, see [Tools for Amazon Web Services](#).

Topics

- [Get the list of available Trusted Advisor checks \(p. 52\)](#)
- [Refresh the list of available Trusted Advisor checks \(p. 53\)](#)
- [Poll a Trusted Advisor check for status changes \(p. 53\)](#)
- [Request a Trusted Advisor check result \(p. 54\)](#)
- [Print details of a Trusted Advisor check \(p. 55\)](#)

Get the list of available Trusted Advisor checks

The following Java code snippet creates an instance of an AWS Support client that you can use to call all Trusted Advisor API operations. Next, the code gets the list of Trusted Advisor checks and their corresponding `CheckId` values by calling the [DescribeTrustedAdvisorChecks](#) API operation. You can use this information to build user interfaces that enable users to select the check they want to run or refresh.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
```

```
}  
// Get the List of Available Trusted Advisor Checks  
public static void getTAChecks() {  
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),  
    "zh" (Chinese)  
    DescribeTrustedAdvisorChecksRequest request = new  
    DescribeTrustedAdvisorChecksRequest().withLanguage("en");  
    DescribeTrustedAdvisorChecksResult result =  
    createClient().describeTrustedAdvisorChecks(request);  
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {  
        // Do something with check description.  
        System.out.println(description.getId());  
        System.out.println(description.getName());  
    }  
}
```

Refresh the list of available Trusted Advisor checks

The following Java code snippet creates an instance of an AWS Support client that you can use to refresh Trusted Advisor data.

```
// Refresh a Trusted Advisor Check  
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using  
// this operation.  
// Specifying the check ID of a check that is automatically refreshed causes an  
// InvalidParameterValue error.  
public static void refreshTACheck(final String checkId) {  
    RefreshTrustedAdvisorCheckRequest request = new  
    RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);  
    RefreshTrustedAdvisorCheckResult result =  
    createClient().refreshTrustedAdvisorCheck(request);  
    System.out.println("CheckId: " + result.getStatus().getCheckId());  
    System.out.println("Milliseconds until refreshable: " +  
    result.getStatus().getMillisUntilNextRefreshable());  
    System.out.println("Refresh Status: " + result.getStatus().getStatus());  
}
```

Poll a Trusted Advisor check for status changes

After you submit the request to run a Trusted Advisor check to generate the latest status data, you use the [DescribeTrustedAdvisorCheckRefreshStatuses](#) API operation to request the progress of the check's run, and when new data is ready for the check.

The following Java code snippet gets the status of the check requested in the following section, using the value corresponding in the `CheckId` variable. In addition, the code demonstrates several other uses of the Trusted Advisor service:

1. You can call `getMillisUntilNextRefreshable` by traversing the objects contained in the `DescribeTrustedAdvisorCheckRefreshStatusesResult` instance. You can use the value returned to test whether you want your code to proceed with refreshing the check.
2. If `timeUntilRefreshable` equals zero, you can request a refresh of the check.
3. Using the status returned, you can continue to poll for status changes; the code snippet sets the polling interval to a recommended ten seconds. If the status is either `enqueued` or `in_progress`, the loop returns and requests another status. If the call returns `successful`, the loop terminates.
4. Finally, the code returns an instance of a `DescribeTrustedAdvisorCheckResultResult` data type that you can use to traverse the information produced by the check.

Note: Use a single refresh request before polling for the status of the request.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
        new DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
        createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the only
    // element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
    // available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") || status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh status
// for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId) throws
InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
// this operation. This method
// is only functional for checks that can be refreshed using the RefreshTrustedAdvisorCheck
// operation.
public static void pollForTACheckResultChanges(final String checkId) throws
InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus())) {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may not
        // be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
        // only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
            getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Request a Trusted Advisor check result

After you select the check for the detailed results that you want, you submit a request by using the [DescribeTrustedAdvisorCheckResult](#) API operation.

Tip

The names and descriptions for Trusted Advisor checks are subject to change. We recommend that you specify the check ID in your code to uniquely identify a check. You can use the [DescribeTrustedAdvisorChecks](#) API operation to get the check ID.

The following Java code snippet uses the `DescribeTrustedAdvisorChecksResult` instance referenced by the variable `result`, which was obtained in the preceding code snippet. Rather than defining a check interactively through a user interface, After you submit the request to run the snippet submits a request for the first check in the list to be run by specifying an index value of 0 in each `result.getChecks().get(0)` call. Next, the code defines an instance of `DescribeTrustedAdvisorCheckResultRequest`, which it passes to an instance of `DescribeTrustedAdvisorCheckResultResult` called `checkResult`. You can use the member structures of this data type to view the results of the check.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
    DescribeTrustedAdvisorCheckResultRequest()
        // Possible language parameters: "en" (English), "ja" (Japanese),
        "fr" (French), "zh" (Chinese)
        .withLanguage("en")
        .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
    createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

Note: Requesting a Trusted Advisor Check Result doesn't generate updated results data.

Print details of a Trusted Advisor check

The following Java code snippet iterates over the `DescribeTrustedAdvisorCheckResultResult` instance returned in the previous section to get a list of resources flagged by the Trusted Advisor check.

```
// Print ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

AWS Trusted Advisor check reference

You can view all Trusted Advisor check names, descriptions, and IDs in the following reference. You can also sign in to the [Trusted Advisor](#) console to view more information about the checks, recommended actions, and their statuses.

If you have a Business or Enterprise Support plan, you can also use the [AWS Support API](#) and the AWS Command Line Interface (AWS CLI) to access your checks. For more information, see the following topics:

- [Using Trusted Advisor as a web service \(p. 52\)](#)
- [Available AWS Support commands](#) in the *AWS CLI Command Reference*

Note

If you have a Basic Support and Developer Support plan, you can use the Trusted Advisor console to access all checks in the [Service limits \(p. 78\)](#) category and the following checks in the security category:

- [Amazon EBS Public Snapshots \(p. 66\)](#)
- [Amazon RDS Public Snapshots \(p. 66\)](#)
- [Amazon S3 Bucket Permissions \(p. 67\)](#)
- [IAM Use \(p. 70\)](#)
- [MFA on Root Account \(p. 70\)](#)
- [Security Groups – Unrestricted Access \(p. 71\)](#)

Check categories

- [Cost optimization \(p. 56\)](#)
- [Performance \(p. 62\)](#)
- [Security \(p. 65\)](#)
- [Fault tolerance \(p. 71\)](#)
- [Service limits \(p. 78\)](#)

Cost optimization

You can use the following checks for the cost optimization category.

Check names

- [Amazon Comprehend Underutilized Endpoints \(p. 57\)](#)
- [Amazon EC2 Reserved Instance Lease Expiration \(p. 57\)](#)
- [Amazon EC2 Reserved Instance Optimization \(p. 57\)](#)
- [Amazon ElastiCache Reserved Node Optimization \(p. 58\)](#)
- [Amazon OpenSearch Service Reserved Instance Optimization \(p. 58\)](#)
- [Amazon RDS Idle DB Instances \(p. 59\)](#)
- [Amazon Redshift Reserved Node Optimization \(p. 59\)](#)

- [Amazon Relational Database Service \(RDS\) Reserved Instance Optimization \(p. 59\)](#)
- [Amazon Route 53 Latency Resource Record Sets \(p. 60\)](#)
- [AWS Lambda Functions with Excessive Timeouts \(p. 60\)](#)
- [AWS Lambda Functions with High Error Rates \(p. 60\)](#)
- [Idle Load Balancers \(p. 60\)](#)
- [Low Utilization Amazon EC2 Instances \(p. 61\)](#)
- [Savings Plan \(p. 61\)](#)
- [Unassociated Elastic IP Addresses \(p. 61\)](#)
- [Underutilized Amazon EBS Volumes \(p. 62\)](#)
- [Underutilized Amazon Redshift Clusters \(p. 62\)](#)

Amazon Comprehend Underutilized Endpoints

Description

Checks the throughput configuration of your endpoints. This check alerts you when endpoints are not actively used for real-time inference requests. An endpoint that isn't used for more than 15 consecutive days is considered underutilized. All endpoints accrue charges based on both the throughput set, and the length of time that the endpoint is active.

Note

This check is automatically refreshed once a day.

Check ID

Cm24dfsM12

Amazon EC2 Reserved Instance Lease Expiration

Description

Checks for Amazon EC2 Reserved Instances that are scheduled to expire within the next 30 days, or have expired in the preceding 30 days.

Reserved Instances don't renew automatically. You can continue using an Amazon EC2 instance covered by the reservation without interruption, but you will be charged On-Demand rates. New Reserved Instances can have the same parameters as the expired ones, or you can purchase Reserved Instances with different parameters.

The estimated monthly savings is the difference between the On-Demand and Reserved Instance rates for the same instance type.

Check ID

1e93e4c0b5

Amazon EC2 Reserved Instance Optimization

Description

An important part of using AWS involves balancing your Reserved Instance (RI) purchase against your On-Demand Instance usage. This check provides recommendations on which RIs will help reduce the costs incurred from using On-Demand Instances.

We create these recommendations by analyzing your On-Demand usage for the past 30 days. We then categorizing the usage into eligible categories for reservations. We simulate every combination of reservations in the generated category of usage to identify the recommended number of each type of RI to purchase. This process of simulation and optimization allows us to maximize your cost savings. This check covers recommendations based on Standard Reserved Instances with the partial upfront payment option.

This check is not available to accounts linked in consolidated billing. The recommendations for this check are only available for the paying account.

Check ID

cX3c2R1chu

Amazon ElastiCache Reserved Node Optimization

Description

Checks your usage of ElastiCache and provides recommendations on purchase of Reserved Nodes. These recommendations are offered to reduce the costs incurred from using ElastiCache On-Demand. We create these recommendations by analyzing your On-Demand usage for the past 30 days.

We use this analysis to simulate every combination of reservations in the generated usage category. This allows us to recommend the number of each type of Reserved Node to purchase to maximize your savings. This check covers recommendations based on the partial upfront payment option with a 1-year or 3-year commitment.

This check is not available to accounts linked in consolidated billing. The recommendations for this check are only available for the paying account.

Check ID

h3L1otH3re

Amazon OpenSearch Service Reserved Instance Optimization

Description

Checks your usage of Amazon OpenSearch Service (successor to Amazon Elasticsearch Service) and provides recommendations on purchase of Reserved Instances. These recommendations are offered to reduce the costs incurred from using OpenSearch On-Demand. We create these recommendations by analyzing your On-Demand usage for the past 30 days.

We use this analysis to simulate every combination of reservations in the generated usage category. This allows us to recommend the number of each type of Reserved Instance to purchase to maximize your savings. This check covers recommendations based on partial upfront payment option with a 1-year or 3-year commitment.

This check is not available to accounts linked in consolidated billing. The recommendations for this check are only available for the paying account.

Check ID

7ujm6yhn5t

Amazon RDS Idle DB Instances

Description

Checks the configuration of your Amazon Relational Database Service (Amazon RDS) for any database (DB) instances that appear to be idle.

If a DB instance has not had a connection for a prolonged period of time, you can delete the instance to reduce costs. A DB instance is considered idle if the instance hasn't had a connection in the past 7 days. If persistent storage is needed for data on the instance, you can use lower-cost options such as taking and retaining a DB snapshot. Manually created DB snapshots are retained until you delete them.

Check ID

Ti39halfu8

Amazon Redshift Reserved Node Optimization

Description

Checks your usage of Amazon Redshift and provides recommendations on purchase of Reserved Nodes to help reduce costs incurred from using Amazon Redshift On-Demand.

We generate these recommendations by analyzing your On-Demand usage for the past 30 days. We use this analysis to simulate every combination of reservations in the generated usage category. This allows us to identify the best number of each type of Reserved Nodes to purchase to maximize your savings. This check covers recommendations based on partial upfront payment option with a 1-year or 3-year commitment.

This check is not available to accounts linked in consolidated billing. The recommendations for this check are only available for the paying account.

Check ID

1qw23er45t

Amazon Relational Database Service (RDS) Reserved Instance Optimization

Description

Checks your usage of RDS and provides recommendations on purchase of Reserved Instances to help reduce costs incurred from using RDS On-Demand.

We generate these recommendations by analyzing your On-Demand usage for the past 30 days. We use this analysis to simulate every combination of reservations in the generated usage category. This allows us to identify the best number of each type of Reserved Instance to purchase to maximize your savings. This check covers recommendations based on partial upfront payment option with 1-year or 3-year commitment.

This check is not available to accounts linked in consolidated billing. The recommendations for this check are only available for the paying account.

Check ID

1qazXsw23e

Amazon Route 53 Latency Resource Record Sets

Description

Checks for Amazon Route 53 latency record sets that are configured inefficiently.

To allow Amazon Route 53 to route queries to the AWS Region with the lowest network latency, you should create latency resource record sets for a particular domain name (such as example.com) in different Regions. If you create only one latency resource record set for a domain name, all queries are routed to one Region, and you pay extra for latency-based routing without getting the benefits.

Hosted zones created by AWS services won't appear in your check results.

Check ID

51fC20e7I2

AWS Lambda Functions with Excessive Timeouts

Description

Checks for Lambda functions with high timeout rates that might result in high cost.

Lambda charges based on run time and number of requests for your function. Function timeouts result in errors that may cause retries. Retrying functions will incur additionally request and run time charges.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

L4dfs2Q3C3

AWS Lambda Functions with High Error Rates

Description

Checks for Lambda functions with high error rates that might result in higher costs.

Lambda charges are based on the number of requests and aggregate run time for your function. Function errors may cause retries that incur additional charges.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

L4dfs2Q3C2

Idle Load Balancers

Description

Checks your Elastic Load Balancing configuration for load balancers that are idle.

Any load balancer that is configured accrues charges. If a load balancer has no associated back-end instances, or if network traffic is severely limited, the load balancer is not being used effectively. This check currently only checks for Classic Load Balancer type within ELB service. It does not include other ELB types (Application Load Balancer, Network Load Balancer).

Check ID

hjLMh88uM8

Low Utilization Amazon EC2 Instances

Description

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days. This check alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less for at least 4 days.

Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Check ID

Qch7DwouX1

Savings Plan

Description

Checks your usage of Amazon EC2, Fargate, and Lambda over the last 30 days and provides Savings Plan purchase recommendations. These recommendations allow you to commit to a consistent usage amount measured in dollars per hour for a one- or three-year term in exchange for discounted rates.

These are sourced from AWS Cost Explorer, which can get more detailed recommendation information. You can also purchase a savings plan through Cost Explorer. These recommendations should be considered an alternative to your RI recommendations. We suggest that you act on one set of recommendations only. Acting on both sets can lead to over-commitment.

This check is not available to accounts linked in consolidated billing. The recommendations for this check are only available for the paying account.

Check ID

vZ2c2W1srf

Unassociated Elastic IP Addresses

Description

Checks for Elastic IP addresses (EIPs) that are not associated with a running Amazon Elastic Compute Cloud (Amazon EC2) instance.

EIPs are static IP addresses designed for dynamic cloud computing. Unlike traditional static IP addresses, EIPs mask the failure of an instance or Availability Zone by remapping a public IP address to another instance in your account. A nominal charge is imposed for an EIP that is not associated with a running instance.

Check ID

Z4AUBRNSmz

Underutilized Amazon EBS Volumes

Description

Checks Amazon Elastic Block Store (Amazon EBS) volume configurations and warns when volumes appear to be underutilized.

Charges begin when a volume is created. If a volume remains unattached or has very low write activity (excluding boot volumes) for a period of time, the volume is underutilized. We recommend that you remove underutilized volumes to reduce costs.

Check ID

DAvU99Dc4C

Underutilized Amazon Redshift Clusters

Description

Checks your Amazon Redshift configuration for clusters that appear to be underutilized.

If an Amazon Redshift cluster has not had a connection for a prolonged period of time, or is using a low amount of CPU, you can use lower-cost options such as downsizing the cluster, or shutting down the cluster and taking a final snapshot. Final snapshots are retained even after you delete your cluster.

Check ID

G31sQ1E9U

Performance

Improve the performance of your service by checking your service quotas (formerly referred to as limits), so that you can take advantage of provisioned throughput, monitor for overutilized instances, and detect any unused resources.

You can use the following checks for the performance category.

Check names

- [Amazon EBS Provisioned IOPS \(SSD\) Volume Attachment Configuration \(p. 63\)](#)
- [Amazon EC2 to EBS Throughput Optimization \(p. 63\)](#)
- [Amazon Route 53 Alias Resource Record Sets \(p. 63\)](#)
- [CloudFront Alternate Domain Names \(p. 64\)](#)
- [CloudFront Content Delivery Optimization \(p. 64\)](#)
- [CloudFront Header Forwarding and Cache Hit Ratio \(p. 64\)](#)

- [High Utilization Amazon EC2 Instances \(p. 64\)](#)
- [Large Number of EC2 Security Group Rules Applied to an Instance \(p. 65\)](#)
- [Large Number of Rules in an EC2 Security Group \(p. 65\)](#)
- [Overutilized Amazon EBS Magnetic Volumes \(p. 65\)](#)

Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration

Description

Checks for Provisioned IOPS (SSD) volumes that are attached to an Amazon EBS optimizable Amazon Elastic Compute Cloud (Amazon EC2) instance that is not EBS-optimized.

Provisioned IOPS (SSD) volumes in the Amazon Elastic Block Store (Amazon EBS) are designed to deliver the expected performance only when they are attached to an EBS-optimized instance.

Check ID

PPkZrjsH2q

Amazon EC2 to EBS Throughput Optimization

Description

Checks for Amazon EBS volumes whose performance might be affected by the maximum throughput capability of the Amazon EC2 instance they are attached to.

To optimize performance, you should ensure that the maximum throughput of an Amazon EC2 instance is greater than the aggregate maximum throughput of the attached EBS volumes. This check computes the total EBS volume throughput for each five-minute period in the preceding day (based on Coordinated Universal Time (UTC)) for each EBS-optimized instance and alerts you if usage in more than half of those periods was greater than 95% of the maximum throughput of the EC2 instance.

Check ID

Bh2xRR2FGH

Amazon Route 53 Alias Resource Record Sets

Description

Checks for resource record sets that can be changed to alias resource record sets to improve performance and save money.

An alias resource record set routes DNS queries to an AWS resource (for example, an Elastic Load Balancing load balancer or an Amazon S3 bucket) or to another Route 53 resource record set. When you use alias resource record sets, Route 53 routes your DNS queries to AWS resources free of charge.

Hosted zones created by AWS services won't appear in your check results.

Check ID

B913Ef6fb4

CloudFront Alternate Domain Names

Description

Checks Amazon CloudFront distributions for alternate domain names (CNAMES) that have incorrectly configured DNS settings.

If a CloudFront distribution includes alternate domain names, the DNS configuration for the domains must route DNS queries to that distribution.

Note

This check assumes Amazon Route 53 DNS and Amazon CloudFront distribution are configured in the same AWS account. As such the alert list might include resources otherwise working as expected due to DNS setting outside of this AWS account.

Check ID

N420c450f2

CloudFront Content Delivery Optimization

Description

Checks for cases where data transfer from Amazon Simple Storage Service (Amazon S3) buckets could be accelerated by using Amazon CloudFront, the AWS global content delivery service.

When you configure CloudFront to deliver your content, requests for your content are automatically routed to the nearest edge location where content is cached. This routing allows content to be delivered to your users with the best possible performance. A high ratio of data transferred out compared to the data stored in the bucket indicates that you could benefit from using Amazon CloudFront to deliver the data.

Check ID

796d6f3D83

CloudFront Header Forwarding and Cache Hit Ratio

Description

Checks the HTTP request headers that CloudFront currently receives from the client and forwards to your origin server.

Some headers, such as date, or user-agent, significantly reduce the cache hit ratio (the proportion of requests that are served from a CloudFront edge cache). This increases the load on your origin and reduces performance, because CloudFront must forward more requests to your origin.

Check ID

N420c450f2

High Utilization Amazon EC2 Instances

Description

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days. An alert is sent if daily CPU utilization was greater than 90% on four or more days.

Consistent high utilization can indicate optimized, steady performance. However, it can also indicate that an application does not have enough resources. To get daily CPU utilization data, download the report for this check.

Check ID

ZRxQlPsb6c

Large Number of EC2 Security Group Rules Applied to an Instance

Description

Checks for Amazon Elastic Compute Cloud (Amazon EC2) instances that have a large number of security group rules. Performance can be degraded if an instance has a large number of rules.

Check ID

j3DFqYTe29

Large Number of Rules in an EC2 Security Group

Description

Checks each Amazon Elastic Compute Cloud (Amazon EC2) security group for an excessive number of rules.

If a security group has a large number of rules, performance can be degraded.

Check ID

tfG86AVHAZ

Overutilized Amazon EBS Magnetic Volumes

Description

Checks for Amazon Elastic Block Store (Amazon EBS) magnetic volumes that are potentially overutilized and might benefit from a more efficient configuration.

A magnetic volume is designed for applications with moderate or bursty input/output (I/O) requirements, and the IOPS rate is not guaranteed. It delivers approximately 100 IOPS on average, with a best-effort ability to burst to hundreds of IOPS. For consistently higher IOPS, you can use a Provisioned IOPS (SSD) volume. For bursty IOPS, you can use a General Purpose (SSD) volume. For more information, see [Amazon EBS Volume Types](#).

Check ID

k3J2hns32g

Security

You can use the following checks for the security category.

Check names

- [Amazon EBS Public Snapshots \(p. 66\)](#)

- [Amazon RDS Public Snapshots \(p. 66\)](#)
- [Amazon RDS Security Group Access Risk \(p. 67\)](#)
- [Amazon Route 53 MX Resource Record Sets and Sender Policy Framework \(p. 67\)](#)
- [Amazon S3 Bucket Permissions \(p. 67\)](#)
- [AWS CloudTrail Logging \(p. 67\)](#)
- [AWS Lambda Functions Using Deprecated Runtimes \(p. 68\)](#)
- [CloudFront Custom SSL Certificates in the IAM Certificate Store \(p. 68\)](#)
- [CloudFront SSL Certificate on the Origin Server \(p. 68\)](#)
- [ELB Listener Security \(p. 69\)](#)
- [ELB Security Groups \(p. 69\)](#)
- [Exposed Access Keys \(p. 69\)](#)
- [IAM Access Key Rotation \(p. 70\)](#)
- [IAM Password Policy \(p. 70\)](#)
- [IAM Use \(p. 70\)](#)
- [MFA on Root Account \(p. 70\)](#)
- [Security Groups – Specific Ports Unrestricted \(p. 71\)](#)
- [Security Groups – Unrestricted Access \(p. 71\)](#)

Amazon EBS Public Snapshots

Description

Checks the permission settings for your Amazon Elastic Block Store (Amazon EBS) volume snapshots and alerts you if any snapshots are marked as public.

When you make a snapshot public, you give all AWS accounts and users access to all the data on the snapshot. If you want to share a snapshot only with specific users or accounts, mark the snapshot as private. Then, specify the user or accounts you want to share the snapshot data with.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

ePs02jT06w

Amazon RDS Public Snapshots

Description

Checks the permission settings for your Amazon Relational Database Service (Amazon RDS) DB snapshots and alerts you if any snapshots are marked as public.

When you make a snapshot public, you give all AWS accounts and users access to all the data on the snapshot. If you want to share a snapshot only with specific users or accounts, mark the snapshot as private. Then, specify the user or accounts you want to share the snapshot data with.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

rSs93HQwa1

Amazon RDS Security Group Access Risk

Description

Checks security group configurations for Amazon Relational Database Service (Amazon RDS) and warns when a security group rule grants overly permissive access to your database. The recommended configuration for a security group rule is to allow access only from specific Amazon Elastic Compute Cloud (Amazon EC2) security groups or from a specific IP address.

Check ID

nNauJisYIT

Amazon Route 53 MX Resource Record Sets and Sender Policy Framework

Description

For each MX resource record set, checks that the TXT or SPF resource record set contains a valid SPF record. The record must start with "v=spf1". The SPF record specifies the servers that are authorized to send email for your domain, which helps detect and stop email address spoofing and to reduce spam. Route 53 recommends that you use a TXT record instead of an SPF record. Trusted Advisor reports this check as green as long as each MX resource record set has at least one SPF or TXT record.

Check ID

c9D319e7sG

Amazon S3 Bucket Permissions

Description

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions, or that allow access to any authenticated AWS user.

This check examines explicit bucket permissions, as well as bucket policies that might override those permissions. Granting list access permissions to all users for an Amazon S3 bucket is not recommended. These permissions can lead to unintended users listing objects in the bucket at high frequency, which can result in higher than expected charges. Permissions that grant upload and delete access to everyone can lead to security vulnerabilities in your bucket.

Check ID

Pfx0RwqBli

AWS CloudTrail Logging

Description

Checks your use of AWS CloudTrail. CloudTrail provides increased visibility into activity in your AWS account by recording information about AWS API calls made on the account. You can use these logs to determine, for example, what actions a particular user has taken during a specified time period, or which users have taken actions on a particular resource during a specified time period.

Because CloudTrail delivers log files to an Amazon Simple Storage Service (Amazon S3) bucket, CloudTrail must have write permissions for the bucket. If a trail applies to all Regions (the default when creating a new trail), the trail appears multiple times in the Trusted Advisor report.

Check ID

vjaFUGJ9H0

AWS Lambda Functions Using Deprecated Runtimes

Description

Checks for Lambda functions that are configured to use a runtime that is approaching deprecation, or is deprecated. Deprecated runtimes are not eligible for security updates or technical support.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

L4dfs2Q4C5

CloudFront Custom SSL Certificates in the IAM Certificate Store

Description

Checks the SSL certificates for CloudFront alternate domain names in the IAM certificate store. This check alerts you if a certificate is expired, will expire soon, uses outdated encryption, or is not configured correctly for the distribution.

When a custom certificate for an alternate domain name expires, browsers that display your CloudFront content might show a warning message about the security of your website. Certificates that are encrypted by using the SHA-1 hashing algorithm are being deprecated by web browsers such as Chrome and Firefox. A certificate must contain a domain name that matches either the Origin Domain Name or the domain name in the host header of a viewer request. If it doesn't match, CloudFront returns an HTTP status code of 502 (bad gateway) to the user.

For more information, see [Using Alternate Domain Names and HTTPS](#).

Check ID

N425c450f2

CloudFront SSL Certificate on the Origin Server

Description

Checks your origin server for SSL certificates that are expired, about to expire, missing, or that use outdated encryption. If a certificate has one of these issues, CloudFront responds to requests for your content with HTTP status code 502, Bad Gateway.

Check ID

N430c450f2

ELB Listener Security

Description

Checks for load balancers with listeners that do not use recommended security configurations for encrypted communication. AWS recommends using a secure protocol (HTTPS or SSL), up-to-date security policies, as well as ciphers and protocols that are secure.

When you use a secure protocol for a front-end connection (client to load balancer), the requests are encrypted between your clients and the load balancer, which create a more secure environment. Elastic Load Balancing provides predefined security policies with ciphers and protocols that adhere to AWS security best practices. New versions of predefined policies are released as new configurations become available.

Check ID

a2sEc6ILx

ELB Security Groups

Description

Checks for load balancers configured with a missing security group, or a security group that allows access to ports that are not configured for the load balancer.

If a security group associated with a load balancer is deleted, the load balancer will not work as expected. If a security group allows access to ports that are not configured for the load balancer, the risk of loss of data or malicious attacks increases.

Check ID

xSqX82fQu

Exposed Access Keys

Description

Checks popular code repositories for access keys that have been exposed to the public and for irregular Amazon Elastic Compute Cloud (Amazon EC2) usage that could be the result of a compromised access key.

An access key consists of an access key ID and the corresponding secret access key. Exposed access keys pose a security risk to your account and other users, could lead to excessive charges from unauthorized activity or abuse, and violate the [AWS Customer Agreement](#).

If your access key is exposed, take immediate action to secure your account. To protect your account from excessive charges, AWS temporarily limits your ability to create some AWS resources. This does not make your account secure. It only partially limits the unauthorized usage for which you could be charged.

Note

This check doesn't guarantee the identification of exposed access keys or compromised EC2 instances. You are ultimately responsible for the safety and security of your access keys and AWS resources.

Check ID

12Fnkp18Y5

IAM Access Key Rotation

Description

Checks for active IAM access keys that have not been rotated in the last 90 days.

When you rotate your access keys regularly, you reduce the chance that a compromised key could be used without your knowledge to access resources. For the purposes of this check, the last rotation date and time is when the access key was created or most recently activated. The access key number and date come from the `access_key_1_last_rotated` and `access_key_2_last_rotated` information in the most recent IAM credential report.

Check ID

DqdJqYeRm5

IAM Password Policy

Description

Checks the password policy for your account and warns when a password policy is not enabled, or if password content requirements have not been enabled.

Password content requirements increase the overall security of your AWS environment by enforcing the creation of strong user passwords. When you create or change a password policy, the change is enforced immediately for new users but does not require existing users to change their passwords.

Check ID

Yw2K9puPz1

IAM Use

Description

Checks for your use of IAM. You can use IAM to create users, groups, and roles in AWS. You can also use permissions to control access to AWS resources. This check is intended to discourage the use of root access by checking for existence of at least one IAM user.

Check ID

zXCkfM1nI3

MFA on Root Account

Description

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

For increased security, we recommend that you protect your account by using MFA, which requires a user to enter a unique authentication code from their MFA hardware or virtual device when interacting with the AWS Management Console and associated websites.

Check ID

7DAFEmoDos

Security Groups – Specific Ports Unrestricted

Description

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.

If you have intentionally configured your security groups in this manner, we recommend using additional security measures to secure your infrastructure (such as IP tables).

Note

This check only evaluates security groups that you create and their inbound rules for IPv4 addresses. Security groups created by AWS Directory Service are flagged as red or yellow, but they don't pose a security risk and can be safely ignored or excluded. For more information, see the [Trusted Advisor FAQ](#).

Check ID

HCP4007jGY

Security Groups – Unrestricted Access

Description

Checks security groups for rules that allow unrestricted access to a resource.

Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

Note

This check only evaluates security groups that you create and their inbound rules for IPv4 addresses. Security groups created by AWS Directory Service are flagged as red or yellow, but they don't pose a security risk and can be safely ignored or excluded. For more information, see the [Trusted Advisor FAQ](#).

Check ID

1iG5NDGVre

Fault tolerance

You can use the following checks for the fault tolerance category.

Check names

- [Amazon Aurora DB Instance Accessibility \(p. 72\)](#)
- [Amazon Comprehend Endpoint Access Risk \(p. 72\)](#)
- [Amazon EBS Snapshots \(p. 72\)](#)
- [Amazon EC2 Availability Zone Balance \(p. 73\)](#)
- [Amazon RDS Backups \(p. 73\)](#)
- [Amazon RDS Multi-AZ \(p. 73\)](#)
- [Amazon Route 53 Deleted Health Checks \(p. 73\)](#)

- [Amazon Route 53 Failover Resource Record Sets \(p. 74\)](#)
- [Amazon Route 53 High TTL Resource Record Sets \(p. 74\)](#)
- [Amazon Route 53 Name Server Delegations \(p. 74\)](#)
- [Amazon S3 Bucket Logging \(p. 75\)](#)
- [Amazon S3 Bucket Versioning \(p. 75\)](#)
- [Auto Scaling Group Health Check \(p. 75\)](#)
- [Auto Scaling Group Resources \(p. 76\)](#)
- [AWS Direct Connect Connection Redundancy \(p. 76\)](#)
- [AWS Direct Connect Location Redundancy \(p. 76\)](#)
- [AWS Direct Connect Virtual Interface Redundancy \(p. 77\)](#)
- [AWS Lambda VPC-enabled Functions without Multi-AZ Redundancy \(p. 77\)](#)
- [ELB Connection Draining \(p. 77\)](#)
- [ELB Cross-Zone Load Balancing \(p. 77\)](#)
- [Load Balancer Optimization \(p. 78\)](#)
- [VPN Tunnel Redundancy \(p. 78\)](#)

Amazon Aurora DB Instance Accessibility

Description

Checks for cases where an Amazon Aurora DB cluster has both private and public instances.

When your primary instance fails, a replica can be promoted to a primary instance. If that replica is private, users who have only public access would no longer be able to connect to the database after failover. We recommend that all the DB instances in a cluster have the same accessibility.

Check ID

xuy7H1avt1

Amazon Comprehend Endpoint Access Risk

Description

Checks the AWS Key Management Service (AWS KMS) key permissions for an endpoint where the underlying model was encrypted by using customer managed keys. If the customer managed key is disabled, or the key policy was changed to alter the allowed permissions for Amazon Comprehend, the endpoint availability might be affected.

Note

This check is automatically refreshed multiple times a day. It might take a few hours for the latest results to appear.

Check ID

Cm24dfsM13

Amazon EBS Snapshots

Description

Checks the age of the snapshots for your Amazon Elastic Block Store (Amazon EBS) volumes (either available or in-use).

Even though Amazon EBS volumes are replicated, failures can occur. Snapshots are persisted to Amazon Simple Storage Service (Amazon S3) for durable storage and point-in-time recovery.

Check ID

H7IgTzjTYb

Amazon EC2 Availability Zone Balance

Description

Checks the distribution of Amazon Elastic Compute Cloud (Amazon EC2) instances across Availability Zones in a Region.

Availability Zones are distinct locations that are insulated from failures in other Availability Zones. This allows inexpensive, low-latency network connectivity between Availability Zones in the same Region. By launching instances in multiple Availability Zones in the same Region, you can help protect your applications from a single point of failure.

Check ID

wuy7G1zxq1

Amazon RDS Backups

Description

Checks for automated backups of Amazon RDS DB instances.

By default, backups are enabled with a retention period of one day. Backups reduce the risk of unexpected data loss and allow for point-in-time recovery.

Check ID

opQPADkZvH

Amazon RDS Multi-AZ

Description

Checks for DB instances that are deployed in a single Availability Zone (AZ).

Multi-AZ deployments enhance database availability by synchronously replicating to a standby instance in a different Availability Zone. During planned database maintenance, or the failure of a DB instance or Availability Zone, Amazon RDS automatically fails over to the standby. This failover allows database operations to resume quickly without administrative intervention. Because Amazon RDS does not support Multi-AZ deployment for Microsoft SQL Server, this check does not examine SQL Server instances.

Check ID

f2iK5R6Dep

Amazon Route 53 Deleted Health Checks

Description

Checks for resource record sets that are associated with health checks that have been deleted.

Route 53 does not prevent you from deleting a health check that is associated with one or more resource record sets. If you delete a health check without updating the associated resource record sets, the routing of DNS queries for your DNS failover configuration will not work as intended.

Hosted zones created by AWS services won't appear in your check results.

Check ID

Cb877eB72b

Amazon Route 53 Failover Resource Record Sets

Description

Checks for Amazon Route 53 failover resource record sets that have a misconfiguration.

When Amazon Route 53 health checks determine that the primary resource is unhealthy, Amazon Route 53 responds to queries with a secondary, backup resource record set. You must create correctly configured primary and secondary resource record sets for failover to work.

Hosted zones created by AWS services won't appear in your check results.

Check ID

b73EEdD790

Amazon Route 53 High TTL Resource Record Sets

Description

Checks for resource record sets that can benefit from having a lower time-to-live (TTL) value.

TTL is the number of seconds that a resource record set is cached by DNS resolvers. When you specify a long TTL, DNS resolvers take longer to request updated DNS records, which can cause unnecessary delay in rerouting traffic. For example, a long TTL creates a delay between when DNS Failover detects an endpoint failure, and when it responds by rerouting traffic.

Hosted zones created by AWS services won't appear in your check results.

Check ID

C056F80cR3

Amazon Route 53 Name Server Delegations

Description

Checks for Amazon Route 53 hosted zones for which your domain registrar or DNS is not using the correct Route 53 name servers.

When you create a hosted zone, Route 53 assigns a delegation set of four name servers. The names of these servers are ns-###.awsdns-##.com, .net, .org, and .co.uk, where ### and ## typically represent different numbers. Before Route 53 can route DNS queries for your domain, you must update your registrar's name server configuration to remove the name servers that the registrar assigned. Then, you must add all four name servers in the Route 53 delegation set. For maximum availability, you must add all four Route 53 name servers.

Hosted zones created by AWS services won't appear in your check results.

Check ID

cF171Db240

Amazon S3 Bucket Logging

Description

Checks the logging configuration of Amazon Simple Storage Service (Amazon S3) buckets.

When server access logging is enabled, detailed access logs are delivered hourly to a bucket that you choose. An access log record contains details about each request, such as the request type, the resources specified in the request, and the time and date the request was processed. By default, bucket logging is not enabled. You should enable logging if you want to perform security audits or learn more about users and usage patterns.

When logging is initially enabled, the configuration is automatically validated. However, future modifications can result in logging failures. This check examines explicit Amazon S3 bucket permissions, but it does not examine associated bucket policies that might override the bucket permissions.

Check ID

BueAdJ7NrP

Amazon S3 Bucket Versioning

Description

Checks for Amazon Simple Storage Service buckets that do not have versioning enabled, or that have versioning suspended.

When versioning is enabled, you can easily recover from both unintended user actions and application failures. Versioning allows you to preserve, retrieve, and restore any version of any object stored in a bucket. You can use lifecycle rules to manage all versions of your objects, as well as their associated costs, by automatically archiving objects to the Glacier storage class. Rules can also be configured to remove versions of your objects after a specified period of time. You can also require multi-factor authentication (MFA) for any object deletions or configuration changes to your buckets.

Versioning can't be deactivated after it has been enabled. However, it can be suspended, which prevents new versions of objects from being created. Using versioning can increase your costs for Amazon S3, because you pay for storage of multiple versions of an object.

Check ID

R365s2Qddf

Auto Scaling Group Health Check

Description

Examines the health check configuration for Auto Scaling groups.

If Elastic Load Balancing is being used for an Auto Scaling group, the recommended configuration is to enable an Elastic Load Balancing health check. If an Elastic Load Balancing health check is not

used, Auto Scaling can only act upon the health of the Amazon Elastic Compute Cloud (Amazon EC2) instance. Auto Scaling will not act on the application running on the instance.

Check ID

CLOG40CD08

Auto Scaling Group Resources

Description

Checks the availability of resources associated with launch configurations and your Auto Scaling groups.

Auto Scaling groups that point to unavailable resources cannot launch new Amazon Elastic Compute Cloud (Amazon EC2) instances. When properly configured, Auto Scaling causes the number of Amazon EC2 instances to increase seamlessly during demand spikes, and decrease automatically during demand lulls. Auto Scaling groups and launch configurations that point to unavailable resources do not operate as intended.

Check ID

8CNsS11I5v

AWS Direct Connect Connection Redundancy

Description

Checks for AWS Regions that have only one AWS Direct Connect connection. Connectivity to your AWS resources should have two Direct Connect connections configured at all times to provide redundancy in case a device is unavailable.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

0t121N1Ty3

AWS Direct Connect Location Redundancy

Description

Checks for AWS Regions with one or more AWS Direct Connect connections and only one AWS Direct Connect location. Connectivity to your AWS resources should have Direct Connect connections configured to different Direct Connect locations to provide redundancy in case a location is unavailable.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

8M012Ph3U5

AWS Direct Connect Virtual Interface Redundancy

Description

Checks for virtual private gateways with AWS Direct Connect virtual interfaces (VIFs) that are not configured on at least two AWS Direct Connect connections. Connectivity to your virtual private gateway should have multiple VIFs configured across multiple Direct Connect connections and locations. This provides redundancy in case that a device or location is unavailable.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

4g3Nt5M1Th

AWS Lambda VPC-enabled Functions without Multi-AZ Redundancy

Description

Checks for VPC-enabled Lambda functions that are vulnerable to service interruption in a single Availability Zone. It is recommended for VPC-enabled functions to be connected to multiple Availability Zones for high availability.

Note

Results for this check are automatically refreshed several times daily, and refresh requests are not allowed. It might take a few hours for changes to appear.

Check ID

L4dfs2Q4C6

ELB Connection Draining

Description

Checks for load balancers that do not have connection draining enabled.

When connection draining is not enabled and you deregister an Amazon EC2 instance from a load balancer, the load balancer stops routing traffic to that instance and closes the connection. When connection draining is enabled, the load balancer stops sending new requests to the deregistered instance but keeps the connection open to serve active requests.

Check ID

7qGXsKIUw

ELB Cross-Zone Load Balancing

Description

With cross-zone load balancing turned off, there is a risk of service unavailability due to uneven distribution of traffic or backend overloading. This problem can occur when clients incorrectly cache

DNS information. The problem can also occur when there are an unequal number of instances in each Availability Zone (for example, if you have taken down some instances for maintenance).

Check ID

xdeXZKIUy

Load Balancer Optimization

Description

Checks your load balancer configuration.

To help increase the level of fault tolerance in Amazon Elastic Compute Cloud (Amazon EC2) when using Elastic Load Balancing, we recommend running an equal number of instances across multiple Availability Zones in a Region. A load balancer that is configured accrues charges, so this is a cost-optimization check as well.

Check ID

iqdCTZKCUp

VPN Tunnel Redundancy

Description

Checks the number of tunnels that are active for each of your VPNs.

A VPN should have two tunnels configured at all times. This provides redundancy in case of outage or planned maintenance of the devices at the AWS endpoint. For some hardware, only one tunnel is active at a time. If a VPN has no active tunnels, charges for the VPN might still apply. For more information, see [AWS Client VPN Administrator Guide](#).

Check ID

S45wrEXrLz

Service limits

See the following checks for the service limits (also known as quotas) category.

Note

Values are based on a snapshot, so your current usage might differ. Quota and usage data can take up to 24 hours to reflect any changes. In cases where quotas have been recently increased, you might temporarily see utilization that exceeds the quota.

Check names

- [Auto Scaling Groups \(p. 80\)](#)
- [Auto Scaling Launch Configurations \(p. 80\)](#)
- [CloudFormation Stacks \(p. 80\)](#)
- [DynamoDB Read Capacity \(p. 80\)](#)
- [DynamoDB Write Capacity \(p. 80\)](#)
- [EBS Active Snapshots \(p. 81\)](#)

- [EBS Cold HDD \(sc1\) Volume Storage \(p. 81\)](#)
- [EBS General Purpose SSD \(gp2\) Volume Storage \(p. 81\)](#)
- [EBS General Purpose SSD \(gp3\) Volume Storage \(p. 81\)](#)
- [EBS Magnetic \(standard\) Volume Storage \(p. 81\)](#)
- [EBS Provisioned IOPS \(SSD\) Volume Aggregate IOPS \(p. 82\)](#)
- [EBS Provisioned IOPS SSD \(io1\) Volume Storage \(p. 82\)](#)
- [EBS Provisioned IOPS SSD \(io2\) Volume Storage \(p. 82\)](#)
- [EBS Throughput Optimized HDD \(st1\) Volume Storage \(p. 82\)](#)
- [EC2 On-Demand Instances \(p. 82\)](#)
- [EC2 Reserved Instance Leases \(p. 83\)](#)
- [EC2-Classic Elastic IP Addresses \(p. 83\)](#)
- [EC2-VPC Elastic IP Address \(p. 83\)](#)
- [ELB Application Load Balancers \(p. 83\)](#)
- [ELB Classic Load Balancers \(p. 83\)](#)
- [ELB Network Load Balancers \(p. 83\)](#)
- [IAM Group \(p. 84\)](#)
- [IAM Instance Profiles \(p. 84\)](#)
- [IAM Policies \(p. 84\)](#)
- [IAM Roles \(p. 84\)](#)
- [IAM Server Certificates \(p. 84\)](#)
- [IAM Users \(p. 85\)](#)
- [Kinesis Shards per Region \(p. 85\)](#)
- [RDS Cluster Parameter Groups \(p. 85\)](#)
- [RDS Cluster Roles \(p. 85\)](#)
- [RDS Clusters \(p. 85\)](#)
- [RDS DB Instances \(p. 85\)](#)
- [RDS DB Manual Snapshots \(p. 86\)](#)
- [RDS DB Parameter Groups \(p. 86\)](#)
- [RDS DB Security Groups \(p. 86\)](#)
- [RDS Event Subscriptions \(p. 86\)](#)
- [RDS Max Auths per Security Group \(p. 86\)](#)
- [RDS Option Groups \(p. 87\)](#)
- [RDS Read Replicas per Master \(p. 87\)](#)
- [RDS Reserved Instances \(p. 87\)](#)
- [RDS Subnet Groups \(p. 87\)](#)
- [RDS Subnets per Subnet Group \(p. 87\)](#)
- [RDS Total Storage Quota \(p. 87\)](#)
- [Route 53 Hosted Zones \(p. 88\)](#)
- [Route 53 Max Health Checks \(p. 88\)](#)
- [Route 53 Reusable Delegation Sets \(p. 88\)](#)
- [Route 53 Traffic Policies \(p. 88\)](#)

- [Route 53 Traffic Policy Instances \(p. 88\)](#)
- [SES Daily Sending Quota \(p. 89\)](#)
- [VPC \(p. 89\)](#)
- [VPC Internet Gateways \(p. 89\)](#)

Auto Scaling Groups

Description

Checks for usage that is more than 80% of the Auto Scaling Groups quota.

Check ID

fW7HH017J9

Auto Scaling Launch Configurations

Description

Checks for usage that is more than 80% of the Auto Scaling launch configurations quota.

Check ID

aW7HH017J9

CloudFormation Stacks

Description

Checks for usage that is more than 80% of the CloudFormation stacks quota.

Check ID

gW7HH017J9

DynamoDB Read Capacity

Description

Checks for usage that is more than 80% of the DynamoDB provisioned throughput limit for reads per AWS account.

Check ID

6gtQddfEw6

DynamoDB Write Capacity

Description

Checks for usage that is more than 80% of the DynamoDB provisioned throughput limit for writes per AWS account.

Check ID

c5ftjdfkMr

EBS Active Snapshots

Description

Checks for usage that is more than 80% of the EBS active snapshots quota.

Check ID

eI7KK017J9

EBS Cold HDD (sc1) Volume Storage

Description

Checks for usage that is more than 80% of the EBS Cold HDD (sc1) volume storage quota.

Check ID

gH5CC0e3J9

EBS General Purpose SSD (gp2) Volume Storage

Description

Checks for usage that is more than 80% of the EBS General Purpose SSD (gp2) volume storage quota.

Check ID

dH7RR016J9

EBS General Purpose SSD (gp3) Volume Storage

Description

Checks for usage that is more than 80% of the EBS General Purpose SSD (gp3) volume storage quota.

Check ID

dH7RR016J3

EBS Magnetic (standard) Volume Storage

Description

Checks for usage that is more than 80% of the EBS Magnetic (standard) volume storage quota.

Check ID

cG7HH017J9

EBS Provisioned IOPS (SSD) Volume Aggregate IOPS

Description

Checks for usage that is more than 80% of the EBS Provisioned IOPS (SSD) volume aggregate IOPS quota.

Check ID

tV7YY017J9

EBS Provisioned IOPS SSD (io1) Volume Storage

Description

Checks for usage that is more than 80% of the EBS Provisioned IOPS SSD (io1) volume storage quota.

Check ID

gI7MM017J9

EBS Provisioned IOPS SSD (io2) Volume Storage

Description

Checks for usage that is more than 80% of the EBS Provisioned IOPS SSD (io2) volume storage quota.

Check ID

gI7MM017J2

EBS Throughput Optimized HDD (st1) Volume Storage

Description

Checks for usage that is more than 80% of the EBS Throughput Optimized HDD (st1) volume storage quota.

Check ID

wH7DD013J9

EC2 On-Demand Instances

Description

Checks for usage that is more than 80% of the EC2 On-Demand Instances quota.

Check ID

0Xc6LMYG8P

EC2 Reserved Instance Leases

Description

Checks for usage that is more than 80% of the EC2 Reserved Instance leases quota.

Check ID

iH7PP017J9

EC2-Classic Elastic IP Addresses

Description

Checks for usage that is more than 80% of the EC2-Classic Elastic IP addresses quota.

Check ID

aW9HH018J6

EC2-VPC Elastic IP Address

Description

Checks for usage that is more than 80% of the EC2-VPC Elastic IP address quota.

Check ID

1N7RR017J9

ELB Application Load Balancers

Description

Checks for usage that is more than 80% of the ELB Application Load Balancers quota.

Check ID

EM8b3yLRTr

ELB Classic Load Balancers

Description

Checks for usage that is more than 80% of the ELB Classic Load Balancers quota.

Check ID

iK700017J9

ELB Network Load Balancers

Description

Checks for usage that is more than 80% of the ELB Network Load Balancers quota.

Check ID

8wIqYSt25K

IAM Group

Description

Checks for usage that is more than 80% of the IAM group quota.

Check ID

sU7XX017J9

IAM Instance Profiles

Description

Checks for usage that is more than 80% of the IAM instance profiles quota.

Check ID

nO7SS017J9

IAM Policies

Description

Checks for usage that is more than 80% of the IAM policies quota.

Check ID

pR7UU017J9

IAM Roles

Description

Checks for usage that is more than 80% of the IAM roles quota.

Check ID

oQ7TT017J9

IAM Server Certificates

Description

Checks for usage that is more than 80% of the IAM server certificates quota.

Check ID

rT7WW017J9

IAM Users

Description

Checks for usage that is more than 80% of the IAM users quota.

Check ID

qS7VV017J9

Kinesis Shards per Region

Description

Checks for usage that is more than 80% of the Kinesis shards per Region quota.

Check ID

bW7HH017J9

RDS Cluster Parameter Groups

Description

Checks for usage that is more than 80% of the RDS cluster parameter groups quota.

Check ID

jtlIMO3qZM

RDS Cluster Roles

Description

Checks for usage that is more than 80% of the RDS cluster roles quota.

Check ID

7fuccf1Mx7

RDS Clusters

Description

Checks for usage that is more than 80% of the RDS clusters quota.

Check ID

gjqMBn6pjz

RDS DB Instances

Description

Checks for usage that is more than 80% of the RDS DB instances quota.

Check ID

XG0aXHpIEt

RDS DB Manual Snapshots

Description

Checks for usage that is more than 80% of the RDS DB manual snapshots quota.

Check ID

dV84wpqRUs

RDS DB Parameter Groups

Description

Checks for usage that is more than 80% of the RDS DB parameter groups quota.

Check ID

jEECYg2YVU

RDS DB Security Groups

Description

Checks for usage that is more than 80% of the RDS DB security groups quota.

Check ID

gfZAn3W7w1

RDS Event Subscriptions

Description

Checks for usage that is more than 80% of the RDS event subscriptions quota.

Check ID

keAhfbH5yb

RDS Max Auths per Security Group

Description

Checks for usage that is more than 80% of the RDS max auths per security group quota.

Check ID

dBkuNCvqn5

RDS Option Groups

Description

Checks for usage that is more than 80% of the RDS option groups quota.

Check ID

3Njm0DJQ09

RDS Read Replicas per Master

Description

Checks for usage that is more than 80% of the RDS read replicas per master quota.

Check ID

pYW8UkYz2w

RDS Reserved Instances

Description

Checks for usage that is more than 80% of the RDS Reserved Instances quota.

Check ID

UUDvOa5r34

RDS Subnet Groups

Description

Checks for usage that is more than 80% of the RDS subnet groups quota.

Check ID

dYWBaXaaMM

RDS Subnets per Subnet Group

Description

Checks for usage that is more than 80% of the RDS subnets per subnet group quota.

Check ID

jEhCtdJKOY

RDS Total Storage Quota

Description

Checks for usage that is more than 80% of the RDS total storage quota.

Check ID

P1jhKWEmLa

Route 53 Hosted Zones

Description

Checks for usage that is more than 80% of the Route 53 hosted zones quota per account.

Check ID

dx3xfcdfMr

Route 53 Max Health Checks

Description

Checks for usage that is more than 80% of the Route 53 health checks quota per account.

Check ID

ru4xfcdfMr

Route 53 Reusable Delegation Sets

Description

Checks for usage that is more than 80% of the Route 53 reusable delegation sets quota per account.

Check ID

ty3xfcdfMr

Route 53 Traffic Policies

Description

Checks for usage that is more than 80% of the Route 53 traffic policies quota per account.

Check ID

dx3xfbjfMr

Route 53 Traffic Policy Instances

Description

Checks for usage that is more than 80% of the Route 53 traffic policy instances quota per account.

Check ID

dx8afcdfMr

SES Daily Sending Quota

Description

Checks for usage that is more than 80% of the Amazon SES daily sending quota.

Check ID

hJ7NN017J9

VPC

Description

Checks for usage that is more than 80% of the VPC quota.

Check ID

jL7PP017J9

VPC Internet Gateways

Description

Checks for usage that is more than 80% of the VPC Internet gateways quota.

Check ID

kM7QQ017J9

Security in AWS Support

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is 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 AWS Support, 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 AWS Support. The following topics show you how to configure AWS Support to meet your security and compliance objectives. You also learn how to use other Amazon Web Services that help you to monitor and secure your AWS Support resources.

Topics

- [Data protection in AWS Support \(p. 90\)](#)
- [Identity and access management for AWS Support \(p. 91\)](#)
- [Incident response \(p. 113\)](#)
- [Logging and Monitoring in AWS Support \(p. 113\)](#)
- [Compliance validation for AWS Support \(p. 133\)](#)
- [Resilience in AWS Support \(p. 134\)](#)
- [Infrastructure security in AWS Support \(p. 134\)](#)
- [Configuration and vulnerability analysis in AWS Support \(p. 134\)](#)

Data protection in AWS Support

The AWS [shared responsibility model](#) applies to data protection in AWS Support. 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 AWS Support 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.

Identity and access management for AWS Support

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use AWS Support resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience \(p. 91\)](#)
- [Authenticating with identities \(p. 92\)](#)
- [Managing access using policies \(p. 93\)](#)
- [How AWS Support works with IAM \(p. 95\)](#)
- [AWS Support identity-based policy examples \(p. 96\)](#)
- [Using service-linked roles \(p. 98\)](#)
- [AWS managed policies for AWS Support and AWS Trusted Advisor \(p. 102\)](#)
- [Manage access for AWS Trusted Advisor \(p. 107\)](#)
- [Troubleshooting AWS Support identity and access \(p. 111\)](#)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in AWS Support.

Service user – If you use the AWS Support service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more AWS Support features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in AWS Support, see [Troubleshooting AWS Support identity and access \(p. 111\)](#).

Service administrator – If you're in charge of AWS Support resources at your company, you probably have full access to AWS Support. It's your job to determine which AWS Support features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with AWS Support, see [How AWS Support works with IAM \(p. 95\)](#).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to AWS Support. To view example AWS Support identity-based policies that you can use in IAM, see [AWS Support identity-based policy examples \(p. 96\)](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see [Signing in to the AWS Management Console as an IAM user or root user](#) in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the [AWS Management Console](#), use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see [Signature Version 4 signing process](#) in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the [best practice of using the root user only to create your first IAM user](#). Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see [Managing access keys for IAM users](#) in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or AWS API

operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an [identity provider](#). For more information about federated users, see [Federated users and roles](#) in the *IAM User Guide*.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
- **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, Resources, and Condition Keys for AWS Support](#) in the *Service Authorization Reference*.
- **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

How AWS Support works with IAM

Before you use IAM to manage access to AWS Support, you should understand what IAM features are available to use with AWS Support. To get a high-level view of how AWS Support and other AWS services work with IAM, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Topics

- [AWS Support identity-based policies \(p. 95\)](#)
- [AWS Support IAM roles \(p. 95\)](#)

AWS Support identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. AWS Support supports specific actions. To learn about the elements that you use in a JSON policy, see [IAM JSON policy elements reference](#) in the *IAM User Guide*.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The **Action** element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in AWS Support use the following prefix before the action: `support:`. For example, to grant someone permission to run an Amazon EC2 instance with the Amazon EC2 `RunInstances` API operation, you include the `ec2:RunInstances` action in their policy. Policy statements must include either an **Action** or **NotAction** element. AWS Support defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [
    "ec2:action1",
    "ec2:action2"
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "ec2:Describe*"
```

To see a list of AWS Support actions, see [Actions Defined by AWS Support](#) in the *IAM User Guide*.

Examples

To view examples of AWS Support identity-based policies, see [AWS Support identity-based policy examples \(p. 96\)](#).

AWS Support IAM roles

An [IAM role](#) is an entity within your AWS account that has specific permissions.

Using temporary credentials with AWS Support

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as [AssumeRole](#) or [GetFederationToken](#).

AWS Support supports using temporary credentials.

Service-linked roles

[Service-linked roles](#) allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

AWS Support supports service-linked roles. For details about creating or managing AWS Support service-linked roles, see [Using service-linked roles for AWS Support \(p. 98\)](#).

Service roles

This feature allows a service to assume a [service role](#) on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

AWS Support supports service roles.

AWS Support identity-based policy examples

By default, IAM users and roles don't have permission to create or modify AWS Support resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see [Creating policies on the JSON tab](#) in the *IAM User Guide*.

Topics

- [Policy best practices \(p. 96\)](#)
- [Using the AWS Support console \(p. 97\)](#)
- [Allow users to view their own permissions \(p. 97\)](#)

Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete AWS Support resources in your account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get Started Using AWS Managed Policies** – To start using AWS Support quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see [Get started using permissions with AWS managed policies](#) in the *IAM User Guide*.
- **Grant Least Privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see [Grant least privilege](#) in the *IAM User Guide*.

- **Enable MFA for Sensitive Operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.
- **Use Policy Conditions for Extra Security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.

Using the AWS Support console

To access the AWS Support console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS Support resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (IAM users or roles) with that policy.

To be sure that those entities can still use the AWS Support console, also attach the following AWS managed policy to the entities. For more information, see [Adding permissions to a user](#) in the *IAM User Guide*:

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or 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": "*"
    }
  ]
}
```



```
} ]
```

Using service-linked roles

AWS Support and AWS Trusted Advisor use AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique IAM role that is linked directly to AWS Support and Trusted Advisor. In each case, the service-linked role is a predefined role. This role includes all the permissions that AWS Support or Trusted Advisor require to call other AWS services on your behalf. The following topics explain what service-linked roles do and how to work with them in AWS Support and Trusted Advisor.

Topics

- [Using service-linked roles for AWS Support \(p. 98\)](#)
- [Using service-linked roles for Trusted Advisor \(p. 99\)](#)

Using service-linked roles for AWS Support

AWS Support tools gather information about your AWS resources through API calls to provide customer service and technical support. To increase the transparency and auditability of support activities, AWS Support uses an AWS Identity and Access Management (IAM) [service-linked role](#).

The `AWSServiceRoleForSupport` service-linked role is a unique IAM role that is linked directly to AWS Support. This service-linked role is predefined, and it includes the permissions that AWS Support requires to call other AWS services on your behalf.

The `AWSServiceRoleForSupport` service-linked role trusts the `support.amazonaws.com` service to assume the role.

To provide these services, the role's predefined permissions give AWS Support access to resource metadata, not customer data. Only AWS Support tools can assume this role, which exists within your AWS account.

We redact fields that could contain customer data. For example, the `Input` and `Output` fields of the [GetExecutionHistory](#) for the AWS Step Functions API call aren't visible to AWS Support.

Note

AWS Trusted Advisor uses a separate IAM service-linked role to access AWS resources for your account to provide best practice recommendations and checks. For more information, see [Using service-linked roles for Trusted Advisor \(p. 99\)](#).

The `AWSServiceRoleForSupport` service-linked role enables all AWS Support API calls to be visible to customers through AWS CloudTrail. This helps with monitoring and auditing requirements, because it provides a transparent way to understand the actions that AWS Support performs on your behalf. For information about CloudTrail, see the [AWS CloudTrail User Guide](#).

Service-linked role permissions for AWS Support

This role uses the `AWSSupportServiceRolePolicy` AWS managed policy. This managed policy is attached to the role and allows the role permission to complete actions on your behalf.

These actions might include the following:

- **Billing, administrative, support, and other customer services** – AWS customer service uses the permissions granted by the managed policy to perform a number of services as part of your support plan. These include investigating and answering account and billing questions, providing

administrative support for your account, increasing service quotas, and offering additional customer support.

- **Processing of service attributes and usage data for your AWS account** – AWS Support might use the permissions granted by the managed policy to access service attributes and usage data for your AWS account. This policy allows AWS Support to provide billing, administrative, and technical support for your account. Service attributes include your account's resource identifiers, metadata tags, roles, and permissions. Usage data includes usage policies, usage statistics, and analytics.
- **Maintaining the operational health of your account and its resources** – AWS Support uses automated tools to perform actions related to operational and technical support.

For more information about the allowed services and actions, see the [AWSSupportServiceRolePolicy](#) policy in the IAM console.

Note

AWS Support automatically updates the `AWSSupportServiceRolePolicy` policy once per month to add permissions for new AWS services and actions.

For more information, see [AWS managed policies for AWS Support and AWS Trusted Advisor \(p. 102\)](#).

Creating a service-linked role for AWS Support

You don't need to manually create the `AWSServiceRoleForSupport` role. When you create an AWS account, this role is automatically created and configured for you.

Important

If you used AWS Support before it began supporting service-linked roles, then AWS created the `AWSServiceRoleForSupport` role in your account. For more information, see [A new role appeared in my IAM account](#).

Editing and deleting a service-linked role for AWS Support

You can use IAM to edit the description for the `AWSServiceRoleForSupport` service-linked role. For more information, see [Editing a service-linked role](#) in the *IAM User Guide*.

The `AWSServiceRoleForSupport` role is necessary for AWS Support to provide administrative, operational, and technical support for your account. As a result, this role can't be deleted through the IAM console, API, or AWS Command Line Interface (AWS CLI). This protects your AWS account, because you can't inadvertently remove necessary permissions for administering support services.

For more information about the `AWSServiceRoleForSupport` role or its uses, contact [AWS Support](#).

Using service-linked roles for Trusted Advisor

AWS Trusted Advisor uses the AWS Identity and Access Management (IAM) [service-linked role](#). A service-linked role is a unique IAM role that is linked directly to AWS Trusted Advisor. Service-linked roles are predefined by Trusted Advisor, and they include all the permissions that the service requires to call other AWS services on your behalf. Trusted Advisor uses this role to check your usage across AWS and to provide recommendations to improve your AWS environment. For example, Trusted Advisor analyzes your Amazon Elastic Compute Cloud (Amazon EC2) instance use to help you reduce costs, increase performance, tolerate failures, and improve security.

Note

AWS Support uses a separate IAM service-linked role for accessing your account's resources to provide billing, administrative, and support services. For more information, see [Using service-linked roles for AWS Support \(p. 98\)](#).

For information about other services that support service-linked roles, see [AWS services that work with IAM](#). Look for the services that have **Yes** in the **Service-linked role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Topics

- [Service-linked role permissions for Trusted Advisor \(p. 100\)](#)
- [Manage permissions for service-linked roles \(p. 100\)](#)
- [Creating a service-linked role for Trusted Advisor \(p. 101\)](#)
- [Editing a service-linked role for Trusted Advisor \(p. 102\)](#)
- [Deleting a service-linked role for Trusted Advisor \(p. 102\)](#)

Service-linked role permissions for Trusted Advisor

Trusted Advisor uses two service-linked roles:

- [AWSServiceRoleForTrustedAdvisor](#) – This role trusts the Trusted Advisor service to assume the role to access AWS services on your behalf. The role permissions policy allows Trusted Advisor read-only access for all AWS resources. This role simplifies getting started with your AWS account, because you don't have to add the necessary permissions for Trusted Advisor. When you open an AWS account, Trusted Advisor creates this role for you. The defined permissions include the trust policy and the permissions policy. You can't attach the permissions policy to any other IAM entity.

For more information about the attached policy, see [AWSTrustedAdvisorServiceRolePolicy \(p. 103\)](#).

- [AWSServiceRoleForTrustedAdvisorReporting](#) – This role trusts the Trusted Advisor service to assume the role for the organizational view feature. This role enables Trusted Advisor as a trusted service in your AWS Organizations organization. Trusted Advisor creates this role for you when you enable organizational view.

For more information about the attached policy, see [AWSTrustedAdvisorReportingServiceRolePolicy \(p. 105\)](#).

You can use the organizational view to create reports for Trusted Advisor check results for all accounts in your organization. For more information about this feature, see [Organizational view for AWS Trusted Advisor \(p. 31\)](#).

Manage permissions for service-linked roles

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. The following examples use the `AWSServiceRoleForTrustedAdvisor` service-linked role.

Example : Allow an IAM entity to create the `AWSServiceRoleForTrustedAdvisor` service-linked role

This step is necessary only if the Trusted Advisor account is disabled, the service-linked role is deleted, and the user must recreate the role to reenable Trusted Advisor.

You can add the following statement to the permissions policy for the IAM entity to create the service-linked role.

```
{
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole",
    "iam:PutRolePolicy"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor*",
  "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Allow an IAM entity to edit the description of the `AWSServiceRoleForTrustedAdvisor` service-linked role

You can only edit the description for the `AWSServiceRoleForTrustedAdvisor` role. You can add the following statement to the permissions policy for the IAM entity to edit the description of a service-linked role.

```
{
  "Effect": "Allow",
  "Action": [
    "iam:UpdateRoleDescription"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor*",
  "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Allow an IAM entity to delete the `AWSServiceRoleForTrustedAdvisor` service-linked role

You can add the following statement to the permissions policy for the IAM entity to delete a service-linked role.

```
{
  "Effect": "Allow",
  "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor*",
  "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

You can also use an AWS managed policy, such as [AdministratorAccess](#), to provide full access to Trusted Advisor.

Creating a service-linked role for Trusted Advisor

You don't need to manually create the `AWSServiceRoleForTrustedAdvisor` service-linked role. When you open an AWS account, Trusted Advisor creates the service-linked role for you.

Important

If you were using the Trusted Advisor service before it began supporting service-linked roles, then Trusted Advisor already created the `AWSServiceRoleForTrustedAdvisor` role in your account. To learn more, see [A new role appeared in my IAM account](#) in the *IAM User Guide*.

If your account doesn't have the `AWSServiceRoleForTrustedAdvisor` service-linked role, then Trusted Advisor won't work as expected. This can happen if someone in your account disabled Trusted Advisor and then deleted the service-linked role. In this case, you can use IAM to create the `AWSServiceRoleForTrustedAdvisor` service-linked role, and then reenable Trusted Advisor.

To enable Trusted Advisor (console)

1. Use the IAM console, AWS CLI, or the IAM API to create a service-linked role for Trusted Advisor. For more information, see [Creating a service-linked role](#).
2. Sign in to the AWS Management Console, and then navigate to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.

The **Disabled Trusted Advisor** status banner appears in the console.

3. Choose **Enable Trusted Advisor Role** from the status banner. If the required `AWSServiceRoleForTrustedAdvisor` isn't detected, the disabled status banner remains.

Editing a service-linked role for Trusted Advisor

You can't change the name of a service-linked role because various entities might reference the role. However, you can use the IAM console, AWS CLI, or the IAM API to edit the description of the role. For more information, see [Editing a service-linked role](#) in the *IAM User Guide*.

Deleting a service-linked role for Trusted Advisor

If you don't need to use the features or services of Trusted Advisor, you can delete the `AWSServiceRoleForTrustedAdvisor` role. You must disable Trusted Advisor before you can delete this service-linked role. This prevents you from removing permissions required by Trusted Advisor operations. When you disable Trusted Advisor, you disable all service features, including offline processing and notifications. Also, if you disable Trusted Advisor for a member account, then the separate payer account is also affected, which means you won't receive Trusted Advisor checks that identify ways to save costs. You can't access the Trusted Advisor console. API calls to Trusted Advisor return an access denied error.

You must recreate the `AWSServiceRoleForTrustedAdvisor` service-linked role in the account before you can reenable Trusted Advisor.

You must first disable Trusted Advisor in the console before you can delete the `AWSServiceRoleForTrustedAdvisor` service-linked role.

To disable Trusted Advisor

1. Sign in to the AWS Management Console and navigate to the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor>.
2. In the navigation pane, choose **Preferences**.
3. In the **Service Linked Role Permissions** section, choose **Disable Trusted Advisor**.
4. In the confirmation dialog box, choose **OK** to confirm that you want to disable Trusted Advisor.

After you disable Trusted Advisor, all Trusted Advisor functionality is disabled, and the Trusted Advisor console displays only the disabled status banner.

You can then use the IAM console, the AWS CLI, or the IAM API to delete the Trusted Advisor service-linked role named `AWSServiceRoleForTrustedAdvisor`. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

AWS managed policies for AWS Support and AWS Trusted Advisor

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to [create IAM customer managed policies](#) that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](#) in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy

is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ViewOnlyAccess** AWS managed policy provides read-only access to many AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](#) in the *IAM User Guide*.

Contents

- [AWS managed policy: AWSSupportServiceRolePolicy](#) (p. 103)
- [AWS managed policy: AWSTrustedAdvisorServiceRolePolicy](#) (p. 103)
- [AWS managed policy: AWSTrustedAdvisorReportingServiceRolePolicy](#) (p. 105)
- [AWS Support and Trusted Advisor updates to AWS managed policies](#) (p. 106)

AWS managed policy: AWSSupportServiceRolePolicy

AWS Support uses the [AWSSupportServiceRolePolicy](#) AWS managed policy. This managed policy is attached to the `AWSServiceRoleForSupport` service-linked role. The policy allows the service-linked role to complete actions on your behalf. You can't attach this policy to your IAM entities. For more information, see [Service-linked role permissions for AWS Support](#) (p. 98).

AWS managed policy: AWSTrustedAdvisorServiceRolePolicy

This policy is attached to the `AWSServiceRoleForTrustedAdvisor` service-linked role. It allows the service-linked role to perform actions on your behalf. You can't attach the [AWSTrustedAdvisorServiceRolePolicy](#) to your IAM entities. For more information, see [Using service-linked roles for Trusted Advisor](#) (p. 99).

This policy grants administrative permissions that allow the service-linked role to access AWS services. These permissions allow the checks for Trusted Advisor to evaluate your account.

Permissions details

This policy includes the following permissions.

- `AutoScaling` – Describes Amazon EC2 Auto Scaling account quotas and resources
- `cloudformation` – Describes AWS CloudFormation (CloudFormation) account quotas and stacks
- `cloudfront` – Describes Amazon CloudFront distributions
- `cloudtrail` – Describes AWS CloudTrail (CloudTrail) trails
- `dynamodb` – Describes Amazon DynamoDB account quotas and resources
- `ec2` – Describes Amazon Elastic Compute Cloud (Amazon EC2) account quotas and resources
- `elasticloadbalancing` – Describes Elastic Load Balancing account quotas and resources
- `iam` – Gets IAM resources, such as credentials, password policy, and certificates
- `kinesis` – Describes Amazon Kinesis (Kinesis) account quotas
- `rds` – Describes Amazon Relational Database Service (Amazon RDS) resources

- `redshift` – Describes Amazon Redshift resources
- `route53` – Describes Amazon Route 53 account quotas and resources
- `s3` – Describes Amazon Simple Storage Service (Amazon S3) resources
- `ses` – Gets Amazon Simple Email Service (Amazon SES) send quotas
- `sqs` – Lists Amazon Simple Queue Service (Amazon SQS) queues
- `cloudwatch` – Gets Amazon CloudWatch Events (CloudWatch Events) metric statistics
- `ce` – Gets Cost Explorer Service (Cost Explorer) recommendations

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "kinesis:DescribeLimits",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",

```

```
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:ListQueues",
        "cloudwatch:GetMetricStatistics",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation"
    ],
    "Resource": "*"
}
]
```

AWS managed policy: AWSTrustedAdvisorReportingServiceRolePolicy

This policy is attached to the `AWSServiceRoleForTrustedAdvisorReporting` service-linked role that allows Trusted Advisor to perform actions for the organizational view feature. You can't attach the [AWSTrustedAdvisorReportingServiceRolePolicy](#) to your IAM entities. For more information, see [Using service-linked roles for Trusted Advisor](#) (p. 99).

This policy grants administrative permissions that allow the service-linked role to perform AWS Organizations actions.

Permissions details

This policy includes the following permissions.

- `organizations` – Describes your organization and lists the service access, accounts, parents, children, and organizational units

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

AWS Support and Trusted Advisor updates to AWS managed policies

View details about updates to AWS managed policies for AWS Support and Trusted Advisor since these services began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the [Document history \(p. 137\)](#) page.

Change	Description	Date
AWS Trusted Advisor Service Role Policy – Update to an existing policy	<p>Trusted Advisor added new actions to grant the <code>DescribeTargetGroups</code> and <code>GetAccountPublicAccessBlock</code> permissions.</p> <p>The <code>DescribeTargetGroup</code> permission is required for the Auto Scaling Group Health Check to retrieve non-Classic Load Balancers that are attached to an Auto Scaling group.</p> <p>The <code>GetAccountPublicAccessBlock</code> permission is required for the Amazon S3 Bucket Permissions check to retrieve the block public access settings for an AWS account.</p>	August 10, 2021
AWS Support and Trusted Advisor started tracking changes	AWS Support and Trusted Advisor started tracking changes for their AWS managed policies.	August 10, 2021

Manage access for AWS Trusted Advisor

You can access AWS Trusted Advisor from the AWS Management Console. All AWS accounts have access to a select core [Trusted Advisor checks](#). If you have a Business or Enterprise support plan, you can access all checks. For more information, see [AWS Trusted Advisor check reference \(p. 56\)](#).

You can use AWS Identity and Access Management (IAM) to control access to Trusted Advisor.

Topics

- [Permissions for the Trusted Advisor console \(p. 107\)](#)
- [Trusted Advisor actions \(p. 107\)](#)
- [IAM policy examples \(p. 109\)](#)
- [See also \(p. 111\)](#)

Permissions for the Trusted Advisor console

You must have a minimum set of permissions to access the Trusted Advisor console. These permissions must allow you to list and view details about the Trusted Advisor resources in your AWS account.

You can use the following options to control access to Trusted Advisor:

- Use the tag filter feature of the Trusted Advisor console. The user or role must have permissions associated with the tags.

You can use AWS managed policies or custom policies to assign permissions by tags. For more information, see [Obtaining Permissions for Tagging](#).

- Create an IAM policy with the `trustedadvisor` namespace, so that you can specify permissions to actions and resources.

When you create a policy, you can specify the namespace of the service to allow or deny an action. The namespace for Trusted Advisor is `trustedadvisor`.

Important

You can't use the `trustedadvisor` namespace to allow or deny Trusted Advisor API operations in the AWS Support API. The namespace for AWS Support is `support`.

Trusted Advisor actions

You can perform the following Trusted Advisor actions in the console. You can also specify these Trusted Advisor actions in an IAM policy to allow or deny specific actions.

Action	Description
<code>DescribeAccount</code>	Grants permission to view the AWS Support plan and various Trusted Advisor preferences.
<code>DescribeAccountAccess</code>	Grants permission to view if the AWS account has enabled or disabled Trusted Advisor.
<code>DescribeCheckItems</code>	Grants permission to view details for the check items.
<code>DescribeCheckRefreshStatuses</code>	Grants permission to view the refresh statuses for Trusted Advisor checks.

Action	Description
<code>DescribeCheckSummaries</code>	Grants permission to view Trusted Advisor check summaries.
<code>DescribeChecks</code>	Grants permission to view details for Trusted Advisor checks.
<code>DescribeNotificationPreferences</code>	Grants permission to view the notification preferences for the AWS account.
<code>ExcludeCheckItems</code>	Grants permission to exclude recommendations for Trusted Advisor checks.
<code>IncludeCheckItems</code>	Grants permission to include recommendations for Trusted Advisor checks.
<code>RefreshCheck</code>	Grants permission to refresh a Trusted Advisor check.
<code>SetAccountAccess</code>	Grants permission to enable or disable Trusted Advisor for the account.
<code>UpdateNotificationPreferences</code>	Grants permission to update notification preferences for Trusted Advisor.

The following Trusted Advisor actions are for the organizational view feature. For more information, see [Organizational view for AWS Trusted Advisor \(p. 31\)](#).

Action	Description
<code>DescribeOrganization</code>	Grants permission to view if the AWS account meets the requirements to enable the organizational view feature.
<code>DescribeOrganizationAccounts</code>	Grants permission to view the linked AWS accounts that are in the organization.
<code>DescribeReports</code>	Grants permission to view details for organizational view reports, such as the report name, runtime, date created, status, and format.
<code>DescribeServiceMetadata</code>	Grants permission to view information about organizational view reports, such as the AWS Regions, check categories, check names, and resource statuses.
<code>GenerateReport</code>	Grants permission to create a report for Trusted Advisor checks in your organization.
<code>ListAccountsForParent</code>	Grants permission to view, in the Trusted Advisor console, all of the accounts in an AWS organization that are contained by a root or organizational unit (OU).
<code>ListOrganizationalUnitsForParent</code>	Grants permission to view, in the Trusted Advisor console, all of the organizational units (OUs) in a parent organizational unit or root.

Action	Description
ListRoots	Grants permission to view, in the Trusted Advisor console, all of the roots that are defined in an AWS organization.
SetOrganizationAccess	Grants permission to enable the organizational view feature for Trusted Advisor.

IAM policy examples

The following policies show you how to allow and deny access to Trusted Advisor. You can use one of the following policies to create a *customer managed policy* in the IAM console. For example, you can copy an example policy, and then paste it into the [JSON tab](#) of the IAM console. Then, you attach the policy to your IAM user, group, or role.

For more information about how to create an IAM policy, see [Creating IAM policies \(console\)](#) in the *IAM User Guide*.

Examples

- [Full access to Trusted Advisor \(p. 109\)](#)
- [Read-only access to Trusted Advisor \(p. 109\)](#)
- [Deny access to Trusted Advisor \(p. 110\)](#)
- [Allow and deny specific actions \(p. 110\)](#)
- [Control access to the AWS Support API operations for Trusted Advisor \(p. 110\)](#)

Full access to Trusted Advisor

The following policy allows users to view and take all actions on all Trusted Advisor checks in the Trusted Advisor console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "trustedadvisor:*",
      "Resource": "*"
    }
  ]
}
```

Read-only access to Trusted Advisor

The following policy allows users read-only access to the Trusted Advisor console. Users can't make changes, such as refresh checks or change notification preferences.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "trustedadvisor:Describe*",
      "Resource": "*"
    }
  ]
}
```

```
}
```

Deny access to Trusted Advisor

The following policy doesn't allow users to view or take actions for Trusted Advisor checks in the Trusted Advisor console.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "trustedadvisor:*",
      "Resource": "*"
    }
  ]
}
```

Allow and deny specific actions

The following policy allows users to view all Trusted Advisor checks in the Trusted Advisor console, but doesn't allow them to refresh any checks.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "trustedadvisor:*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "trustedadvisor:RefreshCheck",
      "Resource": "*"
    }
  ]
}
```

Control access to the AWS Support API operations for Trusted Advisor

In the AWS Management Console, a separate `trustedadvisor` IAM namespace controls access to Trusted Advisor. You can't use the `trustedadvisor` namespace to allow or deny Trusted Advisor API operations in the AWS Support API. Instead, you use the `support` IAM namespace. You must have permissions to the AWS Support API to call Trusted Advisor programmatically.

For example, if you want to call the [RefreshTrustedAdvisorCheck](#) operation, you must have permissions to this action in the policy.

Example : Allow Trusted Advisor API operations only

The following policy allows users access to the AWS Support API operations for Trusted Advisor, but not the rest of the AWS Support API operations. For example, users can use the API to view and refresh checks. They can't create, view, update, or resolve AWS Support cases.

You can use this policy to call the Trusted Advisor API operations programmatically, but you can't use this policy to view or refresh checks in the Trusted Advisor console.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "support:DescribeTrustedAdvisorCheckRefreshStatuses",
    "support:DescribeTrustedAdvisorCheckResult",
    "support:DescribeTrustedAdvisorChecks",
    "support:DescribeTrustedAdvisorCheckSummaries",
    "support:RefreshTrustedAdvisorCheck",
    "trustedadvisor:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Deny",
  "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeAttachment",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:DescribeServices",
    "support:DescribeSeverityLevels",
    "support:ResolveCase"
  ],
  "Resource": "*"
}
]
```

For more information about how IAM works with AWS Support and Trusted Advisor, see [Actions \(p. 95\)](#).

See also

For more information about Trusted Advisor permissions, see the following resources:

- [Actions defined by AWS Trusted Advisor in the IAM User Guide](#).
- [Controlling Access to the Trusted Advisor Console](#)

Troubleshooting AWS Support identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS Support and IAM.

Topics

- [I'm not authorized to perform iam:PassRole \(p. 111\)](#)
- [I want to view my access keys \(p. 112\)](#)
- [I'm an administrator and want to allow others to access AWS Support \(p. 112\)](#)
- [I want to allow people outside of my AWS account to access my AWS Support resources \(p. 112\)](#)

I'm not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to AWS Support.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in AWS Support. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

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

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

Important

Do not provide your access keys to a third party, even to help [find your canonical user ID](#). By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see [Managing access keys](#) in the *IAM User Guide*.

I'm an administrator and want to allow others to access AWS Support

To allow others to access AWS Support, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in AWS Support.

To get started right away, see [Creating your first IAM delegated user and group](#) in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my AWS Support resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether AWS Support supports these features, see [How AWS Support works with IAM](#) (p. 95).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.

- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

Incident response

Incident response for AWS Support is an AWS responsibility. AWS has a formal, documented policy and program that governs incident response. For more information, see the [Introducing the AWS Security Incident Response Whitepaper](#).

Use the following options to inform yourself about operational issues:

- View AWS operational issues with broad impact on the [AWS Service Health Dashboard](#). For example, events that affect a service or Region that isn't specific to your account.
- View operational issues for individual accounts in the [AWS Personal Health Dashboard](#). For example, events that affect services or resources in your account. For more information, see [Getting started with the AWS Personal Health Dashboard](#) in the *AWS Health User Guide*.

Logging and Monitoring in AWS Support

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

- *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](#).
- *Amazon CloudWatch Events* delivers a near real-time stream of system events that describe changes in AWS resources. CloudWatch Events enables automated event-driven computing, as you can write rules that watch for certain events and trigger automated actions in other AWS services when these events happen. For more information, see the [Amazon CloudWatch Events User Guide](#).
- *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](#).

Topics

- [Logging AWS Support API calls with AWS CloudTrail \(p. 113\)](#)
- [Logging AWS Trusted Advisor console actions with AWS CloudTrail \(p. 118\)](#)
- [Monitoring Trusted Advisor checks \(p. 122\)](#)

Logging AWS Support API calls with AWS CloudTrail

AWS Support is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Support. CloudTrail captures API calls for AWS Support as events. The calls captured include calls from the AWS Support console and code calls to the AWS Support API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon Simple Storage Service (Amazon S3) bucket, including events for AWS Support. 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 AWS Support, 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, including how to configure and enable it, see the [AWS CloudTrail User Guide](#).

AWS Support information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in AWS Support, 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 AWS Support, 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](#) and [Receiving CloudTrail log files from multiple accounts](#)

All AWS Support API operations are logged by CloudTrail and are documented in the [AWS Support API Reference](#).

For example, calls to the `CreateCase`, `DescribeCases` and `ResolveCase` operations 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](#).

You can also aggregate AWS Support log files from multiple AWS Regions and multiple AWS accounts into a single Amazon S3 bucket.

AWS Trusted Advisor information in CloudTrail logging

Trusted Advisor is an AWS Support service that you can use to check your AWS account for ways to save costs, improve security, and optimize your account.

All Trusted Advisor API operations are logged by CloudTrail and are documented in the [AWS Support API Reference](#).

For example, calls to the `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` and `RefreshTrustedAdvisorCheck` operations generate entries in the CloudTrail log files.

Note

CloudTrail also logs Trusted Advisor console actions. See [Logging AWS Trusted Advisor console actions with AWS CloudTrail \(p. 118\)](#).

Understanding AWS Support 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. It includes information about the requested operation, the date and time of the operation, 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.

Example : Log entry for CreateCase

The following example shows a CloudTrail log entry for the [CreateCase](#) operation.

```
{
  "Records": [
    {
      "eventVersion": "1.04",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "janedoe",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2016-04-13T17:51:37Z"
          }
        }
      },
      "invokedBy": "signin.amazonaws.com"
    },
    {
      "eventTime": "2016-04-13T18:05:53Z",
      "eventSource": "support.amazonaws.com",
      "eventName": "CreateCase",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "198.51.100.15",
      "userAgent": "signin.amazonaws.com",
      "requestParameters": {
        "severityCode": "low",
        "categoryCode": "other",
        "language": "en",
        "serviceCode": "support-api",
        "issueType": "technical"
      },
      "responseElements": {
        "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
      },
      "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
      "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ],
  ...
}
```

Example : Log entry for RefreshTrustedAdvisorCheck

The following example shows a CloudTrail log entry for the [RefreshTrustedAdvisorCheck](#) operation.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/Admin",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Admin"
  },
  "eventTime": "2020-10-21T16:34:13Z",
  "eventSource": "support.amazonaws.com",
  "eventName": "RefreshTrustedAdvisorCheck",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.21.198.67",
  "userAgent": "aws-cli/1.18.140 Python/3.6.12
Linux/4.9.217-0.3.ac.206.84.332.metall1.x86_64 botocore/1.17.63",
  "requestParameters": {
    "checkId": "Pfx0RwqBli"
  },
  "responseElements": null,
  "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
  "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Logging changes to your AWS Support plan

When you change or view your Support plan on the [Support plans](#) page, CloudTrail logs the following console actions:

- `DescribeSupportLevelSummary` – This action appears in your log when you open the [Support plans](#) page.
- `UpdateProbationAutoCancellation` – After you sign up for Developer Support or Business Support and then try to cancel within 30 days, your plan will be automatically canceled at the end of that period. This action appears in your log when you choose **Opt-out of automatic cancellation** in the banner that appears on the [Support plans](#) page. You will resume your plan for Developer Support or Business Support.
- `UpdateSupportLevel` – This action appears in your log when you change your Support plan.

Notes

- Only a root user in your AWS account can perform these actions on the [Support plans](#) page. For more information, see [Changing your AWS Support plan \(p. 12\)](#).
- The `eventSource` field has the `support-subscription.amazonaws.com` namespace for these actions.

Example : Log entry for DescribeSupportLevelSummary

The following example shows a CloudTrail log entry for the `DescribeSupportLevelSummary` action.

```
{
  "eventVersion": "1.08",
```

```
"userIdentity": {
  "type": "Root",
  "principalId": "111122223333",
  "arn": "arn:aws:iam::111122223333:root",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "sessionIssuer": {},
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-01-07T22:08:05Z"
    }
  }
},
"eventTime": "2021-01-07T22:08:07Z",
"eventSource": "support-subscription.amazonaws.com",
"eventName": "DescribeSupportLevelSummary",
"awsRegion": "us-east-1",
"sourceIPAddress": "100.127.8.67",
"userAgent": "AWS-SupportPlansConsole, aws-internal/3",
"requestParameters": {
  "lang": "en"
},
"responseElements": null,
"requestID": "b423b84d-829b-4090-a239-2b639b123abc",
"eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333"
}
```

Example : Log entry for UpdateProbationAutoCancellation

The following example shows a CloudTrail log entry for the UpdateProbationAutoCancellation action.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

```
}
```

Example : Log entry for UpdateSupportLevel

The following example shows a CloudTrail log entry for the UpdateSupportLevel action to change to Developer Support.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Logging AWS Trusted Advisor console actions with AWS CloudTrail

Trusted Advisor is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Trusted Advisor. CloudTrail captures actions for Trusted Advisor as events. The calls captured include calls from the Trusted Advisor console. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon Simple Storage Service (Amazon S3) bucket, including events for Trusted Advisor. 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 Trusted Advisor, 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, including how to configure and enable it, see the [AWS CloudTrail User Guide](#).

Trusted Advisor information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in the Trusted Advisor console, 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 Trusted Advisor, 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](#) and [Receiving CloudTrail Log Files from Multiple Accounts](#)

Trusted Advisor supports logging a subset of the Trusted Advisor console actions as events in CloudTrail log files. CloudTrail logs the following actions:

- DescribeAccount
- DescribeAccountAccess
- DescribeChecks
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeNotificationPreferences
- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- IncludeCheckItems
- ListAccountsForParent
- ListRoots
- ListOrganizationalUnitsForParent
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateNotificationPreferences

For a complete list of Trusted Advisor console actions, see [Trusted Advisor actions \(p. 107\)](#).

Note

CloudTrail also logs the Trusted Advisor API operations in the [AWS Support API Reference](#). For more information, see [Logging AWS Support API calls with AWS CloudTrail \(p. 113\)](#).

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](#).

Example: Trusted Advisor 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.

Example : Log entry for RefreshCheck

The following example shows a CloudTrail log entry that demonstrates the RefreshCheck action for the Amazon S3 Bucket Versioning check (ID R365s2Qddf).

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "janedoe",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-10-21T22:06:18Z"
      }
    }
  },
  "eventTime": "2020-10-21T22:06:33Z",
  "eventSource": "trustedadvisor.amazonaws.com",
  "eventName": "RefreshCheck",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.34.136",
  "userAgent": "AWS-TrustedAdvisor, aws-internal/3 aws-sdk-java/1.11.841
Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
java/1.8.0_262 vendor/Oracle_Corporation",
  "requestParameters": {
    "checkId": "R365s2Qddf"
  },
  "responseElements": {
    "status": {
      "checkId": "R365s2Qddf",
      "status": "enqueued",
      "millisUntilNextRefreshable": 3599993
    }
  },
  "requestID": "d23ec729-8995-494c-8054-dedeaEXAMPLE",
  "eventID": "a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
  "eventType": "AwsApiCall",
}
```

```
}
  "recipientAccountId": "123456789012"
}
```

Example : Log entry for UpdateNotificationPreferences

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

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "janedoe",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-10-21T22:06:18Z"
      }
    }
  },
  "eventTime": "2020-10-21T22:09:49Z",
  "eventSource": "trustedadvisor.amazonaws.com",
  "eventName": "UpdateNotificationPreferences",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.34.167",
  "userAgent": "AWS-TrustedAdvisor, aws-internal/3 aws-sdk-java/1.11.841
Linux/4.9.217-0.3.ac.206.84.332.metall1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
java/1.8.0_262 vendor/Oracle_Corporation",
  "requestParameters": {
    "contacts": [
      {
        "id": "billing",
        "type": "email",
        "active": false
      },
      {
        "id": "operational",
        "type": "email",
        "active": false
      },
      {
        "id": "security",
        "type": "email",
        "active": false
      }
    ],
    "language": "en"
  },
  "responseElements": null,
  "requestID": "695295f3-c81c-486e-9404-fa148EXAMPLE",
  "eventID": "5f923d8c-d210-4037-bd32-997c6EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Example : Log entry for GenerateReport

The following example shows a CloudTrail log entry that demonstrates the GenerateReport action. This action creates a report for your AWS organization.

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "janedoe",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-11-03T13:03:10Z"
      }
    }
  },
  "eventTime": "2020-11-03T13:04:29Z",
  "eventSource": "trustedadvisor.amazonaws.com",
  "eventName": "GenerateReport",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.36.171",
  "userAgent": "AWS-TrustedAdvisor, aws-internal/3 aws-sdk-java/1.11.864
Linux/4.9.217-0.3.ac.206.84.332.metall1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
java/1.8.0_262 vendor/Oracle_Corporation",
  "requestParameters": {
    "refresh": false,
    "includeSuppressedResources": false,
    "language": "en",
    "format": "JSON",
    "name": "organizational-view-report",
    "preference": {
      "accounts": [

      ],
      "organizationalUnitIds": [
        "r-j134"
      ],
      "preferenceName": "organizational-view-report",
      "format": "json",
      "language": "en"
    }
  },
  "responseElements": {
    "status": "ENQUEUED"
  },
  "requestID": "bb866dc1-60af-47fd-a660-21498EXAMPLE",
  "eventID": "2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Monitoring Trusted Advisor checks

AWS Trusted Advisor checks identify ways for you to reduce cost, increase performance, and improve security for your AWS account. You can use Amazon CloudWatch Events to monitor the status of Trusted Advisor checks. You can then use Amazon CloudWatch to create alarms on Trusted Advisor metrics. These alarms notify you when the status changes for a Trusted Advisor check, such as an updated resource or a service quota that is reached.

For example, Trusted Advisor provides the **Amazon S3 Bucket Permissions** check. This check identifies if you have buckets that have open access permissions or allow access to any authenticated AWS user. If a

bucket permission changes, the status changes for the Trusted Advisor check. CloudWatch Events detects this event and then sends you a notification so that you can take action.

Topics

- [Monitoring Trusted Advisor check results with Amazon CloudWatch Events \(p. 123\)](#)
- [Creating Amazon CloudWatch alarms to monitor AWS Trusted Advisor metrics \(p. 124\)](#)

Monitoring Trusted Advisor check results with Amazon CloudWatch Events

You can use Amazon CloudWatch Events to detect and react to changes in the status of Trusted Advisor checks. Then, based on the rules that you create, CloudWatch Events invokes one or more target actions when a check status changes to the value you specify in a rule. Depending on the type of status change, you might want to send notifications, capture status information, take corrective action, initiate events, or take other actions. You can select the following types of targets when using CloudWatch Events as a part of your Trusted Advisor workflow:

- AWS Lambda functions
- Amazon Kinesis streams
- Amazon Simple Queue Service queues
- Built-in targets (CloudWatch alarm actions)
- Amazon Simple Notification Service topics

The following are some use cases:

- Use a Lambda function to pass a notification to a Slack channel when check status changes.
- Push data about checks to a Kinesis stream to support comprehensive, real-time status monitoring.

For examples of using CloudWatch Events and Lambda functions to automate the response to Trusted Advisor check results, see [Trusted Advisor tools](#).

The remainder of this topic describes the basic procedure for creating a CloudWatch Events rule for Trusted Advisor. Before you create event rules for Trusted Advisor, however, you should do the following:

- Familiarize yourself with events, rules, and targets in CloudWatch Events. For more information, see [What is Amazon CloudWatch Events?](#) and [New CloudWatch Events – track and respond to changes to your AWS resources](#).
- Create the target or targets you will use in your event rules.

To create a CloudWatch Events rule for Trusted Advisor

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation bar, choose the **US East (N. Virginia)** Region.
3. In the navigation pane, choose **Events**.
4. Choose **Create rule**, and then under **Event Source**, for **Service Name**, choose **Trusted Advisor**.
5. Specify status values:
 - To make a rule that applies to all status values, choose **Check Item Refresh Status**, and then choose **Any status** (the default).
 - To make a rule that applies to some status values only, choose **Specific status(es)**, and then choose one or more status values from the list.

6. Specify Trusted Advisor checks:
 - To make a rule that applies to all Trusted Advisor checks, choose **Any check**.
 - To make a rule that applies to some checks only, choose **Specific check(s)**, and then choose one or more check names from the list.
7. Specify AWS resources:
 - To make a rule that applies to all resources, choose **Any resource ID**.
 - To make a rule that applies to one or more resources only, choose **Specific resource ID(s) by ARN**. Then, enter the ARNs of the resources.
8. Review your rule setup to make sure it meets your event-monitoring requirements.
9. In the **Targets** area, choose **Add target***.
10. In the **Select target type** list, choose the type of target you prepared to use with this rule. Then, configure any additional options required by that type.
11. Choose **Configure details**.
12. On the **Configure rule details** page, enter a name and description for the rule. To enable the rule as soon as it's created, choose the **State** box.
13. If you're satisfied with the rule, choose **Create rule**.

Creating Amazon CloudWatch alarms to monitor AWS Trusted Advisor metrics

When AWS Trusted Advisor refreshes your checks, Trusted Advisor publishes metrics about your check results to CloudWatch. You can view the metrics in CloudWatch. You can also create alarms to detect status changes to Trusted Advisor checks and status changes for resources, and service quota usage (formerly referred to as limits). For example, you might create an alarm to track status changes for checks in the **Service Limits** category. The alarm will then notify you when you reach or exceed a service quota for your AWS account.

Follow this procedure to create a CloudWatch alarm for a specific Trusted Advisor metric.

Topics

- [Prerequisites \(p. 124\)](#)
- [CloudWatch metrics for Trusted Advisor \(p. 127\)](#)
- [Trusted Advisor metrics and dimensions \(p. 132\)](#)

Prerequisites

Before you create CloudWatch alarms for Trusted Advisor metrics, review the following information:

- Understand how CloudWatch uses metrics and alarms. For more information, see [How CloudWatch works](#) in the *Amazon CloudWatch User Guide*.
- Use the Trusted Advisor console or the AWS Support API to refresh your checks and get the latest check results. For more information, see [Refresh check results \(p. 30\)](#).

To create a CloudWatch alarm for Trusted Advisor metrics

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Use the **Region selector** and choose the **US East (N. Virginia)** AWS Region.
3. In the navigation pane, choose **Alarms**.
4. Choose **Create alarm**.

5. Choose **Select metric**.
6. For **Metrics**, enter one or more dimension values to filter the metric list. For example, you can enter the metric name **ServiceLimitUsage** or the dimension, such as the Trusted Advisor check name.

Tip

- You can search for **Trusted Advisor** to list all metrics for the service.
 - For a list of metric and dimension names, see [Trusted Advisor metrics and dimensions \(p. 132\)](#).
7. In the results table, select the check box for the metric.

In the following example, the check name is **IAM Access Key Rotation** and the metric name is **YellowResources**.

N. Virginia	All > TrustedAdvisor > Check Metrics	Trusted	Advisor	IAM	Access	Key
<input type="checkbox"/>	CheckName (2)	Metric Name				
<input type="checkbox"/>	IAM Access Key Rotation	RedResources				
<input checked="" type="checkbox"/>	IAM Access Key Rotation	YellowResources				

8. Choose **Select metric**.
9. On the **Specify metric and conditions** page, verify that the **Metric name** and **CheckName** that you chose appear on the page.
10. For **Period**, you can specify the time period that you want the alarm to start when the check status changes, such as 5 minutes.
11. Under **Conditions**, choose **Static**, and then specify the alarm condition for when the alarm should start.

For example, if you choose **Greater/Equal >=threshold** and enter **1** for the threshold value, this means that the alarm starts when Trusted Advisor detects at least one IAM access key that hasn't been rotated in the last 90 days.

Notes

- For the **GreenChecks**, **RedChecks**, **YellowChecks**, **RedResources**, and **YellowResources** metrics, you can specify a threshold that is any whole number greater than or equal to zero.
 - Trusted Advisor doesn't send metrics for **GreenResources**, which are resources for which Trusted Advisor hasn't detected any issues.
12. Choose **Next**.
 13. On the **Configure actions** page, for **Alarm state trigger**, choose **In alarm**.
 14. For **Select an SNS topic**, choose an existing Amazon Simple Notification Service (Amazon SNS) topic or create one.

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

☒ In alarm
The metric or expression is outside of the defined threshold.

☐ OK
The metric or expression is within the defined threshold.

☐ Insufficient data
The alarm has just started or not enough data is available.

Select an SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ Select an existing SNS topic

☐ Create new topic

☐ Use topic ARN

Send a notification to...

Only email lists for this account are available.

Email (endpoints)

janedoe@example.com - [View in SNS Console](#)

Add notification

Remove

15. Choose **Next**.
16. For **Name and description**, enter a name and description for your alarm.
17. Choose **Next**.
18. On the **Preview and create** page, review your alarm details, and then choose **Create alarm**.

When the status for the **IAM Access Key Rotation** check changes to red for 5 minutes, your alarm will send a notification to your SNS topic.

Example : Email notification for a CloudWatch alarm

The following email message shows that an alarm detected a change for the **IAM Access Key Rotation** check.

```
You are receiving this email because your Amazon CloudWatch Alarm
"IAMAccessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the ALARM
state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAccessKeyRotationCheckAlarm

Alarm Details:
- Name: IAMAccessKeyRotationCheckAlarm
- Description: This alarm starts when one or more AWS access keys in my AWS
account have not been rotated in the last 90 days.
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [9.0
(26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint
for OK -> ALARM transition).
```

```
- Timestamp:                Friday 26 March, 2021 22:49:42 UTC
- AWS Account:              123456789012
- Alarm Arn:                 arn:aws:cloudwatch:us-east-1:123456789012:alarm:IAMAccessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for 300 seconds.

Monitored Metric:
- MetricNamespace:           AWS/TrustedAdvisor
- MetricName:                 RedResources
- Dimensions:                 [CheckName = IAM Access Key Rotation]
- Period:                     300 seconds
- Statistic:                   Average
- Unit:                       not specified
- TreatMissingData:           missing

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

CloudWatch metrics for Trusted Advisor

You can use the CloudWatch console or the AWS Command Line Interface (AWS CLI) to find the metrics available for Trusted Advisor.

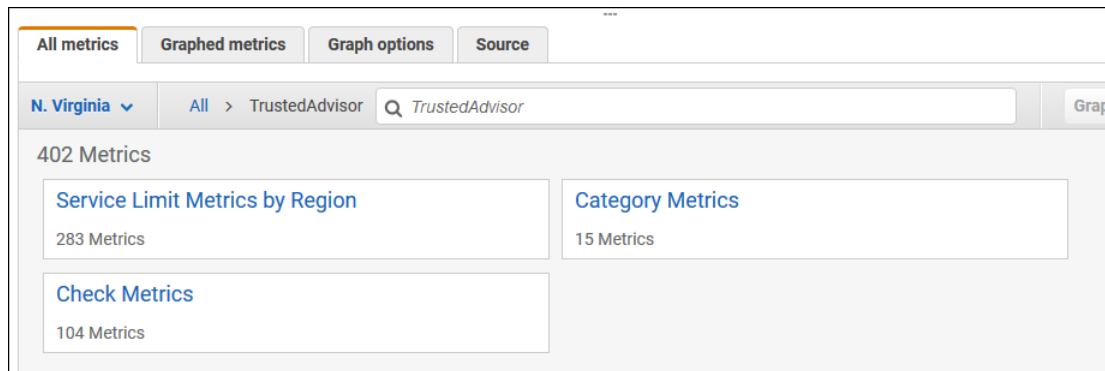
For a list of the namespaces, metrics, and dimensions for all services that publish metrics, see [AWS services that publish CloudWatch metrics](#) in the *Amazon CloudWatch User Guide*.

View Trusted Advisor metrics (console)

You can sign in to the CloudWatch console and view the available metrics for Trusted Advisor.

To view available Trusted Advisor metrics (console)

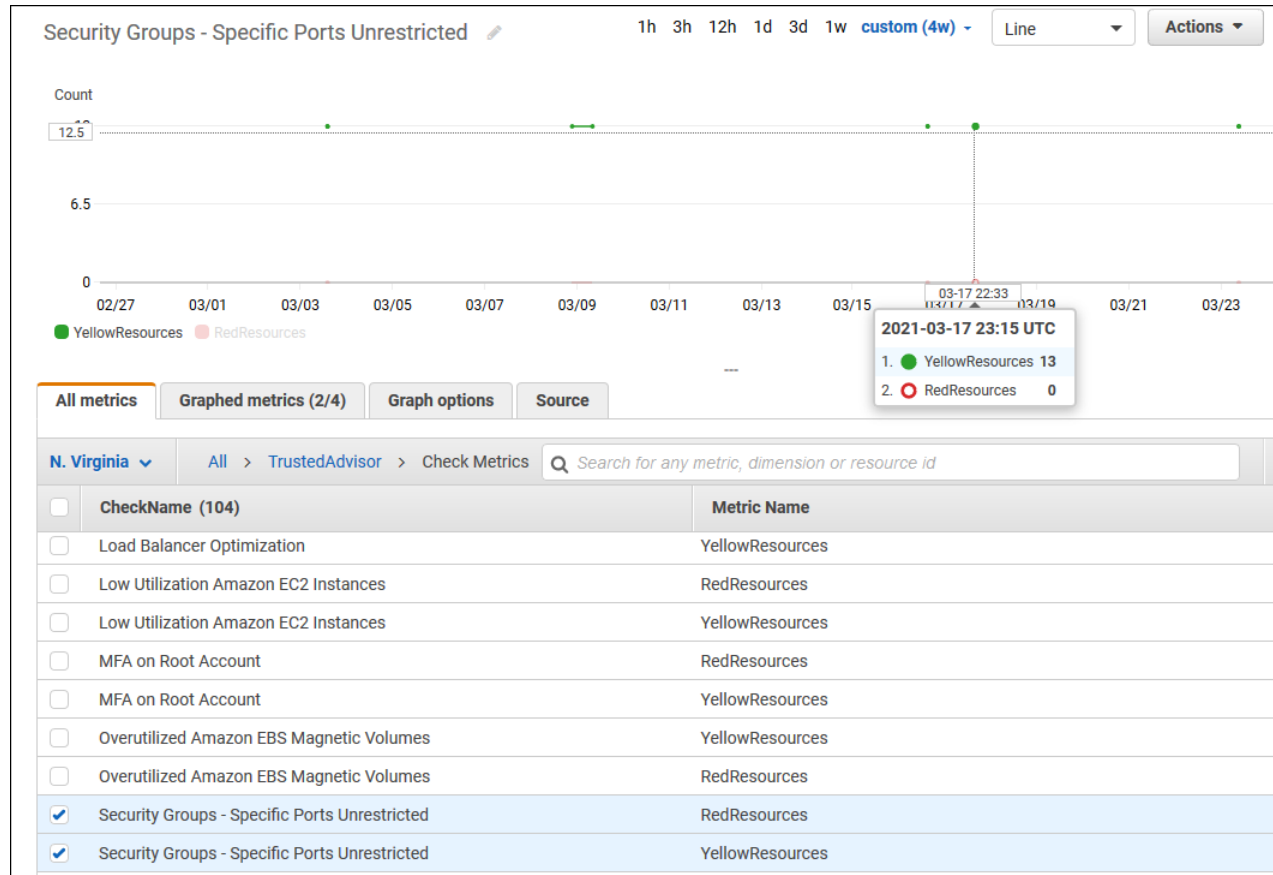
1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Use the **Region selector** and choose the **US East (N. Virginia)** AWS Region.
3. In the navigation pane, choose **Metrics**.
4. Enter a metric namespace, such as **TrustedAdvisor**.
5. Choose a metric dimension, such as **Check Metrics**.



6. The **All metrics** tab shows metrics for that dimension in the namespace. You can do the following:
 - a. To sort the table, choose the column heading.

- b. To graph a metric, select the check box next to the metric. To select all metrics, select the check box in the heading row of the table.
- c. To filter by metric, choose the metric name, and then choose **Add to search**.

The following example shows the results for the **Security Groups - Specific Ports Unrestricted** check. The check identifies 13 resources that are yellow. Trusted Advisor recommends that you investigate checks that are yellow.



7. (Optional) To add this graph to a CloudWatch dashboard, choose **Actions**, and then choose **Add to dashboard**.

For more information about creating a graph to view your metrics, see [Graphing a metric](#) in the *Amazon CloudWatch User Guide*.

View Trusted Advisor metrics (CLI)

You can use the `aws cloudwatch list-metrics` AWS CLI command to view available metrics for Trusted Advisor.

Example : List all metrics for Trusted Advisor

The following example specifies the `AWS/TrustedAdvisor` namespace to view all metrics for Trusted Advisor.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

Your output might look like the following.

```
{
  "Metrics": [
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "ServiceName",
          "Value": "EBS"
        },
        {
          "Name": "ServiceLimit",
          "Value": "Magnetic (standard) volume storage (TiB)"
        },
        {
          "Name": "Region",
          "Value": "ap-northeast-2"
        }
      ],
      "MetricName": "ServiceLimitUsage"
    },
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "CheckName",
          "Value": "Overutilized Amazon EBS Magnetic Volumes"
        }
      ],
      "MetricName": "YellowResources"
    },
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "ServiceName",
          "Value": "EBS"
        },
        {
          "Name": "ServiceLimit",
          "Value": "Provisioned IOPS"
        },
        {
          "Name": "Region",
          "Value": "eu-west-1"
        }
      ],
      "MetricName": "ServiceLimitUsage"
    },
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "ServiceName",
          "Value": "EBS"
        },
        {
          "Name": "ServiceLimit",
          "Value": "Provisioned IOPS"
        },
        {
          "Name": "Region",
          "Value": "ap-south-1"
        }
      ]
    }
  ]
}
```

```
    ],  
    "MetricName": "ServiceLimitUsage"  
  },  
  ...  
]  
}
```

Example : List all metrics for a dimension

The following example specifies the AWS/TrustedAdvisor namespace and the Region dimension to view the metrics available for the specified AWS Region.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions  
Name=Region,Value=us-east-1
```

Your output might look like the following.

```
{  
  "Metrics": [  
    {  
      "Namespace": "AWS/TrustedAdvisor",  
      "Dimensions": [  
        {  
          "Name": "ServiceName",  
          "Value": "SES"  
        },  
        {  
          "Name": "ServiceLimit",  
          "Value": "Daily sending quota"  
        },  
        {  
          "Name": "Region",  
          "Value": "us-east-1"  
        }  
      ],  
      "MetricName": "ServiceLimitUsage"  
    },  
    {  
      "Namespace": "AWS/TrustedAdvisor",  
      "Dimensions": [  
        {  
          "Name": "ServiceName",  
          "Value": "AutoScaling"  
        },  
        {  
          "Name": "ServiceLimit",  
          "Value": "Launch configurations"  
        },  
        {  
          "Name": "Region",  
          "Value": "us-east-1"  
        }  
      ],  
      "MetricName": "ServiceLimitUsage"  
    },  
    {  
      "Namespace": "AWS/TrustedAdvisor",  
      "Dimensions": [  
        {  
          "Name": "ServiceName",  
          "Value": "CloudFormation"  
        },  
        {  
          "Name": "ServiceLimit",  
          "Value": "Launch configurations"  
        },  
        {  
          "Name": "Region",  
          "Value": "us-east-1"  
        }  
      ],  
      "MetricName": "ServiceLimitUsage"  
    }  
  ]  
}
```



```
        "Name": "ServiceLimit",
        "Value": "Stacks"
      },
      {
        "Name": "Region",
        "Value": "us-east-1"
      }
    ],
    "MetricName": "ServiceLimitUsage"
  },
  ...
]
}
```

Example : List metrics for a specific metric name

The following example specifies the AWS/TrustedAdvisor namespace and the RedResources metric name to view the results for only this specific metric.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

Your output might look like the following.

```
{
  "Metrics": [
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "CheckName",
          "Value": "Amazon RDS Security Group Access Risk"
        }
      ],
      "MetricName": "RedResources"
    },
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "CheckName",
          "Value": "Exposed Access Keys"
        }
      ],
      "MetricName": "RedResources"
    },
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "CheckName",
          "Value": "Large Number of Rules in an EC2 Security Group"
        }
      ],
      "MetricName": "RedResources"
    },
    {
      "Namespace": "AWS/TrustedAdvisor",
      "Dimensions": [
        {
          "Name": "CheckName",
          "Value": "Auto Scaling Group Health Check"
        }
      ],
      "MetricName": "RedResources"
    }
  ]
}
```

```
        "MetricName": "RedResources"  
    },  
    ...  
]  
}
```

Trusted Advisor metrics and dimensions

See the following tables for the Trusted Advisor metrics and dimensions that you can use for your CloudWatch alarms and graphs.

Trusted Advisor check-level metrics

You can use the following metrics for Trusted Advisor checks.

Metric	Description
RedResources	The number of resources that are in a red state (action recommended).
YellowResources	The number of resources that are in a yellow state (investigation recommended).

Trusted Advisor category-level metrics

You can use the following metrics for Trusted Advisor categories.

Metric	Description
GreenChecks	The number of Trusted Advisor checks that are in a green state (no issues detected).
RedChecks	The number of Trusted Advisor checks that are in a red state (action recommended).
YellowChecks	The number of Trusted Advisor checks that are in a yellow state (investigation recommended).

Trusted Advisor service quota-level metrics

You can use the following metrics for AWS service quotas.

Metric	Description
ServiceLimitUsage	The percentage of resource usage against a service quota (formerly referred to as limits).

Dimensions for check-level metrics

You can use the following dimension for Trusted Advisor checks.

Dimension	Description
CheckName	The name of the Trusted Advisor check.

Dimension	Description
	You can find all check names in the Trusted Advisor console or the AWS Trusted Advisor check reference (p. 56) .

Dimensions for category-level metrics

You can use the following dimension for Trusted Advisor check categories.

Dimension	Description
Category	The name of a Trusted Advisor check category. You can find all check categories in the Trusted Advisor console or the View check categories (p. 27) page.

Dimensions for service quota metrics

You can use the following dimensions for Trusted Advisor service quota metrics.

Dimension	Description
Region	The AWS Region for a service quota.
ServiceName	The name of the AWS service.
ServiceLimit	The name of the service quota. For more information about service quotas, see AWS service quotas in the <i>AWS General Reference</i> .

Compliance validation for AWS Support

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether AWS Support or other AWS services are 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 AWS services 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 baseline environments on AWS that are security and compliance focused.
- [Architecting for HIPAA Security and Compliance Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

Note

Not all services are compliant with HIPAA.

- [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.
- [AWS Audit Manager](#) – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in AWS Support

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 AWS Support

As a managed service, AWS Support 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 AWS Support 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.

Configuration and vulnerability analysis in AWS Support

For AWS Trusted Advisor, AWS handles basic security tasks such as guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

Configuration and IT controls are a shared responsibility between AWS and you, our customer. For more information, see the AWS [shared responsibility model](#).

Troubleshooting resources

For answers to common troubleshooting questions, see the [AWS Support Knowledge Center](#).

For Windows, Amazon EC2 offers EC2Rescue, which allows customers to examine their Windows instances to help identify common problems, collect log files, and help AWS Support to troubleshoot your issues. You can also use EC2Rescue to analyze boot volumes from non-functional instances. For more information, see [How can I use EC2Rescue to troubleshoot and fix common issues on my EC2 Windows instance?](#)

Service-specific troubleshooting

Most AWS service documentation contains troubleshooting topics that can get you started before contacting AWS Support. The following table provides links to troubleshooting topics, arranged by service.

Service	Link
Amazon Web Services	Troubleshooting AWS Signature Version 4 errors
Amazon AppStream	Troubleshoot Amazon AppStream
Amazon EC2 Auto Scaling	Troubleshooting Auto Scaling
AWS Certificate Manager (ACM)	Troubleshooting
AWS CloudFormation	Troubleshooting AWS CloudFormation
Amazon CloudFront	Troubleshooting Troubleshooting RTMP distributions
AWS CloudHSM	Troubleshooting
Amazon CloudSearch	Troubleshooting Amazon CloudSearch
AWS CodeDeploy	Troubleshooting AWS CodeDeploy
AWS Data Pipeline	Troubleshooting
AWS Direct Connect	Troubleshooting AWS Direct Connect
AWS Directory Service	Troubleshooting AWS Directory Service administration issues
Amazon DynamoDB	Troubleshooting
AWS Elastic Beanstalk	Troubleshooting
Amazon Elastic Compute Cloud (Amazon EC2)	Troubleshooting instances Troubleshooting Windows instances Troubleshooting VM Import/Export Troubleshooting API request errors Troubleshooting the AWS management pack Troubleshooting AWS Systems Manager for Microsoft SCVMM AWS diagnostics for Microsoft Windows server
Amazon Elastic Container Service (Amazon ECS)	Amazon ECS troubleshooting

Service	Link
Elastic Load Balancing	Troubleshoot your application load balancers Troubleshoot your Classic Load Balancer
Amazon EMR (Amazon EMR)	Troubleshoot a cluster
Amazon ElastiCache for Memcached	Troubleshooting applications
Amazon ElastiCache for Redis	Troubleshooting applications
AWS Flow Framework	Troubleshooting and debugging tips
AWS GovCloud (US)	Troubleshooting
AWS Identity and Access Management (IAM)	Troubleshooting IAM
Kinesis	Troubleshooting Kinesis producers Troubleshooting Kinesis streams consumers
AWS Lambda	Troubleshooting and monitoring AWS Lambda functions with CloudWatch
AWS OpsWorks	Debugging and troubleshooting guide
Amazon Redshift	Troubleshooting queries Troubleshooting data loads Troubleshooting connection issues in Amazon Redshift Troubleshooting Amazon Redshift audit logging
Amazon Relational Database Service (Amazon RDS)	Troubleshooting Troubleshooting applications
Amazon Route 53	Troubleshooting Amazon Route 53
Amazon Silk	Troubleshooting
Amazon Simple Email Service (Amazon SES)	Troubleshooting Amazon SES
Amazon Simple Storage Service (Amazon S3)	Troubleshooting CORS issues Handling REST and SOAP errors
Amazon Simple Workflow Service (Amazon SWF)	AWS flow framework for Java: Troubleshooting and debugging tips AWS flow framework for Ruby: Troubleshooting and debugging workflows
AWS Storage Gateway	Troubleshooting your gateway
Amazon Virtual Private Cloud (Amazon VPC)	Troubleshooting
Amazon WorkMail	Troubleshooting the Amazon WorkMail web application
Amazon WorkSpaces	Troubleshooting Amazon WorkSpaces administration issues Troubleshooting amazon WorkSpaces client issues
Amazon WorkSpaces Application Manager (Amazon WAM)	Troubleshooting Amazon WAM application issues

Document history

The following table describes the important changes to the documentation since the last release of the AWS Support service.

- **API version:** 2013-04-15
- **Latest documentation update:** September 29, 2021

The following table describes important updates to the AWS Support and AWS Trusted Advisor documentation, beginning in May 10, 2021. You can subscribe to the RSS feed to receive notifications about the updates.

update-history-change	update-history-description	update-history-date
Updated documentation for Trusted Advisor (p. 137)	Trusted Advisor added two new checks for Amazon Comprehend. For more information, see the AWS Trusted Advisor check reference .	September 29, 2021
Updated documentation for Trusted Advisor (p. 137)	The check name for Amazon Elasticsearch Reserved Instance Optimization is renamed to Amazon OpenSearch Service Reserved Instance Optimization. For more information, see Change log for AWS Trusted Advisor checks .	September 8, 2021
Updated documentation for Trusted Advisor checks (p. 137)	Added a reference topic for all Trusted Advisor checks. For more information, see AWS Trusted Advisor check reference .	September 1, 2021
Updated documentation for Trusted Advisor managed policies (p. 137)	Updated documentation for the Trusted Advisor managed policies. For more information, see AWS managed policies for AWS Support and AWS Trusted Advisor .	August 10, 2021
Updated documentation for Trusted Advisor (p. 137)	Updated documentation for the Trusted Advisor console. For more information, see Get started with AWS Trusted Advisor .	July 16, 2021
Updated documentation for creating AWS Support cases (p. 137)	Added documentation about how to create a related support case for cases that are permanently closed. For more information, see Reopening a closed case and Creating a related case .	June 8, 2021

Updated documentation for Trusted Advisor (p. 137)	Trusted Advisor added two new checks for Amazon Elastic Block Store (Amazon EBS) volume storage. For more information, see Change log for AWS Trusted Advisor checks .	June 8, 2021
Updated documentation (p. 137)	<p>The following topics are updated:</p> <ul style="list-style-type: none"> Updated procedures and added content to the Creating Amazon CloudWatch alarms to monitor AWS Trusted Advisor metrics topic Added the Service quotas for the AWS Support API section 	May 12, 2021

Earlier updates

Change	Description	Date
Updated documentation for Trusted Advisor	<p>Added documentation to filter, refresh, and download check results. For more information, see the following sections:</p> <ul style="list-style-type: none"> Filter your checks (p. 29) Refresh check results (p. 30) Download check results (p. 30) 	March 16, 2021
Updated documentation about AWS managed policies	Added information about the <code>AWSSupportServiceRolePolicy</code> AWS managed policy. For more information, see Using service-linked roles for AWS Support (p. 98) .	March 16, 2021
Added checks for AWS Lambda	Added four AWS Trusted Advisor checks for Lambda in the Change log for AWS Trusted Advisor checks (p. 49) .	March 8, 2021
Updated service limit checks for Amazon Elastic Block Store	Updated five AWS Trusted Advisor checks for Amazon EBS in the Change log for AWS Trusted Advisor checks (p. 49) .	March 5, 2021
Updated documentation for CloudTrail logging	CloudTrail supports logging for console actions when you change your AWS Support plan. For more information, see Logging changes to your AWS Support plan (p. 116) .	February 9, 2021
Updated documentation for Trusted Advisor	Updated the Get started with AWS Trusted Advisor (p. 25) topic.	January 29, 2021
Updated documentation for Trusted Advisor reports	Added a Troubleshooting (p. 48) section for using Trusted Advisor reports with other AWS services.	December 4, 2020

Change	Description	Date
Added AWS Trusted Advisor support for AWS CloudTrail logging	CloudTrail supports logging for a subset of Trusted Advisor console actions. For more information, see Logging AWS Trusted Advisor console actions with AWS CloudTrail (p. 118) .	November 23, 2020
Added a change log topic	View changes to AWS Trusted Advisor checks and categories in the Change log for AWS Trusted Advisor checks (p. 49) .	November 18, 2020
Added support for organizational units	You can now create reports for Trusted Advisor checks for organizational units (OUs). For more information, see Create organizational view reports (p. 33) .	November 17, 2020
Updated the logging with AWS CloudTrail topic	Added an example log entry for a Trusted Advisor API operation. See AWS Trusted Advisor information in CloudTrail logging (p. 114) .	October 22, 2020
Added AWS Support quotas	Added information about the current quotas and restrictions for AWS Support. See the AWS Support endpoints and quotas in the <i>AWS General Reference</i> .	August 4, 2020
Organizational view for AWS Trusted Advisor	You can now create reports for Trusted Advisor checks for accounts that are part of AWS Organizations. See Organizational view for AWS Trusted Advisor (p. 31) .	July 17, 2020
Security and AWS Support	Updated information about security considerations when using AWS Support and Trusted Advisor. See Security in AWS Support (p. 90)	May 5, 2020
Security and AWS Support	Added information about security considerations when using AWS Support.	January 10, 2020
Using Trusted Advisor as a web service	Added updated instructions to refresh Trusted Advisor data after getting list of Trusted Advisor checks.	November 1, 2018
Using Service-linked roles	Added new section.	July 11, 2018
Getting Started: Troubleshooting	Added troubleshooting links for Route 53 and AWS Certificate Manager.	September 1, 2017
Case Management Example: Creating a Case	Added a note about the CC box for users who have the Basic support plan.	August 1, 2017
Monitoring Trusted Advisor Check Results with CloudWatch Events	Added new section.	November 18, 2016
Case Management	Updated the names of case severity levels.	October 27, 2016

Change	Description	Date
Logging AWS Support Calls with AWS CloudTrail	Added new section.	April 21, 2016
Getting Started: Troubleshooting	Added more troubleshooting links.	May 19, 2015
Getting Started: Troubleshooting	Added more troubleshooting links.	November 18, 2014
Getting Started: Case Management	Updated to reflect AWS Service Catalog in the AWS Management Console.	October 30, 2014
Programming the Life of an AWS Support Case	Added information about new API elements for adding attachments to cases and for omitting case communications when retrieving case history.	July 16, 2014
Accessing AWS Support	Removed named support contacts as an access method.	May 28, 2014
Getting Started	Added the Getting Started section.	December 13, 2013
Initial publication	New AWS Support service released.	April 30, 2013

AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.