# Table of Contents

Get started with AWS Support .................................................................................................. 1
Features of AWS Support plans .............................................................................................. 1
Create support cases and case management ........................................................................ 2
  Creating a support case ........................................................................................................ 3
  Describing your problem ....................................................................................................... 4
  Choosing a severity ............................................................................................................... 4
  Example: Create a support case for account and billing .................................................... 5
Create a service quota increase ............................................................................................... 9
Update, resolve, and reopen your cases .................................................................................. 10
  Update an existing support case .......................................................................................... 11
  Resolve a support case ....................................................................................................... 11
  Reopen a resolved case ...................................................................................................... 12
  Creating a related case ....................................................................................................... 13
  Case history ........................................................................................................................ 14
Troubleshooting ....................................................................................................................... 14
  I want to reopen a live chat for my case ........................................................................... 14
  I can't connect to a live chat ............................................................................................. 14
Access permissions for AWS Support ..................................................................................... 15
  AWS account ....................................................................................................................... 15
  IAM ..................................................................................................................................... 15
  Access to AWS Trusted Advisor ........................................................................................ 16
Changing your AWS Support plan ........................................................................................... 17
Working with AWS SDKs ......................................................................................................... 17
About the AWS Support API ................................................................................................... 18
  Support case management ................................................................................................. 18
  Trusted Advisor .................................................................................................................. 18
  Endpoint ............................................................................................................................... 19
  Support in AWS SDKs ......................................................................................................... 19
Programming an AWS Support case ....................................................................................... 20
  Overview ............................................................................................................................ 20
    Using IAM with the AWS Support API ........................................................................... 20
    Create an AWS Support client ........................................................................................ 20
    Discover Amazon Web Services and issue severity levels .......................................... 21
    Create an attachment set ............................................................................................... 22
    Create a support case ...................................................................................................... 23
    Retrieve and update support case communications ..................................................... 25
    Retrieve all support case information ......................................................................... 27
    Resolve a support case ..................................................................................................... 28
    Service quotas for the AWS Support API ...................................................................... 28
AWS Trusted Advisor ............................................................................................................. 29
  Get started with AWS Trusted Advisor ............................................................................ 29
    Sign in to the Trusted Advisor console ....................................................................... 30
    View check categories ..................................................................................................... 31
    View specific checks ....................................................................................................... 32
    Filter your checks .......................................................................................................... 33
    Refresh check results ....................................................................................................... 34
    Download check results ................................................................................................. 34
    Organizational view ........................................................................................................ 35
    Preferences ..................................................................................................................... 35
Using Trusted Advisor as a web service ................................................................................. 36
  Get the list of available Trusted Advisor checks .............................................................. 36
  Refresh the list of available Trusted Advisor checks ....................................................... 37
  Poll a Trusted Advisor check for status changes .............................................................. 37
  Request a Trusted Advisor check result .......................................................................... 38
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing access using policies</td>
<td>155</td>
</tr>
<tr>
<td>How AWS Support works with IAM</td>
<td>157</td>
</tr>
<tr>
<td>Identity-based policy examples</td>
<td>158</td>
</tr>
<tr>
<td>Using service-linked roles</td>
<td>160</td>
</tr>
<tr>
<td>AWS managed policies</td>
<td>164</td>
</tr>
<tr>
<td>Manage access for AWS Trusted Advisor</td>
<td>177</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>183</td>
</tr>
<tr>
<td>Incident response</td>
<td>184</td>
</tr>
<tr>
<td>Logging and monitoring in AWS Support and AWS Trusted Advisor</td>
<td>185</td>
</tr>
<tr>
<td>Compliance validation</td>
<td>185</td>
</tr>
<tr>
<td>Resilience</td>
<td>186</td>
</tr>
<tr>
<td>Infrastructure security</td>
<td>186</td>
</tr>
<tr>
<td>Configuration and vulnerability analysis</td>
<td>186</td>
</tr>
<tr>
<td>Monitoring and logging for AWS Support</td>
<td>187</td>
</tr>
<tr>
<td>Monitoring AWS Support cases with EventBridge</td>
<td>187</td>
</tr>
<tr>
<td>Creating an EventBridge rule for AWS Support cases</td>
<td>187</td>
</tr>
<tr>
<td>Example AWS Support events</td>
<td>188</td>
</tr>
<tr>
<td>See also</td>
<td>190</td>
</tr>
<tr>
<td>Logging AWS Support API calls with AWS CloudTrail</td>
<td>190</td>
</tr>
<tr>
<td>AWS Support information in CloudTrail</td>
<td>190</td>
</tr>
<tr>
<td>AWS Trusted Advisor information in CloudTrail logging</td>
<td>191</td>
</tr>
<tr>
<td>Understanding AWS Support log file entries</td>
<td>191</td>
</tr>
<tr>
<td>Logging console actions for changes to your AWS Support plan</td>
<td>193</td>
</tr>
<tr>
<td>Monitoring and logging for Trusted Advisor</td>
<td>196</td>
</tr>
<tr>
<td>Monitoring Trusted Advisor check results with EventBridge</td>
<td>196</td>
</tr>
<tr>
<td>Creating CloudWatch alarms to monitor Trusted Advisor metrics</td>
<td>198</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>198</td>
</tr>
<tr>
<td>CloudWatch metrics for Trusted Advisor</td>
<td>201</td>
</tr>
<tr>
<td>Trusted Advisor metrics and dimensions</td>
<td>206</td>
</tr>
<tr>
<td>Logging AWS Trusted Advisor console actions with AWS CloudTrail</td>
<td>207</td>
</tr>
<tr>
<td>Trusted Advisor information in CloudTrail</td>
<td>208</td>
</tr>
<tr>
<td>Example: Trusted Advisor Log File Entries</td>
<td>209</td>
</tr>
<tr>
<td>Troubleshooting resources</td>
<td>212</td>
</tr>
<tr>
<td>Service-specific troubleshooting</td>
<td>212</td>
</tr>
<tr>
<td>Document history</td>
<td>214</td>
</tr>
<tr>
<td>Earlier updates</td>
<td>218</td>
</tr>
<tr>
<td>AWS glossary</td>
<td>221</td>
</tr>
</tbody>
</table>
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. 3).

Topics

• Features of AWS Support plans (p. 1)
• Creating support cases and case management (p. 2)
• Creating a service quota increase (p. 9)
• Updating, resolving, and reopening your case (p. 10)
• Troubleshooting (p. 14)
• Access permissions for AWS Support (p. 15)
• Changing your AWS Support plan (p. 17)
• Using AWS Support with an AWS SDK (p. 17)

Features of AWS Support plans

AWS Support offers five support plans:

• Basic
• Developer
• Business
• Enterprise On-Ramp
• 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:
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.
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. 15).
- 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 Support Center Console.
   
   Tip
   In the AWS Management Console, you can also choose the question mark icon (_QUESTION_MARK) and then choose Support Center.

2. Choose Create case.

3. Choose one of the following options:
   - Account and billing
   - Technical
   - For service quota increases, choose Looking for service limit increases? and then follow the instructions for Creating a service quota increase (p. 9).

   
   Tip
   You can use the recommended solutions that appear for commonly asked questions.

5. Choose Next step: Additional information

6. On the Additional information page, for Subject, enter a title about your issue.

7. For Description, 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

8. (Optional) Choose Attach files to add any relevant files to your case, such as error logs or screenshots. You can attach up to three files. Each file can be up to 5 MB.

9. Choose Next step: Solve now or contact us.

10. On the Contact us page, choose your preferred language and how you want to be contacted. You can choose one of the following options:
a. **Web** – Receive a reply in Support Center.

b. **Chat** – Start a live chat with a support agent. If you can't connect to a chat, see Troubleshooting (p. 14).

c. **Phone** – Receive a phone call from a support agent. If you choose this option, enter the following information:
   - **Country or region**
   - **Phone number**
   - (Optional) **Extension**

**Notes**
- The contact options that appear depend on the type of case and your support plan.
- You can choose **Discard draft** to clear your support case draft.

11. (Optional) If you have a Business, Enterprise On-Ramp, or Enterprise Support plan, the **Additional contacts** option appears. You can enter the email addresses of people to notify 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 root account email address and password, you don't need to include your email address.

   **Note**
   If you have the Basic Support plan, the **Additional contacts** option 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.

12. Review your case details and then choose **Submit**. Your case ID number and summary appear.

### 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.

**Notes**
- You can't change the severity code for a support case after you create one. If your situation changes, work with the AWS Support for your support case.
- For more information about the severity level, see the AWS Support API Reference.
<table>
<thead>
<tr>
<th>Severity</th>
<th>Severity level code</th>
<th>First-response time</th>
<th>Description and support plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>General guidance</td>
<td>low</td>
<td>24 hours</td>
<td>You have a general development question, or you want to request a feature. (Developer*, Business, Enterprise On-Ramp, or Enterprise Support plan)</td>
</tr>
<tr>
<td>System impaired</td>
<td>normal</td>
<td>12 hours</td>
<td>Non-critical functions of your application are behaving abnormally, or you have a time-sensitive development question. (Developer*, Business, Enterprise On-Ramp, or Enterprise Support plan)</td>
</tr>
<tr>
<td>Production system impaired</td>
<td>high</td>
<td>4 hours</td>
<td>Important functions of your application are impaired or degraded. (Business, Enterprise On-Ramp, or Enterprise Support plan)</td>
</tr>
<tr>
<td>Production system down</td>
<td>urgent</td>
<td>1 hour</td>
<td>Your business is significantly impacted. Important functions of your application aren't available. (Business, Enterprise On-Ramp, or Enterprise Support plan)</td>
</tr>
<tr>
<td>Business-critical system down</td>
<td>critical</td>
<td>15 minutes</td>
<td>Your business is at risk. Critical functions of your application aren't available (Enterprise Support plan). Note that this is 30 minutes for the Enterprise On-Ramp Support plan.</td>
</tr>
</tbody>
</table>

* 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.

**Example: Create a support case for account and billing**

The following example is a support case for a billing and account issue.
Hello!
We're here to help.
Account: 123456789012 • Support plan: Basic • Change

How can we help?
Choose the related issue for your case.

1. **Create case** – Choose the type of case to create. In this example, the case type is **Account and billing**.
   
   **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.

3. **Category** – Choose the category that best fits your use case. When you choose a category, links to information that might resolve your problem appear below.
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 a Business Support plan can choose **Production system impaired** (4-hour response) or **Production system down** (1-hour response). Customers with an Enterprise On-Ramp or Enterprise Support plan can choose **Business-critical system down** (15-minute response for Enterprise Support and 30-minute response for Enterprise On-Ramp).

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. 4).

**Note**
Based on your category choice, you might be prompted for more information.

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

Describe your issue

1. **Subject** – Enter a title that briefly describes your issue.

2. **Description** – Describe your support case. This is the most important information that you provide to AWS Support. For some service and category combinations, a prompt appears with related information. Use these links to help resolve your issue. For more information, see Describing your problem (p. 4).

3. **Attach files**
   
   Up to 3 attachments, each less than 5MB

---

**Guidance**

Provide a detailed description of your issue. If you have a question about a charge, provide the date, amount, or any other details about the charge.
3. **Attachments** – Attach screenshots and other files that can help support agents resolve your case faster.

After you add your case details, you can choose how you want to be contacted.

1. **Preferred contact language** – Currently, you can choose English or Japanese.
2. Choose a contact method. The contact options that appear 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.
   - Choose **Chat** or **Phone**. If you choose **Phone**, you're prompted for a callback number.
3. Choose **Submit** when your information is complete and you're ready to create the case.

---

### Creating a service quota increase

To improve the performance of your service, request increases to your service quotas (formerly referred to as limits).

**Note**
You can also use the Service Quotas service to request increases directly for your services. Currently, Service Quotas doesn't support service quotas for all services. For more information, see [What is Service Quotas?](https://docs.aws.amazon.com/service-quotas/latest/userguide/what-is-service-quotas.html) in the [Service Quotas User Guide](https://docs.aws.amazon.com/service-quotas/latest/userguide/).

**To create a support case for service quota increases**

Tip

In the AWS Management Console, you can also choose the question mark icon and then choose Support Center.

2. Choose Create case.
3. Choose Looking for service limit increases?
4. To request an increase, follow the prompts. Possible options include the following:
   - Limit type
   - Severity
   
   Note
   Based on your category choice, the prompts might request more information.

5. For Requests, choose the Region.
6. For Limit, choose the service limit type.
7. For New limit value, enter the value that you want.
8. (Optional) To request another increase, choose Add another request.
9. For Case description, describe your support case.
10. For Contact options page, choose your preferred language and how you want to be contacted. You can choose one of the following options:
   - Web – Receive a reply in Support Center.
   - Chat – Start a live chat with a support agent. If you can't connect to a chat, see Troubleshooting (p. 14).
   - Phone – Receive a phone call from a support agent. If you choose this option, enter the following information:
     - Country/Region
     - Phone number
     - (Optional) Extension

Updating, 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. 15).
- 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. 13).
Topics

- Updating an existing support case (p. 11)
- Resolving a support case (p. 11)
- Reopening a resolved case (p. 12)
- Creating a related case (p. 13)
- Case history (p. 14)

Updating an existing support case

You can update your case to provide more information for the support agent. For example, you can reply to correspondences, start another live chat, add additional email recipients, and so on. However, you can't update the severity of a case after you've created it. For more information, see Choosing a severity (p. 4).

To update an existing support case

1. Sign in to the AWS Support Center Console.

   Tip
   
   In the AWS Management Console, you can also choose the question mark icon (qid) and then choose Support Center.

2. Under Open support cases, choose the Subject of the support case.

3. Choose Reply. In the Correspondence section, you can also make any of the following changes:

   • Provide information that the support agent requested
   • Upload file attachments
   • Change your preferred contact method
   • Add email addresses to receive case updates

4. Choose Submit.

   Tip
   
   If you closed a chat window and you want to start another live chat, add a Reply to your support case, choose Chat, and then choose Submit. A new pop-up chat window opens.

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 Support Center Console.

   Tip
   
   In the AWS Management Console, you can also choose the question mark icon (qid) and then choose Support Center.

2. Under Open support cases, choose the Subject of the support case that you want to resolve.

3. (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.

4. Choose Resolve case.
5. 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.

![Feedback links screenshot]

**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. 13).
- 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 Support Center Console.

   **Tip**
   In the AWS Management Console, you can also choose the question mark icon (?) and then choose **Support Center**.

2. Choose **View all cases** and then choose the **Subject** or the **Case ID** of the support case that you want to reopen.

3. Choose **Reopen case**.

4. Under **Correspondence**, for **Reply**, enter the case details.

5. (Optional) Choose **Choose files** to attach files to your case. You can attach up to 3 files.

6. 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.

7. (Optional) For **Additional contacts**, enter email addresses for other people that you want to receive case correspondences.

8. 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 Support Center Console.
   
   Tip
   
   In the AWS Management Console, you can also choose the question mark icon (️) and then choose Support Center.

2. Choose View all cases and then choose the Subject or the Case ID of the support case that you want to reopen.

3. Choose Reopen case.

4. 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.

5. Follow the same steps to create your case. See Creating a support case (p. 3).

   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.

6. 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 history

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

Troubleshooting

If you have difficulty when you create or manage your support case, see the following troubleshooting information.

**I want to reopen a live chat for my case**

You can reply to your existing support case to open another chat window. For more information, see Updating an existing support case (p. 11).

**I can't connect to a live chat**

If you chose the Chat option but you can't connect to the chat window, first perform the following checks:
• Ensure that you’ve configured your browser to allow pop-up windows in Support Center.

  **Note**
  Review the settings for your browser. For more information, see the Chrome Help and Firefox Support websites.

• Ensure that you’ve configured your network so that you can use AWS Support:
  • Your network can access the *.connect.us-east-1.amazonaws.com endpoint.

  **Note**
  For AWS GovCloud (US), the endpoint is *.connect-fips.us-east-1.amazonaws.com.
  • Your firewall supports web socket connections.
  • For more information, see Set up your network in the Amazon Connect Administrator Guide.

If you still can’t connect to the chat window, contact your AWS account administrator.

## Access permissions for AWS Support

You must have permissions to access Support Center and to create a support case (p. 3).

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, Enterprise On-Ramp, or Enterprise Support plan, you can also use the AWS Support API (p. 18) 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.

```json
{
  "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.

```json
{
  "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. 153).

**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. 177).
Changing your AWS Support plan

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

To change your support plan

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 an Enterprise On-Ramp or Enterprise Support plan, 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 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.

<table>
<thead>
<tr>
<th>SDK documentation</th>
<th>Code examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS SDK for C++</td>
<td>AWS SDK for C++ code examples</td>
</tr>
<tr>
<td>AWS SDK for Go</td>
<td>AWS SDK for Go code examples</td>
</tr>
<tr>
<td>AWS SDK for Java</td>
<td>AWS SDK for Java code examples</td>
</tr>
<tr>
<td>AWS SDK for JavaScript</td>
<td>AWS SDK for JavaScript code examples</td>
</tr>
<tr>
<td>AWS SDK for .NET</td>
<td>AWS SDK for .NET code examples</td>
</tr>
<tr>
<td>AWS SDK for PHP</td>
<td>AWS SDK for PHP code examples</td>
</tr>
<tr>
<td>AWS SDK for Python (Boto3)</td>
<td>AWS SDK for Python (Boto3) code examples</td>
</tr>
<tr>
<td>AWS SDK for Ruby</td>
<td>AWS SDK for Ruby code examples</td>
</tr>
</tbody>
</table>

Example availability

Can't find what you need? Request a code example by using the Provide feedback link at the bottom of this page.
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. 18)** operations to manage the entire life cycle of your AWS support cases, from creating a case to resolving it
- **Trusted Advisor (p. 18)** operations to access AWS Trusted Advisor (p. 29) checks

**Note**
You must have a Business, Enterprise On-Ramp, 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. 18)
- Trusted Advisor (p. 18)
- Endpoint (p. 19)
- Support in AWS SDKs (p. 19)

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. 190).

For example Java code that demonstrates how to manage the entire life cycle of a support case, see Programming an AWS Support case (p. 20).

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. 191).

You can use Amazon CloudWatch Events to monitor for changes to your check results for Trusted Advisor. For more information, see Monitoring AWS Trusted Advisor check results with Amazon EventBridge (p. 196).

For example Java code that demonstrates how to use the Trusted Advisor operations, see Using Trusted Advisor as a web service (p. 36).

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. 20)
- Create an AWS Support client (p. 20)
- Discover Amazon Web Services and issue severity levels (p. 21)
- Create an attachment set (p. 22)
- Create a support case (p. 23)
- Retrieve and update support case communications (p. 25)
- Retrieve all support case information (p. 27)
- Resolve a support case (p. 28)
- Service quotas for the AWS Support API (p. 28)

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. 28)
- 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. 15).

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
AWS Support User Guide
Discover Amazon Web Services and issue severity levels

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.

```java
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.

```java
// 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.
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.

```java
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);
}
```
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.

```
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();
    }
```
```java
} 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);
}
```
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 printCommunications method is provided for your convenience.

```java
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.

```java
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());
    }
}
```
Resolve a support case

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

```java
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.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum number of AWS Support cases that you can create.</td>
<td>10 per hour</td>
</tr>
<tr>
<td>The maximum number of AWS Support API operations that you can perform per second.</td>
<td>5</td>
</tr>
<tr>
<td>The maximum number of AWS Trusted Advisor API operations that you can perform per second.</td>
<td>100</td>
</tr>
</tbody>
</table>
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, Enterprise On-Ramp, or Enterprise Support plan, you can use the Trusted Advisor console and the AWS Support API (p. 18) 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 AWS Trusted Advisor check results with Amazon EventBridge (p. 196).

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. 177).

For more information, see Trusted Advisor.

Topics
- Get started with AWS Trusted Advisor (p. 29)
- Using Trusted Advisor as a web service (p. 36)
- Organizational view for AWS Trusted Advisor (p. 39)
- Viewing AWS Security Hub controls in AWS Trusted Advisor (p. 57)
- Opt in AWS Compute Optimizer for Trusted Advisor checks (p. 62)
- Get started with AWS Trusted Advisor Priority (p. 63)
- AWS Trusted Advisor check reference (p. 71)
- Change log for AWS Trusted Advisor checks (p. 146)

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. 30)
- View check categories (p. 31)
- View specific checks (p. 32)
- Filter your checks (p. 33)
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. 177).

**To sign in to the Trusted Advisor console**

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.
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

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 (ダウンロード) to create an .xls file that includes the results for this check.
Example: Cost optimization category

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

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

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.

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.

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

2. In the navigation pane or the Dashboard page, choose the check category.
3. For Search by keyword, enter a keyword from the check name or description to filter your results.
4. 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.
5. 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**.

6. In the table for the check, the check results only show items that have the specified key and value.
7. 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. If you have a Developer or Basic support plan, you can sign in to the Trusted Advisor console to refresh the checks. If you have a Business, Enterprise On-Ramp, or Enterprise Support plan, Trusted Advisor automatically refreshes the checks in your account on a weekly basis.

**To refresh Trusted Advisor checks**

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 (_circle) for an individual check.
- Use the **RefreshTrustedAdvisorCheck** API operation.

**Notes**

- Trusted Advisor automatically refreshes some checks several times a day, such as the **AWS Well-Architected high risk issues for reliability** check. It might take a few hours for changes to appear in your account. For these automatically refreshed checks, you can't choose the refresh icon (circle) to manually refresh your results.
- If you enabled AWS Security Hub for your account, you can't use the Trusted Advisor console to refresh Security Hub controls. For more information, see Refresh your Security Hub findings (p. 60).

**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

   - 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 (Download).
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. 39).

Preferences

On the Preferences page in the Trusted Advisor console, you can disable Trusted Advisor.

On the Notifications page, you can configure your weekly email messages for the check summary.

On the Organizations page, you can enable or disable the organizational view feature.

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

2. In the navigation pane, under Preferences, choose Notifications.
3. For Weekly email notification, select whom to notify for your check results. You receive about an email notification about your Trusted Advisor check summary once a week. 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 your 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. 39).

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

2. In the navigation pane, choose **Preferences**.
4. In the navigation pane, under **Preferences**, choose **Manage Trusted Advisor**.
5. Under **Trusted Advisor**, turn off **Enabled**. This action disables Trusted Advisor for all checks in your account.
6. You can then manually delete the **AWSServiceRoleForTrustedAdvisor** from your account. For more information, see Deleting a service-linked role for Trusted Advisor (p. 164).

**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. 71)

**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. 36)
- Refresh the list of available Trusted Advisor checks (p. 37)
- Poll a Trusted Advisor check for status changes (p. 37)
- Request a Trusted Advisor check result (p. 38)
- Print details of a Trusted Advisor check (p. 39)

**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.

```java
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());
    }
}
```
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.

```java
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.

```java
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String... checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request = new DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result = createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
```
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.

```java
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
        DescribeTrustedAdvisorCheckResultRequest()
            .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.

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

## 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. 40)
- Enable organizational view (p. 40)
- Refresh Trusted Advisor checks (p. 40)
- Create organizational view reports (p. 41)
- View the report summary (p. 43)
- Download an organizational view report (p. 44)
- Disable organizational view (p. 48)
- Using IAM policies to allow access to organizational view (p. 49)

API Version 2013-04-15
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, Enterprise On-Ramp, 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. 49).

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. 161).

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, under Preferences, choose Your organization.
3. Under Enable trusted access with AWS Organizations, turn on Enabled.

Note

Enabling organizational view for the management account doesn’t provide the same checks for all member accounts. For example, if your member accounts all have Basic Support, those accounts won’t have the same checks available as your management account. The AWS Support plan determines which Trusted Advisor checks are available for an account.

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, Enterprise On-Ramp, or Enterprise Support plan, 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
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 (.internet_explosion) 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

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

![Report summary for an organization](image)

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](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.
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.

```json
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountId": ["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"]
}
```
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.

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

<table>
<thead>
<tr>
<th>AccountId</th>
<th>CheckId</th>
<th>ResourceId</th>
<th>TimeStamp</th>
<th>CheckName</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.11122E+11</td>
<td>OchIdWououX1</td>
<td>LnW14f1M4ONMjmMLvY5i</td>
<td>1.58983E+12</td>
<td>Low Utilization Amazon EC2 Instances</td>
<td>Cost Optimizing</td>
</tr>
<tr>
<td>1.11122E+11</td>
<td>HCP006TJGY</td>
<td>dJrZxW36z2sw8eo9WU1</td>
<td>1.58983E+12</td>
<td>Security Groups - Specific Ports Unrestricted</td>
<td>Security</td>
</tr>
<tr>
<td>1.11122E+11</td>
<td>HCF006TJGY</td>
<td>1h2kmTBlw5dnuMAM_06</td>
<td>1.58983E+12</td>
<td>Security Groups - Specific Ports Unrestricted</td>
<td>Security</td>
</tr>
<tr>
<td>4.444566E+11</td>
<td>165NDGyre</td>
<td>dJrZxW36z2sw8eo9WU1</td>
<td>1.58983E+12</td>
<td>Security Groups - Unrestricted Access</td>
<td>Security</td>
</tr>
<tr>
<td>4.444566E+11</td>
<td>165NDGyre</td>
<td>1h2kmTBlw5dnuMAM_06</td>
<td>1.58983E+12</td>
<td>Security Groups - Unrestricted Access</td>
<td>Security</td>
</tr>
<tr>
<td>4.444566E+11</td>
<td>Pk0RwqBli</td>
<td>vioZmab45k1j2IWe_Woj5</td>
<td>1.58983E+12</td>
<td>Amazon S3 Bucket Permissions</td>
<td>Security</td>
</tr>
<tr>
<td>4.444566E+11</td>
<td>Pk0RwqBli</td>
<td>wAvA53YQowY6WxxBHF</td>
<td>1.58983E+12</td>
<td>Amazon S3 Bucket Permissions</td>
<td>Security</td>
</tr>
<tr>
<td>1.23457E+11</td>
<td>Pk0RwqBli</td>
<td>LucRrS1G5SmgaMa5V</td>
<td>1.58983E+12</td>
<td>Amazon S3 Bucket Permissions</td>
<td>Security</td>
</tr>
<tr>
<td>1.23457E+11</td>
<td>Pk0RwqBli</td>
<td>gWB2TMfC2eYe2Ms5yBgn</td>
<td>1.58983E+12</td>
<td>Amazon S3 Bucket Permissions</td>
<td>Security</td>
</tr>
<tr>
<td>7.77789E+11</td>
<td>Pk0RwqBli</td>
<td>M3LBS9e15C99xxppcppx</td>
<td>1.58983E+12</td>
<td>Amazon S3 Bucket Permissions</td>
<td>Security</td>
</tr>
<tr>
<td>7.77789E+11</td>
<td>Pk0RwqBli</td>
<td>47DEOpq38HBSa_TimW-SjH</td>
<td>1.58983E+12</td>
<td>IAM Password Policy</td>
<td>Security</td>
</tr>
<tr>
<td>7.77789E+11</td>
<td>H7igTZYB</td>
<td>1hIG50vV0D05H12-t7Kb1L</td>
<td>1.58983E+12</td>
<td>Amazon EBS Snapshots</td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td>7.77789E+11</td>
<td>w7g1z6lxecl</td>
<td>10Fe6GVAF0F-MuL8cd-d1l</td>
<td>1.58983E+12</td>
<td>Amazon EC2 Availability Zone Balance</td>
<td>Fault Tolerance</td>
</tr>
</tbody>
</table>

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, Enterprise On-Ramp, 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. 40).
- 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. 51).

# 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 reenable organizational view from the Trusted Advisor console. See Enable organizational view (p. 40).

## 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. 51)
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 and disable 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:DescribeCheckSummaries",
        "trustedadvisor:DescribeAccountAccess",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeReports",
        "trustedadvisor:DescribeServiceMetadata",
        "trustedadvisor:DescribeOrganizationAccounts",
        "trustedadvisor:ListAccountsForParent",
        "trustedadvisor:ListRoots",
        "trustedadvisor:ListOrganizationalUnitsForParent"
      ],
      "Resource": "*"
    },
    {  
      "Sid": "CreateReportStatement",
      "Effect": "Allow",
      "Action": [  
        "trustedadvisor:GenerateReport"
      ],
      "Resource": "*"
    },
    {  
      "Sid": "ManageOrganizationalViewStatement",
      "Effect": "Allow",
      "Action": [  
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource": "*"
    }
  ],
  "Resource": "*"
}
```

API Version: 2013-04-15
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.

```json
{
    "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:DescribeCheckSummaries",
                "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. 161).
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

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.
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.

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

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
```


Example: Athena query

The following example shows 10 sample entries from the report.
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
Using other AWS services to view Trusted Advisor reports

- 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. 40).

**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

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. 57) 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. 40).
2. Create and download another JSON report in the Trusted Advisor console. See Create organizational view reports (p. 41). 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. 52).

Note

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

Viewing AWS Security Hub controls in AWS Trusted Advisor

After you enable AWS Security Hub for your AWS account, you can view your security controls and their findings in the Trusted Advisor console. You can use Security Hub controls to identify security vulnerabilities in your account in the same way that you can use Trusted Advisor checks. You can view the check's status, the list of affected resources, and then follow Security Hub recommendations to address
your security issues. You can use this feature to find security recommendations from Trusted Advisor and Security Hub in one convenient location.

**Notes**

- From Trusted Advisor, you can view controls in the AWS Foundational Security Best Practices security standard except for controls that have the Category: Recover > Resilience. For a list of supported controls, see AWS Foundational Security Best Practices controls in the AWS Security Hub User Guide.

  For more information about the Security Hub categories, see Control categories.

- Currently, when Security Hub adds new controls to the AWS Foundational Security Best Practices security standard, there can be a delay of two to four weeks before you can view them in Trusted Advisor. This time frame is best effort and is not guaranteed.

**Topics**

- Prerequisites (p. 58)
- View your Security Hub findings (p. 58)
- Refresh your Security Hub findings (p. 60)
- Disable Security Hub from Trusted Advisor (p. 60)
- Troubleshooting (p. 60)

**Prerequisites**

You must meet the following requirements to enable the Security Hub integration with Trusted Advisor:

- You must have a Business, Enterprise On-Ramp, or Enterprise Support plan for this feature. You can find your support plan from the AWS Support Center or from the Support plans page. For more information, see Compare AWS Support plans.

- You must enable resource recording in AWS Config for the AWS Regions that you want for your Security Hub controls. For more information, see Enabling and configuring AWS Config.


  **Note**
  
  If you already completed these prerequisites, you can skip to View your Security Hub findings (p. 58).

**About AWS Organizations accounts**

If you already completed the prerequisites for a management account, this integration is enabled automatically for all member accounts in your organization. Individual member accounts don’t need to contact AWS Support to enable this feature. However, member accounts in your organization must enable Security Hub if they want to see their findings in Trusted Advisor.

If you want to disable this integration for a specific member account, see Disable this feature for AWS Organizations accounts (p. 60).

**View your Security Hub findings**

After you enable Security Hub for your account, it can take up to 24 hours for your Security Hub findings to appear in the Security page of the Trusted Advisor console.
To view your Security Hub findings in Trusted Advisor

1. Navigate to the Trusted Advisor console, and then choose the Security category.
2. In the Search by keyword field, enter the control name or description in the field.
   
   **Tip**
   For Source, you can choose AWS Security Hub to filter for Security Hub controls.

3. Choose the Security Hub control name to view the following information:
   
   - **Description** – Describes how this control checks your account for security vulnerabilities.
   - **Source** – Whether the check comes from AWS Trusted Advisor or AWS Security Hub. For Security Hub controls, you can find the control ID.
   - **Alert Criteria** – The status of the control. For example, if Security Hub detects an important issue, the status might be **Red: Critical or High**.
   - **Recommended Action** – Use the Security Hub documentation link to find the recommended steps to fix the issue.
   - **Security Hub resources** – You can find the resources in your account where Security Hub has detected an issue.

**Notes**

- You must use Security Hub to exclude resources from your findings. Currently, you can’t use the Trusted Advisor console to exclude items from Security Hub controls. For more information, see [Setting the workflow status for findings](#).
- The organizational view feature supports this integration with Security Hub. You can view your findings for your Security Hub controls across your organization, and then create and download reports. For more information, see [Organizational view for AWS Trusted Advisor](#).

**Example Example : Security Hub control for IAM user access key should not exist**

The following is an example finding for a Security Hub control in the Trusted Advisor console.
Refresh your Security Hub findings

After you enable a security standard, it can take up to two hours for Security Hub to have findings for your resources. It can then take up to 24 hours for that data to appear in the Trusted Advisor console. If you recently enabled the AWS Foundational Security Best Practices v1.0.0 security standard, check the Trusted Advisor console again later.

**Note**

- The refresh schedule for each Security Hub control is periodic or change triggered. Currently, you can't use the Trusted Advisor console or the AWS Support API to refresh your Security Hub controls. For more information, see Schedule for running security checks.
- You must use Security Hub if you want to exclude resources from your findings. Currently, you can't use the Trusted Advisor console to exclude items from Security Hub controls. For more information, see Setting the workflow status for findings.

Disable Security Hub from Trusted Advisor

Follow this procedure if you don't want your Security Hub information to appear in the Trusted Advisor console. This procedure only disables the Security Hub integration with Trusted Advisor. It won't affect your configurations with Security Hub. You can continue to use the Security Hub console to view your security controls, resources, and recommendations.

**To disable the Security Hub integration**

1. Contact AWS Support and request to disable the Security Hub integration with Trusted Advisor.

   After AWS Support disables this feature, Security Hub no longer sends data to Trusted Advisor. Your Security Hub data will be removed from Trusted Advisor.

2. If you want to enable this integration again, contact AWS Support.

Disable this feature for AWS Organizations accounts

If you already completed the previous procedure for a management account, Security Hub integration is automatically removed from all member accounts in your organization. Individual member accounts in your organization don't need to contact AWS Support separately.

If you're a member account in an organization, you can contact AWS Support to remove this feature from only your account.

Troubleshooting

If you're having issues with this integration, see the following troubleshooting information.

**Contents**

- I don't see Security Hub findings in the Trusted Advisor console (p. 61)
- I configured Security Hub and AWS Config correctly, but my findings are still missing (p. 61)
- I want to disable specific Security Hub controls (p. 61)
- I want to find my excluded Security Hub resources (p. 61)
- I want to enable or disable this feature for a member account that belongs to an AWS organization (p. 62)
- I see multiple AWS Regions for the same affected resource for a Security Hub check (p. 62)
- I turned off Security Hub or AWS Config in a Region (p. 62)
I still can't view my Security Hub findings (p. 62)

I don't see Security Hub findings in the Trusted Advisor console

Verify that you completed the following steps:

- You have a Business, Enterprise On-Ramp, or Enterprise Support plan.
- You enabled resource recording in AWS Config within the same Region as Security Hub.
- New controls from Security Hub are added as checks in Trusted Advisor within two to four weeks. See the note (p. 58).

For more information, see the Prerequisites (p. 58).

I configured Security Hub and AWS Config correctly, but my findings are still missing

It can take up to two hours for Security Hub to have findings for your resources. It can then take up to 24 hours for that data to appear in the Trusted Advisor console. Check the Trusted Advisor console again later.

Notes

- Only your findings for controls in the AWS Foundational Security Best Practices security standard will appear in Trusted Advisor except for controls that have the Category: Recover > Resilience.
- If there's a service issue with Security Hub or Security Hub isn't available, it can take up to 24 hours for your findings to appear in Trusted Advisor. Check the Trusted Advisor console again later.

I want to disable specific Security Hub controls

Security Hub sends your data to Trusted Advisor automatically. If you disable a Security Hub control or no longer have resources for that control, your findings won't appear in Trusted Advisor.

You can sign in to the Security Hub console and verify if your control is enabled or disabled.

If you disable a Security Hub control or disable all controls for the AWS Foundational Security Best Practices security standard, your findings are archived within the next five days. This five-day period to archive is approximate and best effort only, and isn't guaranteed. When your findings are archived, they are removed from Trusted Advisor.

For more information, see the following topics:

- Disabling and enabling individual controls
- Disabling or enabling a security standard

I want to find my excluded Security Hub resources

From the Trusted Advisor console, you can choose your Security Hub control name, and then choose the Excluded items option. This option displays all resources that are suppressed in Security Hub.
If the workflow status for a resource is set to SUPPRESSED, then that resource is an excluded item in Trusted Advisor. You can't suppress Security Hub resources from the Trusted Advisor console. To do so, use the Security Hub console. For more information, see Setting the workflow status for findings.

I want to enable or disable this feature for a member account that belongs to an AWS organization

By default, member accounts inherit the feature from the management account for AWS Organizations. If the management account has enabled the feature, then all accounts in the organization will also have the feature. If you have a member account and want to make specific changes for your account, you must contact AWS Support.

I see multiple AWS Regions for the same affected resource for a Security Hub check

Some AWS services are global and aren't specific to a Region, such as IAM and Amazon CloudFront. By default, global resources such as Amazon S3 buckets appear in the US East (N. Virginia) Region.

For Security Hub checks that evaluate resources for global services, you might see more than one item for affected resources. For example, if the Hardware MFA should be enabled for the root user check identifies that your account hasn't activated this feature, then you will see multiple Regions in the table for the same resource.

You can configure Security Hub and AWS Config so that multiple Regions won't appear for the same resource. For more information, see AWS Foundational Best Practices controls that you might want to disable.

I turned off Security Hub or AWS Config in a Region

If you stop resource recording with AWS Config or disable Security Hub in an AWS Region, Trusted Advisor no longer receives data for any controls in that Region. Your Security Hub data is removed from Trusted Advisor after 90 days. This time frame is approximate and best effort only, and isn't guaranteed. For more information, see Disabling Security Hub.

To disable this feature for your account, see Disable Security Hub from Trusted Advisor (p. 60).

I still can't view my Security Hub findings

If you still have issues with this feature, you can create a technical support case in the AWS Support Center.

Opt in AWS Compute Optimizer for Trusted Advisor checks

Compute Optimizer is a service that analyzes the configuration and utilization metrics of your AWS resources. This service reports whether your resources are correctly configured for efficiency and reliability. It also suggests improvements you can implement to improve workload performance. With Compute Optimizer, you view the same recommendations in your Trusted Advisor checks.

You can opt in either your AWS account only, or all member accounts that are part of an organization in AWS Organizations. For more information, see Getting started in the AWS Compute Optimizer User Guide.

Once you opt in for Compute Optimizer, the following checks receive data from your Lambda functions and Amazon EBS volumes. It can take up to 12 hours to generate the findings and optimization
recommendations. It can then take up to 48 hours to view your results in Trusted Advisor for the following checks:

**Cost optimization (p. 72)**
- Amazon EBS over-provisioned volumes
- AWS Lambda over-provisioned functions for memory size

**Performance (p. 91)**
- Amazon EBS under-provisioned volumes
- AWS Lambda under-provisioned functions for memory size

**Notes**
- Results for these checks are automatically refreshed several times daily. Refresh requests are not allowed. It might take a few hours for changes to appear. Currently, you can't exclude resources from these checks.
- Trusted Advisor already has the Underutilized Amazon EBS Volumes and the Overutilized Amazon EBS Magnetic Volumes checks.

Once you opt in with Compute Optimizer, we recommend that you use the new Amazon EBS over-provisioned volumes and Amazon EBS under-provisioned volumes checks instead.

**Related information**

For more information, see the following topics:
- Viewing Amazon EBS volume recommendations in the *AWS Compute Optimizer User Guide*
- Viewing Lambda function recommendations in the *AWS Compute Optimizer User Guide*
- Configuring Lambda function memory in the *AWS Lambda Developer Guide*
- Request modifications to your Amazon EBS volumes in the *Amazon EC2 User Guide for Linux Instances*

**Get started with AWS Trusted Advisor Priority**

Trusted Advisor Priority helps you secure and optimize your AWS account to follow AWS best practices. With Trusted Advisor Priority, your AWS account team can proactively monitor your account and create prioritized recommendations when they identify opportunities for you.

For example, your account team can identify if your root account doesn't have multi-factor authentication (MFA). Your account team can create a recommendation so that you take immediate action on a check, such as MFA on Root Account. The recommendation appears as an active prioritized recommendation on the Trusted Advisor Priority page of the Trusted Advisor console. You then follow the recommendations to resolve it.

Trusted Advisor Priority recommendations can come from either of two sources:

- AWS services – Services such as Trusted Advisor, AWS Security Hub, and AWS Well-Architected automatically create recommendations. Your account team shares these recommendations with you, so that they appear in Trusted Advisor Priority.
- Your account team – Your account team can create manual recommendations for risks that they identify in your account.
Trusted Advisor Priority helps you focus on the most important recommendations. You and your account team can keep track of the recommendation lifecycle, from when your account team shared the recommendation to when you accept, resolve, or reject it. You can use Trusted Advisor Priority to find recommendations for all member accounts in your organization.

**Topics**
- Prerequisites (p. 64)
- Enable Trusted Advisor Priority (p. 64)
- View prioritized recommendations (p. 64)
- Accept a recommendation (p. 65)
- Reject a recommendation (p. 66)
- Resolve a recommendation (p. 67)
- Reopen a recommendation (p. 69)
- Download recommendation details (p. 70)
- Register delegated administrators (p. 70)
- Deregister delegated administrators (p. 70)
- Manage Trusted Advisor Priority notifications (p. 70)
- Disable Trusted Advisor Priority (p. 71)

**Prerequisites**
You must have the following requirements for Trusted Advisor Priority:

- Your organization must have all features enabled for AWS Organizations. This adds Trusted Advisor as a trusted service with Organizations. You can enable trusted access from the Your organization page in the Trusted Advisor console or from Organizations. For more information, see Enabling all features in your organization in the AWS Organizations User Guide.
- You must have an Enterprise Support plan and sign in to the organization's management account.
- You must have AWS Identity and Access Management (IAM) permissions to access Trusted Advisor Priority. For information about controlling access to Trusted Advisor Priority, see AWS managed policies for AWS Trusted Advisor (p. 170) and Manage access for AWS Trusted Advisor (p. 177).

**Enable Trusted Advisor Priority**
Contact your account team and ask that they enable this feature for you. You must have an Enterprise Support plan and be the management account owner for your organization.

**View prioritized recommendations**
After Trusted Advisor Priority is enabled for your account, you can view the latest recommendations for your organization.

**To view your prioritized recommendations**
2. On the Trusted Advisor Priority page, you can view the following:
   - **Actions needed**–The number of recommendations that are pending a response or in progress.
• **Overview** – The number of recommendations for the following:
  • Rejected recommendations in the last 90 days
  • Resolved recommendations in the last 90 days
  • Recommendations without a status update in over 30 days
  • Average time to resolve recommendations

3. On the **Active** tab, the **Active prioritized recommendations** show recommendations that your account team prioritized for you.

To filter your results, use the following options:

• **Recommendation** – Enter keywords to search by name. This can be a check name, or a custom name that your account team created.

• **Status** – Whether the recommendation is pending a response, in progress, rejected, or resolved.

• **Source** – The origin of a prioritized recommendation. The recommendation can come from AWS services, your AWS account team, or a planned service event.

• **Category** – The recommendation category, such as security or cost optimization.

• **Age** – When your account team shared the recommendation with you.

4. Choose a recommendation to learn more about its risk details, affected resources and accounts, and the recommended actions that you should take to resolve it. You can then accept (p. 65) or reject (p. 66) the recommendation.

**Example: Trusted Advisor Priority recommendations**

The following example shows recommendations available in Trusted Advisor Priority.

![Image of Trusted Advisor Priority recommendations]

**Accept a recommendation**

On the **Active** tab, you can learn more about the recommendation and then decide if you want to accept it. When you accept a recommendation, you acknowledge the recommendation to your account and plan to address it.

**To accept a recommendation**

2. On the **Trusted Advisor Priority** page, on the **Active** tab, choose a recommendation name.

3. On the recommendation detail page, review the information and the affected resources and accounts in your organization.

4. Choose **Accept**.

5. In the **Accept recommendation** dialog box, enter your name and title, and then choose **Accept**.

   The recommendation status changes to **In progress**. Recommendations in progress or pending a response appear in the **Active** tab on the Trusted Advisor Priority page.

6. Follow the steps in the recommendation details to fix it. You can then resolve the recommendation. For more information, see **Resolve a recommendation** (p. 67).

**Example: Manual recommendation from Trusted Advisor Priority**

The following image shows a recommendation that is pending a response.

![VPC Endpoint Single AZ Configuration](image)

**Reject a recommendation**

You can also reject a recommendation, which means that you acknowledge the risk, but won’t fix it now. You can reject a recommendation if you don’t think it’s a risk, or if it’s not relevant to your account.
To reject a recommendation

2. On the Trusted Advisor Priority page, on the Active tab, choose a recommendation name.
3. On the recommendation detail page, review the information and the affected resources and accounts in your organization.
4. If this isn’t a risk for your account, choose Reject.
5. In the Reject dialog box, specify one of the following:
   - Acknowledged – won’t fix
   - Not a risk
6. For Reason for rejection, enter a reason why you won’t address the recommendation.
7. Enter your name and title.
8. Choose Reject. The recommendation status changes to Rejected and appears in the Closed tab on the Trusted Advisor Priority page.

   Trusted Advisor Priority also notifies your account team that you rejected the recommendation.

Example: Reject a recommendation from Trusted Advisor Priority

The following example shows a recommendation that isn’t a risk to an account.

Resolve a recommendation

After you accepted and fixed the risk, you can resolve the recommendation.
To resolve a recommendation

2. On the Trusted Advisor Priority page, select the recommendation, and then choose Resolve.
3. In the Resolve recommendation dialog box, enter your name and title.

Choose Resolve. Resolved recommendations appear in the Closed tab on the Trusted Advisor Priority page. Trusted Advisor Priority notifies your account team that you resolved the recommendation.

Example : Manual recommendation from Trusted Advisor Priority

The following example shows a resolved manual recommendation that your account team sent to your account.

---

**Overview**

- **Source**: Manual
- **Category**: Performance
- **Age**: 72 day(s)
  
  - **Shared by**: john doe@example.com
  - **Resolved by**: Shirley Rodriguez

**Details**

**Description**

A structured program available to Enterprise Support customers (and Business Support customers for an additional fee) that helps you plan for short-duration, large-scale events such as product or application launches, infrastructure migrations, and marketing events. We evaluate the operational readiness (architecture and scaling, service limit increases, capacity requests, etc.) of your workload, processes and procedures, and personnel to understand the operational risks related to your workload, and recommend an improvement plan. We participate with you during the event to reduce response time to AWS related service issues and escalate problems.

**Affected accounts**

123456789012

**Recommended action**

Proposing an IEM to ensure a smooth upscaling of AppStream fleet in preparation for CAD classes (Seasonal volume change) for October 2022

---
Reopen a recommendation

After you resolve a recommendation, you can reopen the recommendation later. You or your account team can reopen a recommendation if there's another related risk to your account.

To reopen a recommendation

1. On the Trusted Advisor Priority page, choose the Closed tab.
2. Under Closed recommendations, select the recommendation, and then choose Reopen.
3. In the Reopen recommendation dialog box, enter the following:
   - Why you're reopening the recommendation
   - Your name
   - Your title

4. Choose Reopen. The recommendation status changes to In progress and appears in the Active tab.
5. Follow the steps in the recommendation details to fix it.

Example: Reopen a recommendation from Trusted Advisor Priority

The following example shows a recommendation that you want to reopen.

Reopen recommendation

This will return the recommendation to the prioritized recommendations list. You can then take action on this recommendation later.

Reason for reopening

I need to revisit this recommendation

Your name

Mary Major

Your title

AWS account administrator
Download recommendation details

You can also download the results of a prioritized recommendation from Trusted Advisor Priority.

**Note**
Currently, you can download only one recommendation at a time.

**To download a recommendation**
2. On the **Trusted Advisor Priority** page, select the recommendation, and then choose **Download**.

Register delegated administrators

You can add member accounts that are part of your organization as delegated administrators. Delegated administrator accounts can review, accept, resolve, reject, and reopen recommendations in Trusted Advisor Priority.

After you register an account, you must grant the delegated administrator the required IAM permissions to access Trusted Advisor Priority. For more information, see Manage access for AWS Trusted Advisor (p. 177) and AWS managed policies for AWS Trusted Advisor (p. 170).

You can register up to five member accounts. Only the management account can add delegated administrators for the organization.

**To register a delegated administrator**
2. In the navigation pane, under **Preferences**, choose **Your organization**.
3. Under **Delegated administrator**, choose **Register new account**.
4. In the dialog box, enter the member account ID, and then choose **Register**.
5. (Optional) To deregister an account, select an account and choose **Deregister**. In the dialog box, choose **Deregister** again.

Deregister delegated administrators

When you deregister a member account, that account won't have the same access to Trusted Advisor Priority as the management account. Accounts that are no longer delegated administrators won't receive email notifications from Trusted Advisor Priority.

**To deregister a delegated administrator**
2. In the navigation pane, under **Preferences**, choose **Your organization**.
3. Under **Delegated administrator**, select an account and choose **Deregister**.
4. In the dialog box, choose **Deregister**.

Manage Trusted Advisor Priority notifications

Trusted Advisor Priority delivers notifications through email. This email notification includes a summary of the recommendations that your account team prioritized for you. You can specify the frequency that you receive updates from Trusted Advisor Priority.
If you registered member accounts as delegated administrators, they can also set up their accounts to receive Trusted Advisor Priority email notifications.

Trusted Advisor Priority email notifications don’t include check results for individual accounts and are separate from the Trusted Advisor dashboard weekly notification. For more information, see Set up notification preferences (p. 35).

**To manage your Trusted Advisor Priority notifications**

2. In the navigation pane, under Preferences, choose Notifications.
3. Under Trusted Advisor Priority, you can select the following options.
   b. Weekly – Receive an email notification once a week.
   c. Choose the notifications to receive:
      • Summary of prioritized recommendations
      • Resolution dates
4. For Recipients, select other contacts to receive the email notifications. You can add and remove contacts from the Account Settings page in the AWS Billing and Cost Management console.
5. For Language, choose the language for the email notification.
6. Choose Save your preferences.

**Note**

Trusted Advisor Priority sends email notifications from the noreply@notifications.trustedadvisor.us-west-2.amazonaws.com address. You might need to verify that your email client doesn’t identify these emails as spam.

**Disable Trusted Advisor Priority**

Contact your account team and ask that they disable this feature for you. After it’s removed, prioritized recommendations won’t appear in your Trusted Advisor console.

If you disable Trusted Advisor Priority and then enable it again later, you can still view the recommendations that your account team sent before you disabled Trusted Advisor Priority.

**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, Enterprise On-Ramp, 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. 36)
- 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. 133) category and the following checks in the security category:

- Amazon EBS Public Snapshots (p. 102)
- Amazon RDS Public Snapshots (p. 103)
- Amazon S3 Bucket Permissions (p. 105)
- IAM Use (p. 114)
- MFA on Root Account (p. 114)
- Security Groups – Specific Ports Unrestricted (p. 115)

Check categories
- Cost optimization (p. 72)
- Performance (p. 91)
- Security (p. 101)
- Fault tolerance (p. 116)
- Service limits (p. 133)

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

Check names
- Amazon Comprehend Underutilized Endpoints (p. 73)
- Amazon EBS over-provisioned volumes (p. 73)
- Amazon EC2 instances consolidation for Microsoft SQL Server (p. 74)
- Amazon EC2 instances over-provisioned for Microsoft SQL Server (p. 75)
- Amazon EC2 Reserved Instance Lease Expiration (p. 76)
- Amazon EC2 Reserved Instance Optimization (p. 77)
- Amazon ElastiCache Reserved Node Optimization (p. 78)
- Amazon OpenSearch Service Reserved Instance Optimization (p. 78)
- Amazon RDS Idle DB Instances (p. 79)
- Amazon Redshift Reserved Node Optimization (p. 80)
- Amazon Relational Database Service (RDS) Reserved Instance Optimization (p. 81)
- Amazon Route 53 Latency Resource Record Sets (p. 82)
- AWS Lambda Functions with Excessive Timeouts (p. 83)
- AWS Lambda Functions with High Error Rates (p. 84)
- AWS Lambda over-provisioned functions for memory size (p. 85)
- AWS Well-Architected high risk issues for cost optimization (p. 86)
- Idle Load Balancers (p. 86)
- Low Utilization Amazon EC2 Instances (p. 87)
- Savings Plan (p. 88)
- Unassociated Elastic IP Addresses (p. 89)
- Underutilized Amazon EBS Volumes (p. 89)
• Underutilized Amazon Redshift Clusters (p. 90)

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. Currently, you can't exclude resources from this check.

Check ID
Cm24dfsM12

Alert Criteria

Yellow: The endpoint is active, but hasn't been used for real-time inference requests in the past 15 days.

Recommended Action

If the endpoint hasn't been used in the past 15 days, we recommend that you define a scaling policy for the resource by using Application Autoscaling.

If the endpoint has a scaling policy defined and hasn't been used in the past 30 days, consider deleting the endpoint and using asynchronous inference. For more information, see Deleting an endpoint with Amazon Comprehend.

Report columns

• Status
• Region
• Endpoint ARN
• Provisioned Inference Unit
• AutoScaling Status
• Reason
• Last Updated Time

Amazon EBS over-provisioned volumes

Description

Checks the Amazon Elastic Block Store (Amazon EBS) volumes that were running at any time during the lookback period. This check alerts you if any EBS volumes were over-provisioned for your workloads. When you have over-provisioned volumes, you're paying for unused resources. Although some scenarios can result in low optimization by design, you can often lower your costs by changing the configuration of your EBS volumes. Estimated monthly savings are calculated by using the current usage rate for EBS volumes. Actual savings will vary if the volume isn't present for a full month.

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. Currently, you can't exclude resources from this check.
Check ID

COr6dfpM03

Alert Criteria

Yellow: An EBS Volume that was over-provisioned during the lookback period. To determine if a volume is over-provisioned, we consider all default CloudWatch metrics (including IOPS and throughput). The algorithm used to identify over-provisioned EBS volumes follows AWS best practices. The algorithm is updated when a new pattern has been identified.

Recommended Action

Consider downsizing volumes that have low utilization.

For more information, see Opt in AWS Compute Optimizer for Trusted Advisor checks (p. 62).

Report columns

- Status
- Region
- Volume ID
- Volume Type
- Volume Size (GB)
- Volume Baseline IOPS
- Volume Burst IOPS
- Volume Burst Throughput
- Recommended Volume Type
- Recommended Volume Size (GB)
- Recommended Volume Baseline IOPS
- Recommended Volume Burst IOPS
- Recommended Volume Baseline Throughput
- Recommended Volume Burst Throughput
- Lookback Period (days)
- Savings Opportunity (%)
- Estimated Monthly Savings
- Estimated Monthly Savings Currency
- Last Updated Time

Amazon EC2 instances consolidation for Microsoft SQL Server

Description

Checks your Amazon Elastic Compute Cloud (Amazon EC2) instances that are running SQL Server in the past 24 hours. This check alerts you if your instance has less than the minimum number of SQL Server licenses. From the Microsoft SQL Server Licensing Guide, you are paying 4 vCPU licenses even if an instance has only 1 or 2 vCPUs. You can consolidate smaller SQL Server instances to help lower costs.

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. Currently, you can’t exclude resources from this check.

Check ID

Qsdfp3A4L2
Alert Criteria

Yellow: An instance with SQL Server has less than 4 vCPUs.

Recommended Action

Consider consolidating smaller SQL Server workloads into instances with at least 4 vCPUs.

Additional Resources

- Microsoft SQL Server on AWS
- Microsoft Licensing on AWS
- Microsoft SQL Server Licensing Guide

Report columns

- Status
- Region
- Instance ID
- Instance Type
- vCPU
- Minimum vCPU
- SQL Server Edition
- Last Updated Time

Amazon EC2 instances over-provisioned for Microsoft SQL Server

Description

Checks your Amazon Elastic Compute Cloud (Amazon EC2) instances that are running SQL Server in the past 24 hours. An SQL Server database has a compute capacity limit for each instance. An instance with SQL Server Standard edition can use up to 48 vCPUs. An instance with SQL Server Web can use up to 32 vCPUs. This check alerts you if an instance exceeds this vCPU limit.

If your instance is over-provisioned, you pay full price without realizing an improvement in performance. You can manage the number and size of your instances to help lower costs.

Estimated monthly savings are calculated by using the same instance family with the maximum number of vCPUs that an SQL Server instance can use and the On-Demand pricing. Actual savings will vary if you’re using Reserved Instances (RI) or if the instance isn’t running for a full day.

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. Currently, you can’t exclude resources from this check.

Check ID

Qsdfp3A4L1

Alert Criteria

- Red: An instance with SQL Server Standard edition has more than 48 vCPUs.
- Red: An instance with SQL Server Web edition has more than 32 vCPUs.

Recommended Action

For SQL Server Standard edition, consider changing to an instance in the same instance family with 48 vCPUs. For SQL Server Web edition, consider changing to an instance in the same instance family...
with 32 vCPUs. If it is memory intensive, consider changing to memory optimized R5 instances. For more information, see Best Practices for Deploying Microsoft SQL Server on Amazon EC2.

Additional Resources

- Microsoft SQL Server on AWS
- You can use Launch Wizard to simplify your SQL Server deployment on EC2.

Report columns

- Status
- Region
- Instance ID
- Instance Type
- vCPU
- SQL Server Edition
- Maximum vCPU
- Recommended Instance Type
- Estimated Monthly Savings
- Last Updated Time

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

Alert Criteria

- Yellow: The Reserved Instance lease expires in less than 30 days.
- Yellow: The Reserved Instance lease expired in the preceding 30 days.

Recommended Action

Consider purchasing a new Reserved Instance to replace the one that is nearing the end of its term. For more information, see How to Purchase Reserved Instances and Buying Reserved Instances.

Additional Resources

- Reserved Instances
- Instance Types

Report columns

- Status
- Zone
- Instance Type
- Platform
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

Alert Criteria

Yellow: Optimizing the use of partial upfront RIs can help reduce costs.

Recommended Action

See the Cost Explorer page for more detailed and customized recommendations. Additionally, refer to the buying guide to understand how to purchase RIs and the options available.

Additional Resources

- Information on RIs and how they can save you money can be found here.
- For more information on this recommendation, see Reserved Instance Optimization Check Questions in the Trusted Advisor FAQs.

Report columns

- Region
- Instance Type
- Platform
- Recommended Number of RIs to Purchase
- Expected Average RI Utilization
- Estimated Savings with Recommendations (Monthly)
- Upfront Cost of RIs
- Estimated costs of RIs (Monthly)
- Estimated On-Demand Cost Post Recommended RI Purchase (Monthly)
- Estimated Break Even (Months)
- Lookback Period (Months)
- Term (Years)
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

h3L3otH3re

Alert Criteria

Yellow: Optimizing the purchase of ElastiCache Reserved Nodes can help reduce costs.

Recommended Action

See the Cost Explorer page for more detailed recommendations, customization options (e.g. look-back period, payment option, etc.) and to purchase ElastiCache Reserved Nodes.

Additional Resources

- Information on ElastiCache Reserved Nodes and how they can save you money can be found here.
- For more information on this recommendation, see Reserved Instance Optimization Check Questions in the Trusted Advisor FAQs.
- For more detailed description of fields, see Cost Explorer documentation

Report columns

- Region
- Family
- Node Type
- Product Description
- Recommended number of Reserved Nodes to purchase
- Expected Average Reserved Node Utilization
- Estimated Savings with Recommendations (monthly)
- Upfront Cost of Reserved Nodes
- Estimated cost of Reserved Nodes (monthly)
- Estimated On-Demand Cost Post Recommended Reserved Nodes Purchase (monthly)
- Estimated Break Even (months)
- Lookback Period (days)
- Term (years)

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

**Alert Criteria**

Yellow: Optimizing the purchase of Amazon OpenSearch Service Reserved Instances can help reduce costs.

**Recommended Action**

See the Cost Explorer page for more detailed recommendations, customization options (e.g. look-back period, payment option, etc.) and to purchase Amazon OpenSearch Service Reserved Instances.

**Additional Resources**

- Information on Amazon OpenSearch Service Reserved Instances and how they can save you money can be found here.
- For more information on this recommendation, see Reserved Instance Optimization Check Questions in the Trusted Advisor FAQs.
- For more detailed description of fields, see Cost Explorer documentation

**Report columns**

- Region
- Instance Class
- Instance Size
- Recommended number of Reserved Instances to purchase
- Expected Average Reserved Instance Utilization
- Estimated Savings with Recommendation (monthly)
- Upfront Cost of Reserved Instances
- Estimated cost of Reserved Instances (monthly)
- Estimated On-Demand Cost Post Recommended Reserved Instance Purchase (monthly)
- Estimated Break Even (months)
- Lookback Period (days)
- Term (years)

**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

Alert Criteria

Yellow: An active DB instance has not had a connection in the last 7 days.

Recommended Action

Consider taking a snapshot of the idle DB instance and then either stopping it or deleting it. Stopping the DB instance removes some of the costs for it, but does not remove storage costs. A stopped instance keeps all automated backups based upon the configured retention period. Stopping a DB instance usually incurs additional costs when compared to deleting the instance and then retaining only the final snapshot. See Stopping an Amazon RDS instance temporarily and Deleting a DB Instance with a Final Snapshot.

Additional Resources

Back Up and Restore

Report columns

• Region
• DB Instance Name
• Multi-AZ
• Instance Type
• Storage Provisioned (GB)
• Days Since Last Connection
• Estimated Monthly Savings (On Demand)

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

Alert Criteria

Yellow: Optimizing the purchase of Amazon Redshift Reserved Nodes can help reduce costs.

Recommended Action

See the Cost Explorer page for more detailed recommendations, customization options (e.g. look-back period, payment option, etc.) and to purchase Amazon Redshift Reserved Nodes.
Additional Resources

- Information on Amazon Redshift Reserved Nodes and how they can save you money can be found [here](#).
- For more information on this recommendation, see [Reserved Instance Optimization Check Questions](#) in the Trusted Advisor FAQs.
- For more detailed description of fields, see [Cost Explorer documentation](#).

Report columns

- Region
- Family
- Node Type
- Recommended number of Reserved Nodes to purchase
- Expected Average Reserved Node Utilization
- Estimated Savings with Recommendation (monthly)
- UpFront Cost of Reserved Nodes
- Estimated cost of Reserved Nodes (monthly)
- Estimated On-Demand Cost Post Recommended Reserved Nodes Purchase (monthly)
- Estimated Break Even (months)
- Lookback Period (days)
- Term (years)

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

Alert Criteria

Yellow: Optimizing the purchase of Amazon RDS Reserved Instances can help reduce costs.

Recommended Action

See the [Cost Explorer](#) page for more detailed recommendations, customization options (e.g. lookback period, payment option, etc.) and to purchase Amazon RDS Reserved Instances.

Additional Resources

- Information on Amazon RDS Reserved Instances and how they can save you money can be found [here](#).
• For more information on this recommendation, see Reserved Instance Optimization Check Questions in the Trusted Advisor FAQs.
• For more detailed description of fields, see Cost Explorer documentation

Report columns
• Region
• Family
• Instance Type
• Licence Model
• Database Edition
• Database Engine
• Deployment Option
• Recommended number of Reserved Instances to purchase
• Expected Average Reserved Instance Utilization
• Estimated Savings with Recommendation (monthly)
• Upfront Cost of Reserved Instances
• Estimated cost of Reserved Instances (monthly)
• Estimated On-Demand Cost Post Recommended Reserve Instance Purchase (monthly)
• Estimated Break Even (months)
• Lookback Period (days)
• Term (years)

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

Alert Criteria
Yellow: Only one latency resource record set is configured for a particular domain name.

Recommended Action
If you have resources in multiple regions, be sure to define a latency resource record set for each region. See Latency-Based Routing.

If you have resources in only one AWS Region, consider creating resources in more than one AWS Region and define latency resource record sets for each; see Latency-Based Routing.

If you don’t want to use multiple AWS Regions, you should use a simple resource record set. See Working with Resource Record Sets.

Additional Resources
• Amazon Route 53 Developer Guide
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. Currently, you can’t exclude resources from this check.

Check ID
L4dfs2Q3C3

Alert Criteria

Yellow: Functions where > 10% of invocations end in an error due to a timeout on any given day within the last 7 days.

Recommended Action

Inspect function logging and X-ray traces to determine the contributor to the high function duration. Implement logging in your code at relevant parts, such as before or after API calls or database connections. By default, AWS SDK clients timeouts may be longer than the configured function duration. Adjust API and SDK connection clients to retry or fail within the function timeout. If the expected duration is longer than the configured timeout, you can increase the timeout setting for the function. For more information, see Monitoring and troubleshooting Lambda applications.

Additional Resources

- Monitoring and troubleshooting Lambda applications
- Lambda Function Retry Timeout SDK
- Using AWS Lambda with AWS X-Ray
- Accessing Amazon CloudWatch logs for AWS Lambda
- Error Processor Sample Application for AWS Lambda

Report columns

- Status
- Region
- Function ARN
- Max Daily Timeout Rate
- Date of Max Daily Timeout Rate
- Average Daily Timeout Rate
- Function Timeout Settings (millisecond)
AWS Support User Guide
Cost optimization

• Lost Daily Compute Cost
• Average Daily Invokes
• Current Day Invokes
• Current Day Timeout Rate
• Last Updated Time

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. Currently, you can't exclude resources from this check.

Check ID
L4dfe2Q3C2

Alert Criteria

Yellow: Functions where > 10% of invocations end in error on any given day within the last 7 days.

Recommended Action

Consider the following guidelines to reduce errors. Function errors include errors returned by the function's code and errors returned by the function's runtime.

To help you troubleshoot Lambda errors, Lambda integrates with services like Amazon CloudWatch and AWS X-Ray. You can use a combination of logs, metrics, alarms, and X-Ray tracing to quickly detect and identify issues in your function code, API, or other resources that support your application. For more information, see Monitoring and troubleshooting Lambda applications.

For more information on handling errors with specific runtimes, see Error handling and automatic retries in AWS Lambda.

For additional troubleshooting, see Troubleshooting issues in Lambda.

You can also choose from an ecosystem of monitoring and observability tools provided by AWS Lambda partners. For more information, see AWS Lambda Partners.

Additional Resources

- Error Handling and Automatic Retries in AWS Lambda
- Monitoring and Troubleshooting Lambda applications
- Lambda Function Retry Timeout SDK
- Troubleshooting issues in Lambda
- API Invoke Errors
- Error Processor Sample Application for AWS Lambda

Report columns

- Status
- Region
AWS Support User Guide
Cost optimization

- Function ARN
- Max Daily Error Rate
- Date for Max Error Rate
- Average Daily Error Rate
- Lost Daily Compute Cost
- Average Daily Invokes
- Current Day Invokes
- Current Day Error Rate
- Last Updated Time

AWS Lambda over-provisioned functions for memory size

Description

Checks the AWS Lambda functions that were invoked at least once during the lookback period. This check alerts you if any of your Lambda functions were over-provisioned for memory size. When you have Lambda functions that are over-provisioned for memory sizes, you're paying for unused resources. Although some scenarios can result in low utilization by design, you can often lower your costs by changing the memory configuration of your Lambda functions. Estimated monthly savings are calculated by using the current usage rate for Lambda functions.

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. Currently, you can’t exclude resources from this check.

Check ID

COr6dpM05

Alert Criteria

Yellow: A Lambda function that was over-provisioned for memory size during the lookback period. To determine if a Lambda function is over-provisioned, we consider all default CloudWatch metrics for that function. The algorithm used to identify over-provisioned Lambda functions for memory size follows AWS best practices. The algorithm is updated when a new pattern has been identified.

Recommended Action

Consider reducing the memory size of your Lambda functions.

For more information, see Opt in AWS Compute Optimizer for Trusted Advisor checks (p. 62).

Report columns

- Status
- Region
- Function Name
- Function Version
- Memory Size (GB)
- Recommended Memory Size (GB)
- Lookback Period (days)
- Savings Opportunity (%)
- Estimated Monthly Savings
- Estimated Monthly Savings Currency
AWS Well-Architected high risk issues for cost optimization

Description

Checks for high risk issues (HRIs) for your workloads in the cost optimization pillar. This check is based on your AWS-Well Architected reviews. Your check results depend on whether you completed the workload evaluation with AWS Well-Architected.

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. Currently, you can’t exclude resources from this check.

Check ID

Wxdfp4B1L1

Alert Criteria

• Red: At least one active high risk issue was identified in the cost optimization pillar for AWS Well-Architected.
• Green: No active high risk issues were detected in the cost optimization pillar for AWS Well-Architected.

Recommended Action

AWS Well-Architected detected high risk issues during your workload evaluation. These issues present opportunities to reduce risk and save money. Sign in to the AWS Well-Architected tool to review your answers and take action to resolve your active issues.

Report columns

• Status
• Region
• Workload ARN
• Workload Name
• Reviewer Name
• Workload Type
• Workload Started Date
• Workload Last Modified Date
• Number of identified HRIs for Cost Optimization
• Number of HRIs resolved for Cost Optimization
• Number of questions answered for Cost Optimization
• Total number of questions in Cost Optimization pillar
• Last Updated Time

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

**Alert Criteria**

- **Yellow:** A load balancer has no active back-end instances.
- **Yellow:** A load balancer has no healthy back-end instances.
- **Yellow:** A load balancer has had less than 100 requests per day for the last 7 days.

**Recommended Action**

If your load balancer has no active back-end instances, consider registering instances or deleting your load balancer. See [Registering Your Amazon EC2 Instances with Your Load Balancer](#) or [Delete Your Load Balancer](#).

If your load balancer has no healthy back-end instances, see [Troubleshooting Elastic Load Balancing: Health Check Configuration](#).

If your load balancer has had a low request count, consider deleting your load balancer. See [Delete Your Load Balancer](#).

**Additional Resources**

- [Managing Load Balancers](#)
- [Troubleshoot Elastic Load Balancing](#)

**Report columns**

- Region
- Load Balancer Name
- Reason
- Estimated Monthly Savings

## 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

**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 User Guide
- Auto Scaling Developer Guide

**Report columns**
- Region/AZ
- Instance ID
- Instance Name
- Instance Type
- Estimated Monthly Savings
- CPU Utilization 14-day Average
- Network I/O 14-Day Average
- Number of Days Low Utilization

**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**

vZ2cW1srf

**Alert Criteria**

Yellow: Optimizing the purchase of Savings Plans can help reduce costs.

**Recommended Action**

See the Cost Explorer page for more detailed and customized recommendations and to purchase Savings Plans.

**Additional Resources**
- Savings Plan User Guide
- Savings Plans FAQ

**Report columns**
- Savings Plan type
- Payment option
• Upfront cost
• Hourly commitment to purchase
• Estimated average utilization
• Estimated monthly savings
• Estimated savings percentage
• Term (Years)
• Lookback Period (Days)

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

Alert Criteria
Yellow: An allocated Elastic IP address (EIP) is not associated with a running Amazon EC2 instance.

Recommended Action
Associate the EIP with a running active instance, or release the unassociated EIP. For more information, see Associating an Elastic IP Address with a Different Running Instance and Releasing an Elastic IP Address.

Additional Resources
Elastic IP Addresses

Report columns
• Region
• IP Address

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

Alert Criteria
Yellow: A volume is unattached or had less than 1 IOPS per day for the past 7 days.
**Recommended Action**

Consider creating a snapshot and deleting the volume to reduce costs. For more information, see [Creating an Amazon EBS Snapshot](https://docs.aws.amazon.com/elasticblockstore/latest/api/guide/gpfs-aws-create-snapshot.html) and [Deleting an Amazon EBS Volume](https://docs.aws.amazon.com/elasticblockstore/latest/api/gpfs-aws-delete-volumes.html).

**Additional Resources**

- Amazon Elastic Block Store (Amazon EBS)
- Monitoring the Status of Your Volumes

**Report columns**

- Region
- Volume ID
- Volume Name
- Volume Type
- Volume Size
- Monthly Storage Cost
- Snapshot ID
- Snapshot Name
- Snapshot Age

**Note**

If you opted in your account for AWS Compute Optimizer, we recommend that you use the Amazon EBS over-provisioned volumes check instead. For more information, see [Opt in AWS Compute Optimizer for Trusted Advisor checks](https://docs.aws.amazon.com/compute-optimizer/latest/userguide/optimization-configuration-awscomputeoptimizer.html#optimization-configuration-awscomputeoptimizer-over-provisioned-volumes) (p. 62).

---

**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**

G31sQ1B9U

**Alert Criteria**

- Yellow: A running cluster has not had a connection in the last 7 days.
- Yellow: A running cluster had less than 5% cluster-wide average CPU utilization for 99% of the last 7 days.

**Recommended Action**

Consider shutting down the cluster and taking a final snapshot, or downsizing the cluster. See [Shutting Down and Deleting Clusters](https://docs.aws.amazon.com/redshift/latest/gsg/shutdown-cluster.html) and [Resizing a Cluster](https://docs.aws.amazon.com/redshift/latest/gsg/resizing-cluster.html).

**Additional Resources**

- Amazon CloudWatch User Guide

**Report columns**

- Status
- Region
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. 91)
- Amazon EBS under-provisioned volumes (p. 92)
- Amazon EC2 to EBS Throughput Optimization (p. 93)
- Amazon Route 53 Alias Resource Record Sets (p. 94)
- AWS Lambda under-provisioned functions for memory size (p. 94)
- AWS Well-Architected high risk issues for performance (p. 95)
- CloudFront Alternate Domain Names (p. 96)
- CloudFront Content Delivery Optimization (p. 97)
- CloudFront Header Forwarding and Cache Hit Ratio (p. 97)
- High Utilization Amazon EC2 Instances (p. 98)
- Large Number of EC2 Security Group Rules Applied to an Instance (p. 99)
- Large Number of Rules in an EC2 Security Group (p. 99)
- Overutilized Amazon EBS Magnetic Volumes (p. 100)

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

PPk2rjsH2q

Alert Criteria

Yellow: An Amazon EC2 instance that can be EBS-optimized has an attached Provisioned IOPS (SSD) volume but the instance is not EBS-optimized.

Recommended Action

Create a new instance that is EBS-optimized, detach the volume, and reattach the volume to your new instance. For more information, see Amazon EBS-Optimized Instances and Attaching an Amazon EBS Volume to an Instance.
Additional Resources
- Amazon EBS Volume Types
- Amazon EBS Volume Performance

Report columns
- Status
- Region/AZ
- Volume ID
- Volume Name
- Volume Attachment
- Instance ID
- Instance Type
- EBS Optimized

Amazon EBS under-provisioned volumes

Description
Checks the Amazon Elastic Block Store (Amazon EBS) volumes that were running at any time during the lookback period. This check alerts you if any EBS volumes were under-provisioned for your workloads. Consistent high utilization can indicate optimized, steady performance, but can also indicate that an application does not have enough resources.

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. Currently, you can’t exclude resources from this check.

Check ID
COr6dfpM04

Alert Criteria
Yellow: An EBS Volume that was under-provisioned during the lookback period. To determine if a volume is under-provisioned, we consider all default CloudWatch metrics (including IOPS and throughput). The algorithm used to identify under-provisioned EBS volumes follows AWS best practices. The algorithm is updated when a new pattern has been identified.

Recommended Action
Consider upsizing volumes that have high utilization.

For more information, see Opt in AWS Compute Optimizer for Trusted Advisor checks (p. 62).

Report columns
- Status
- Region
- Volume ID
- Volume Type
- Volume Size (GB)
- Volume Baseline IOPS
- Volume Burst IOPS
- Volume Burst Throughput
- Recommended Volume Type
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

Alert Criteria

Yellow: In the preceding day (UTC), the aggregate throughput (megabytes/sec) of the EBS volumes attached to the EC2 instance exceeded 95% of the published throughput between the instance and the EBS volumes more than 50% of time.

Recommended Action

Compare the maximum throughput of your Amazon EBS volumes (see Amazon EBS Volume Types) with the maximum throughput of the Amazon EC2 instance they are attached to. See Instance Types That Support EBS Optimization.

Consider attaching your volumes to an instance that supports higher throughput to Amazon EBS for optimal performance.

Additional Resources

- Amazon EBS Volume Types
- Amazon EBS-Optimized Instances
- Monitoring the Status of Your Volumes
- Attaching an Amazon EBS Volume to an Instance
- Detaching an Amazon EBS Volume from an Instance
- Deleting an Amazon EBS Volume

Report columns

- Status
- Region
- Instance ID
- Instance Type
- Time Near Maximum
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

Alert Criteria

- Yellow: A resource record set is a CNAME to an Amazon S3 website.
- Yellow: A resource record set is a CNAME to an Amazon CloudFront distribution.
- Yellow: A resource record set is a CNAME to an Elastic Load Balancing load balancer.

Recommended Action

Replace the listed CNAME resource record sets with alias resource record sets; see Choosing Between Alias and Non-Alias Resource Record Sets.

You also need to change the record type from CNAME to A or AAAA, depending on the AWS resource. See Values that You Specify When You Create or Edit Amazon Route 53 Resource Record Sets.

Additional Resources

Routing Queries to AWS Resources

Report columns

- Status
- Hosted Zone Name
- Hosted Zone ID
- Resource Record Set Name
- Resource Record Set Type
- Resource Record Set Identifier
- Alias Target

AWS Lambda under-provisioned functions for memory size

Description

Checks the AWS Lambda functions that were invoked at least once during the lookback period. This check alerts you if any of your Lambda functions were under-provisioned for memory size. When you have Lambda functions that are under-provisioned for memory size, these functions take longer time to complete.

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. Currently, you can’t exclude resources from this check.
Check ID

COr6dpM06

Alert Criteria

Yellow: A Lambda function that was under-provisioned for memory size during the lookback period. To determine if a Lambda function is under-provisioned, we consider all default CloudWatch metrics for that function. The algorithm used to identify under-provisioned Lambda functions for memory size follows AWS best practices. The algorithm is updated when a new pattern has been identified.

Recommended Action

Consider increasing the memory size of your Lambda functions.

For more information, see Opt in AWS Compute Optimizer for Trusted Advisor checks (p. 62).

Report columns

- Status
- Region
- Function Name
- Function Version
- Memory Size (GB)
- Recommended Memory Size (GB)
- Lookback Period (days)
- Performance Risk
- Last Updated Time

AWS Well-Architected high risk issues for performance

Description

Checks for high risk issues (HRIs) for your workloads in the performance pillar. This check is based on your AWS-Well Architected reviews. Your check results depend on whether you completed the workload evaluation with AWS Well-Architected.

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. Currently, you can’t exclude resources from this check.

Check ID

Wxdfp4B1L2

Alert Criteria

- Red: At least one active high risk issue was identified in the performance pillar for AWS Well-Architected.
- Green: No active high risk issues were detected in the performance pillar for AWS Well-Architected.

Recommended Action

AWS Well-Architected detected high risk issues during your workload evaluation. These issues present opportunities to reduce risk and save money. Sign in to the AWS Well-Architected tool to review your answers and take action to resolve your active issues.

Report columns

- Status
- Region
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 outsides of this AWS account.

Check ID
N420c450f2

Alert Criteria
- Yellow: A CloudFront distribution includes alternate domain names, but the DNS configuration is not correctly set up with a CNAME record or an Amazon Route 53 alias resource record.
- Yellow: A CloudFront distribution includes alternate domain names, but Trusted Advisor could not evaluate the DNS configuration because there were too many redirects.
- Yellow: A CloudFront distribution includes alternate domain names, but Trusted Advisor could not evaluate the DNS configuration for some other reason, most likely because of a timeout.

Recommended Action
Update the DNS configuration to route DNS queries to the CloudFront distribution; see Using Alternate Domain Names (CNAMEs).

If you’re using Amazon Route 53 as your DNS service, see Routing Traffic to an Amazon CloudFront Web Distribution by Using Your Domain Name. If the check timed out, try refreshing the check.

Additional Resources
Amazon CloudFront Developer Guide

Report columns
- Status
- Distribution ID
- Distribution Domain Name
- Alternate Domain Name
- Reason
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

Alert Criteria

- Yellow: The amount of data transferred out of the bucket to your users by GET requests in the 30 days preceding the check is at least 25 times greater than the average amount of data stored in the bucket.
- Red: The amount of data transferred out of the bucket to your users by GET requests in the 30 days preceding the check is at least 10 TB and at least 25 times greater than the average amount of data stored in the bucket.

Recommended Action

Consider using CloudFront for better performance. See Amazon CloudFront Product Details.

If the data transferred is 10 TB per month or more, see Amazon CloudFront Pricing to explore possible cost savings.

Additional Resources

- Amazon CloudFront Developer Guide
- AWS Case Study: PBS

Report columns

- Status
- Region
- Bucket Name
- S3 Storage (GB)
- Data Transfer Out (GB)
- Ratio of Transfer to Storage

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
Alert Criteria

Yellow: One or more request headers that CloudFront forwards to your origin might significantly reduce your cache hit ratio.

Recommended Action

Consider whether the request headers provide enough benefit to justify the negative effect on the cache hit ratio. If your origin returns the same object regardless of the value of a given header, we recommend that you don’t configure CloudFront to forward that header to the origin. For more information, see Configuring CloudFront to Cache Objects Based on Request Headers.

Additional Resources

- Increasing the Proportion of Requests that Are Served from CloudFront Edge Caches
- CloudFront Cache Statistics Reports
- HTTP Request Headers and CloudFront Behavior

Report columns

- Distribution ID
- Distribution Domain Name
- Cache Behavior Path Pattern
- Headers

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

ZRxQ1Ps6c

Alert Criteria

Yellow: An instance had more than 90% daily average CPU utilization on at least 4 of the previous 14 days.

Recommended Action

Consider adding more instances. For information about scaling the number of instances based on demand, see What is Auto Scaling?

Additional Resources

- Monitoring Amazon EC2
- Instance Metadata and User Data
- Amazon CloudWatch User Guide
- Amazon EC2 Auto Scaling User Guide

Report columns

- Region/AZ
- Instance ID
- Instance Type
• Instance Name
• 14-Day Average CPU Utilization
• Number of Days over 90% CPU Utilization

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

Alert Criteria

• Yellow: An Amazon EC2-VPC instance has more than 50 security group rules.
• Yellow: An Amazon EC2-Classic instance has more than 100 security group rules.

Recommended Action

Reduce the number of rules associated with an instance by deleting unnecessary or overlapping rules. For more information, see Deleting Rules from a Security Group.

Additional Resources

Amazon EC2 Security Groups

Report columns

• Region
• Instance ID
• Instance Name
• VPC ID
• Total Inbound Rules
• Total Outbound Rules

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

Alert Criteria

• Yellow: An Amazon EC2-VPC security group has more than 50 rules.
• Yellow: An Amazon EC2-Classic security group has more than 100 rules.

Recommended Action

Reduce the number of rules in a security group by deleting unnecessary or overlapping rules. For more information, see Deleting Rules from a Security Group.
Additional Resources

Amazon EC2 Security Groups

Report columns
- Region
- Security Group Name
- Group ID
- Description
- Instance Count
- VPC ID
- Total Inbound Rules
- Total Outbound Rules

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.

For a list of instance types that support EBS-optimized behavior, see Amazon EBS-Optimized Instances.

To get daily utilization metrics, download the report for this check. The detailed report shows a column for each of the last 14 days. If there is no active EBS volume, the cell is empty. If there is insufficient data to make a reliable measurement, the cell contains N/A. If there is sufficient data, the cell contains the daily median and the percentage of the variance in relation to the median (for example, 256 / 20%).

Check ID
k3J2hns32g

Alert Criteria
Yellow: An Amazon EBS Magnetic volume is attached to an instance that can be EBS-optimized or is part of a cluster compute network with a daily median of more than 95 IOPS, and varies by less than 10% of the median value for at least 7 of the past 14 days.

Recommended Action
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.

Additional Resources
Amazon Elastic Block Store (Amazon EBS)

Report columns
- Status
- Region
- Volume ID
- Volume Name
Security

You can use the following checks for the security category.

Note
If you enabled Security Hub for your AWS account, you can view your findings in the Trusted Advisor console. For information, see Viewing AWS Security Hub controls in AWS Trusted Advisor (p. 57).

You can view all controls in the AWS Foundational Security Best Practices security standard except for controls that have the Category: Recover > Resilience. For a list of supported controls, see AWS Foundational Security Best Practices controls in the AWS Security Hub User Guide.

Check names
- Amazon EC2 instances with Microsoft SQL Server end of support (p. 101)
- Amazon EBS Public Snapshots (p. 102)
- Amazon RDS Public Snapshots (p. 103)
- Amazon RDS Security Group Access Risk (p. 104)
- Amazon Route 53 MX Resource Record Sets and Sender Policy Framework (p. 104)
- Amazon S3 Bucket Permissions (p. 105)
- AWS CloudTrail Logging (p. 106)
- AWS Lambda Functions Using Deprecated Runtimes (p. 107)
- AWS Well-Architected high risk issues for security (p. 107)
- CloudFront Custom SSL Certificates in the IAM Certificate Store (p. 108)
- CloudFront SSL Certificate on the Origin Server (p. 109)
- ELB Listener Security (p. 110)
- ELB Security Groups (p. 111)
- Exposed Access Keys (p. 111)
- IAM Access Key Rotation (p. 112)
- IAM Password Policy (p. 113)
- IAM Use (p. 114)
- MFA on Root Account (p. 114)
- Security Groups – Specific Ports Unrestricted (p. 115)
- Security Groups – Unrestricted Access (p. 116)

Amazon EC2 instances with Microsoft SQL Server end of support

Description
Checks the SQL Server versions for Amazon Elastic Compute Cloud (Amazon EC2) instances running in the past 24 hours. This check alerts you if the versions are near or have reached the end of support.
support. Each SQL Server version offers 10 years of support, including 5 years of mainstream support and 5 years of extended support. After the end of support, the SQL Server version won’t receive regular security updates. Running applications with unsupported SQL Server versions can bring security or compliance risks.

**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. Currently, you can’t exclude resources from this check.

**Check ID**
Qsdfp3A4L3

**Alert Criteria**
- Red: An EC2 instance has an SQL Server version that reached the end of support.
- Yellow: An EC2 instance has an SQL Server version that will reach the end of support in 12 months.

**Recommended Action**
To modernize your SQL Server workloads, consider refactoring to AWS Cloud native databases like Amazon Aurora. For more information, see Modernize Windows Workloads with AWS.

To move to a fully managed database, consider replatforming to Amazon Relational Database Service (Amazon RDS). For more information, see Amazon RDS for SQL Server.

To upgrade your SQL Server on Amazon EC2, consider using the automation runbook to simplify your upgrade. For more information, see the AWS Systems Manager documentation.

If you can't upgrade your SQL Server on Amazon EC2, consider the End-of-Support Migration Program (EMP) for Windows Server. For more information, see the EMP Website.

**Additional Resources**
- Get ready for SQL Server end of support with AWS
- Microsoft SQL Server on AWS

**Report columns**
- Status
- Region
- Instance ID
- SQL Server Version
- Support Cycle
- End of Support
- Last Updated Time

---

**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

Alert Criteria

Red: The EBS volume snapshot is marked as public.

Recommended Action

Unless you are certain you want to share all the data in the snapshot with all AWS accounts and users, modify the permissions: mark the snapshot as private, and then specify the accounts that you want to give permissions to. For more information, see Sharing an Amazon EBS Snapshot. This check can't be excluded from view in the Trusted Advisor console.

To modify permissions for your snapshots directly, you can use a runbook in the AWS Systems Manager console. For more information, see AWSSupport-ModifyEBSSnapshotPermission.

Additional Resources

Amazon EBS Snapshots

Report columns

- Status
- Region
- Volume ID
- Snapshot ID
- Description

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

Alert Criteria

Red: The Amazon RDS snapshot is marked as public.

Recommended Action

Unless you are certain you want to share all the data in the snapshot with all AWS accounts and users, modify the permissions: mark the snapshot as private, and then specify the accounts that you want to give permissions to. For more information, see Sharing a DB Snapshot or DB Cluster Snapshot. This check can't be excluded from view in the Trusted Advisor console.

To modify permissions for your snapshots directly, you can use a runbook in the AWS Systems Manager console. For more information, see AWSSupport-ModifyRDSSnapshotPermission.
Additional Resources

Back up and restoring Amazon RDS DB instances

Report columns

- Status
- Region
- DB Instance or Cluster ID
- Snapshot ID

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

Alert Criteria

- Yellow: A DB security group rule references an Amazon EC2 security group that grants global access on one of these ports: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Yellow: A DB security group rule grants access to more than a single IP address (the CIDR rule suffix is not /0 or /32).
- Red: A DB security group rule grants global access (the CIDR rule suffix is /0).

Recommended Action

Review your security group rules and restrict access to authorized IP addresses or IP ranges. To edit a security group, use the AuthorizeDBSecurityGroupIngress API or the AWS Management Console. For more information, see Working with DB Security Groups.

Additional Resources

- Amazon RDS Security Groups
- Classless Inter-Domain Routing
- List of TCP and UDP port numbers

Report columns

- Status
- Region
- RDS Security Group Name
- Ingress Rule
- Reason

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

**Alert Criteria**

Yellow: An MX resource record set doesn’t have a TXT or SPF resource record that contains a valid SPF value.

**Recommended Action**

For each MX resource record set, create a TXT resource record set that contains a valid SPF value. For more information, see [Sender Policy Framework: SPF Record Syntax](https://docs.aws.amazon.com/route53/latest/developerguide/sender-policy-framework.html) and [Creating Resource Record Sets By Using the Amazon Route 53 Console](https://docs.aws.amazon.com/route53/latest/developerguide/resource-record-sets.html).

**Additional Resources**

- [Sender Policy Framework](https://docs.aws.amazon.com/route53/latest/developerguide/sender-policy-framework.html)
- [MX record](https://docs.aws.amazon.com/route53/latest/developerguide/resource-record-sets.html)

**Report columns**

- Hosted Zone Name
- Hosted Zone ID
- Resource Record Set Name
- Status

---

**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

**Alert Criteria**

- Yellow: The bucket ACL allows List access for **Everyone** or **Any Authenticated AWS User**.
- Yellow: A bucket policy allows any kind of open access.
- Yellow: Bucket policy has statements that grant public access. The **Block public and cross-account access to buckets that have public policies** setting is turned on and has restricted access to only authorized users of that account until public statements are removed.
- Yellow: Trusted Advisor does not have permission to check the policy, or the policy could not be evaluated for other reasons.
- Red: The bucket ACL allows upload and delete access for **Everyone** or **Any Authenticated AWS User**.

**Recommended Action**

If a bucket allows open access, determine if open access is truly needed. If not, update the bucket permissions to restrict access to the owner or specific users. Use **Amazon S3 Block Public Access**.
to control the settings that allow public access to your data. See Setting Bucket and Object Access Permissions.

Additional Resources

Managing Access Permissions to Your Amazon S3 Resources

Report columns

- Status
- Region Name
- Region API Parameter
- Bucket Name
- ACL Allows List
- ACL Allows Upload/Delete
- Policy Allows Access

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

Alert Criteria

- Yellow: CloudTrail reports log delivery errors for a trail.
- Red: A trail has not been created for a Region, or logging is turned off for a trail.

Recommended Action

To create a trail and start logging from the console, go to the AWS CloudTrail console.

To start logging, see Stopping and Starting Logging for a Trail.

If you receive log delivery errors, check to make sure that the bucket exists and that the necessary policy is attached to the bucket. See Amazon S3 Bucket Policy.

Additional Resources

- AWS CloudTrail User Guide
- Supported Regions
- Supported Services

Report columns

- Status
- Region
- Trail Name
- Logging Status
- Bucket Name
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. Currently, you can’t exclude resources from this check.

Published Lambda function versions are immutable, which means they can be invoked but not updated. Only the $LATEST version for a Lambda function can be updated. For more information, see Lambda function versions.

Check ID
L4df82Q4C5

Alert Criteria

- Red: The function is running on a runtime that is already deprecated.
- Yellow: The function is running on a runtime that will be deprecated within 120 days.

Recommended Action

If you have functions that are running on a runtime that is approaching deprecation, you should prepare for migration to a supported runtime. For more information, see Runtime support policy.

We recommend that you delete earlier function versions that you’re no longer using.

Additional Resources

Lambda runtimes

Report columns

- Status
- Region
- Function ARN
- Runtime
- Days to Deprecation
- Deprecation Date
- Average Daily Invokes
- Last Updated Time

AWS Well-Architected high risk issues for security

Description

Checks for high risk issues (HRIs) for your workloads in the security pillar. This check is based on your AWS-Well Architected reviews. Your check results depend on whether you completed the workload evaluation with AWS Well-Architected.

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. Currently, you can’t exclude resources from this check.
Check ID

Wxdfp4B1L3

Alert Criteria

- Red: At least one active high risk issue was identified in the security pillar for AWS Well-Architected.
- Green: No active high risk issues were detected in the security pillar for AWS Well-Architected.

Recommended Action

AWS Well-Architected detected high risk issues during your workload evaluation. These issues present opportunities to reduce risk and save money. Sign in to the AWS Well-Architected tool to review your answers and take action to resolve your active issues.

Report columns

- Status
- Region
- Workload ARN
- Workload Name
- Reviewer Name
- Workload Type
- Workload Started Date
- Workload Last Modified Date
- Number of identified HRIs for Security
- Number of HRIs resolved for Security
- Number of questions for Security
- Total number of questions in Security pillar
- Last Updated Time

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

Alert Criteria

- Red: A custom SSL certificate is expired.
- Yellow: A custom SSL certificate expires in the next seven days.
- Yellow: A custom SSL certificate was encrypted by using the SHA-1 hashing algorithm.
- Yellow: One or more of the alternate domain names in the distribution don't appear either in the Common Name field or the Subject Alternative Names field of the custom SSL certificate.

**Recommended Action**

Renew an expired certificate or a certificate that is about to expire.

Replace a certificate that was encrypted by using the SHA-1 hashing algorithm with a certificate that is encrypted by using the SHA-256 hashing algorithm.

Replace the certificate with a certificate that contains the applicable values in the Common Name or Subject Alternative Domain Names fields.

**Additional Resources**

**Using an HTTPS Connection to Access Your Objects**

**Report columns**

- Status
- Distribution ID
- Distribution Domain Name
- Certificate Name
- Reason

**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.

Certificates that were encrypted by using the SHA-1 hashing algorithm are being deprecated by web browsers such as Chrome and Firefox. Depending on the number of SSL certificates that you have associated with your CloudFront distributions, this check might add a few cents per month to your bill with your web hosting provider, for example, AWS if you're using Amazon EC2 or Elastic Load Balancing as the origin for your CloudFront distribution. This check does not validate your origin certificate chain or certificate authorities. You can check these in your CloudFront configuration.

**Check ID**

N430c450f2

**Alert Criteria**

- Red: An SSL certificate on your origin has expired or is missing.
- Yellow: An SSL certificate on your origin expires in the next thirty days.
- Yellow: An SSL certificate on your origin was encrypted by using the SHA-1 hashing algorithm.
- Yellow: An SSL certificate on your origin can't be located. The connection might have failed due to timeout, or other HTTPS connection problems.

**Recommended Action**

Renew the certificate on your origin if it has expired or is about to expire.

Add a certificate if one does not exist.

Replace a certificate that was encrypted by using the SHA-1 hashing algorithm with a certificate that is encrypted by using the SHA-256 hashing algorithm.
Additional Resources

Using Alternate Domain Names and HTTPS

Report columns
• Status
• Distribution ID
• Distribution Domain Name
• Origin
• Reason

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

Alert Criteria
• Yellow: A load balancer has no listener that uses a secure protocol (HTTPS or SSL).
• Yellow: A load balancer listener uses an outdated predefined SSL security policy.
• Yellow: A load balancer listener uses a cipher or protocol that is not recommended.
• Red: A load balancer listener uses an insecure cipher or protocol.

Recommended Action
If the traffic to your load balancer must be secure, use either the HTTPS or the SSL protocol for the front-end connection.

Upgrade your load balancer to the latest version of the predefined SSL security policy.

Use only the recommended ciphers and protocols.

For more information, see Listener Configurations for Elastic Load Balancing.

Additional Resources
• Listener Configurations Quick Reference
• Update SSL Negotiation Configuration of Your Load Balancer
• SSL Negotiation Configurations for Elastic Load Balancing
• SSL Security Policy Table

Report columns
• Status
• Region
• Load Balancer Name
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
xSqX82fQ0u

Alert Criteria
- Yellow: The inbound rules of an Amazon VPC security group associated with a load balancer allow access to ports that are not defined in the load balancer's listener configuration.
- Red: A security group associated with a load balancer does not exist.

Recommended Action
Configure the security group rules to restrict access to only those ports and protocols that are defined in the load balancer listener configuration, plus the ICMP protocol to support Path MTU Discovery. See Listeners for Your Classic Load Balancer and Security Groups for Load Balancers in a VPC.

If a security group is missing, apply a new security group to the load balancer. Create security group rules that restrict access to only those ports and protocols that are defined in the load balancer listener configuration. See Security Groups for Load Balancers in a VPC.

Additional Resources
- Elastic Load Balancing User Guide
- Configure Your Classic Load Balancer

Report columns
- Status
- Region
- Load Balancer Name
- Security Group IDs
- Reason

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.

If a deadline is shown for an access key, AWS may suspend your AWS account if the unauthorized usage is not stopped by that date. If you believe an alert is in error, contact AWS Support.

The information displayed in Trusted Advisor might not reflect the most recent state of your account. No exposed access keys are marked as resolved until all exposed access keys on the account have been resolved. This data synchronization can take up to one week.

**Check ID**

12Fnkp18Y5

**Alert Criteria**

- **Red: Potentially compromised** – AWS has identified an access key ID and corresponding secret access key that have been exposed on the Internet and may have been compromised (used).
- **Red: Exposed** – AWS has identified an access key ID and corresponding secret access key that have been exposed on the Internet.
- **Red: Suspected** - Irregular Amazon EC2 usage indicates that an access key may have been compromised, but it has not been identified as exposed on the Internet.

**Recommended Action**

Delete the affected access key as soon as possible. If the key is associated with an IAM user, see Managing Access Keys for IAM Users.

Check your account for unauthorized usage. Sign in to the AWS Management Console and check each service console for suspicious resources. Pay special attention to running Amazon EC2 instances, Spot Instance requests, access keys, and IAM users. You can also check overall usage on the Billing and Cost Management console.

**Additional Resources**

- Best Practices for Managing AWS Access Keys
- AWS Security Audit Guidelines

**Report columns**

- Access Key ID
- User Name (IAM or Root)
- Fraud Type
- Case ID
- Time Updated
- Location
- Deadline
- Usage (USD per Day)

**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.

Because the regeneration frequency of a credential report is restricted, refreshing this check might not reflect recent changes. For more information, see Getting Credential Reports for Your AWS account.

In order to create and rotate access keys, a user must have the appropriate permissions. For more information, see Allow Users to Manage Their Own Passwords, Access Keys, and SSH Keys.

**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. Currently, you can’t exclude resources from this check.

**Check ID**
DqdJqYeRm5

**Alert Criteria**
- Green: The access key is active and has been rotated in the last 90 days.
- Yellow: The access key is active and has been rotated in the last 2 years, but more than 90 days ago.
- Red: The access key is active and has not been rotated in the last 2 years.

**Recommended Action**
Rotate access keys on a regular basis. See Rotating Access Keys and Managing Access Keys for IAM Users.

**Additional Resources**
- IAM Best Practices
- How to rotate access keys for IAM users

**Report columns**
- Status
- IAM user
- Access Key
- Key Last Rotated
- Reason

**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**
Yw2K9puPzl
Alert Criteria

- Yellow: A password policy is enabled, but at least one content requirement is not enabled.
- Red: No password policy is enabled.

Recommended Action

If some content requirements are not enabled, consider enabling them. If no password policy is enabled, create and configure one. See Setting an Account Password Policy for IAM Users.

Additional Resources

Managing Passwords

Report columns

- Password Policy
- Uppercase
- Lowercase
- Number
- Non-alphanumeric

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. You can ignore the alert if you are following best practice of centralizing identities and configuring users in an external identity provider or AWS IAM Identity Center (successor to AWS Single Sign-On).

Check ID

zXCKfM1nI3

Alert Criteria

Yellow: No IAM users have been created for this account.

Recommended Action

Create an IAM user or use AWS IAM Identity Center (successor to AWS Single Sign-On) to create additional users whose permissions are limited to perform specific tasks in your AWS environment.

Additional Resources

- What is AWS IAM Identity Center (successor to AWS Single Sign-On)?
- What Is IAM?

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
Alert Criteria

Red: MFA is not enabled on the root account.

Recommended Action

Log in to your root account and activate an MFA device. See Checking MFA Status and Setting Up an MFA Device.

Additional Resources

Using Multi-Factor Authentication (MFA) Devices with AWS

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

Alert Criteria

• Green: Access to port 80, 25, 443, or 465 is unrestricted.
• Red: Access to port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432, or 5500 is unrestricted.
• Yellow: Access to any other port is unrestricted.

Recommended Action

Restrict access to only those IP addresses that require it. To restrict access to a specific IP address, set the suffix to /32 (for example, 192.0.2.10/32). Be sure to delete overly permissive rules after creating rules that are more restrictive.

Additional Resources

• Amazon EC2 Security Groups
  - List of TCP and UDP port numbers
  - Classless Inter-Domain Routing

Report columns

• Status
• Region
• Security Group Name
• Security Group ID
• Protocol
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

Alert Criteria
Red: A security group rule has a source IP address with a /0 suffix for ports other than 25, 80, or 443.

Recommended Action
Restrict access to only those IP addresses that require it. To restrict access to a specific IP address, set the suffix to /32 (for example, 192.0.2.10/32). Be sure to delete overly permissive rules after creating rules that are more restrictive.

Additional Resources
- Amazon EC2 Security Groups
- Classless Inter-Domain Routing

Report columns
- Status
- Region
- Security Group Name
- Security Group ID
- Protocol
- From Port
- To Port
- IP Range

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

Check names
- Amazon Aurora DB Instance Accessibility (p. 117)
- Amazon Comprehend Endpoint Access Risk (p. 118)
- Amazon EBS Snapshots (p. 118)
- Amazon EC2 Availability Zone Balance (p. 119)
- Amazon RDS Backups (p. 120)
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
xuy7H1avtl

Alert Criteria
Yellow: The instances in an Aurora DB cluster have different accessibility (a mix of public and private).

Recommended Action
Modify the Publicly Accessible setting of the instances in the DB cluster so that they are all either public or private. For details, see the instructions for MySQL instances at Modifying a DB Instance Running the MySQL Database Engine.

Additional Resources
Fault Tolerance for an Aurora DB Cluster

Report columns
- Status
- Region
- Cluster
- Public DB Instances
- Private DB Instances
- Reason
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

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. Currently, you can’t exclude resources from this check.

Check ID

Cm24dfaM13

Alert Criteria

Red: The customer managed key is disabled or the key policy was changed to alter the allowed permissions for Amazon Comprehend access.

Recommended Action

If the customer managed key was disabled, we recommend that you enable it. For more information, see Enabling keys. If the key policy was altered and you want to keep using the endpoint, we recommend that you update the AWS KMS key policy. For more information, see Changing a key policy.

Additional Resources

AWS KMS Key Encryption Permissions

Report columns

- Status
- Region
- Endpoint ARN
- Model ARN
- KMS KeyId
- Last Updated Time

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

Alert Criteria

- Yellow: The most recent volume snapshot is between 7 and 30 days old.
- Red: The most recent volume snapshot is more than 30 days old.
- Red: The volume does not have a snapshot.
Recommended Action

Create weekly or monthly snapshots of your volumes. For more information, see Creating an Amazon EBS Snapshot.

Additional Resources

Amazon Elastic Block Store (Amazon EBS)

Report columns

- Status
- Region
- Volume ID
- Volume Name
- Snapshot ID
- Snapshot Name
- Snapshot Age
- Volume Attachment
- Reason

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

Alert Criteria

- Yellow: The Region has instances in multiple zones, but the distribution is uneven (the difference between the highest and lowest instance counts in utilized Availability Zones is greater than 20%).
- Red: The Region has instances only in a single Availability Zone.

Recommended Action

Balance your Amazon EC2 instances evenly across multiple Availability Zones. You can do this by launching instances manually or by using Auto Scaling to do it automatically. For more information, see Launch Your Instance and Load Balance Your Auto Scaling Group.

Additional Resources

Amazon EC2 Auto Scaling User Guide

Report columns

- Status
- Region
- Zone a Instances
- Zone b Instances
- Zone c Instances
- Zone e Instances
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

Alert Criteria

Red: A DB instance has the backup retention period set to 0 days.

Recommended Action

Set the retention period for the automated DB instance backup to 1 to 35 days as appropriate to the requirements of your application. See Working With Automated Backups.

Additional Resources

Getting Started with Amazon RDS

Report columns

- Status
- Region/AZ
- DB Instance
- VPC ID
- Backup Retention Period

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

Alert Criteria

Yellow: A DB instance is deployed in a single Availability Zone.

Recommended Action

If your application requires high availability, modify your DB instance to enable Multi-AZ deployment. See High Availability (Multi-AZ).
Additional Resources

Regions and Availability Zones

Report columns
- Status
- Region/AZ
- DB Instance
- VPC ID
- Multi-AZ

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

Alert Criteria
Yellow: A resource record set is associated with a health check that has been deleted.

Recommended Action
Create a new health check and associate it with the resource record set. See Creating, Updating, and Deleting Health Checks and Adding Health Checks to Resource Record Sets.

Additional Resources
- Amazon Route 53 Health Checks and DNS Failover
- How Health Checks Work in Simple Amazon Route 53 Configurations

Report columns
- Hosted Zone Name
- Hosted Zone ID
- Resource Record Set Name
- Resource Record Set Type
- Resource Record Set Identifier

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

Alert Criteria

- Yellow: A primary failover resource record set does not have a corresponding secondary resource record set.
- Yellow: A secondary failover resource record set does not have a corresponding primary resource record set.
- Yellow: Primary and secondary resource record sets that have the same name are associated with the same health check.

Recommended Action

If a failover resource set is missing, create the corresponding resource record set. See Creating Failover Resource Record Sets.

If your resource record sets are associated with the same health check, create separate health checks for each one. See Creating, Updating, and Deleting Health Checks.

Additional Resources

Amazon Route 53 Health Checks and DNS Failover

Report columns

- Hosted Zone Name
- Hosted Zone ID
- Resource Record Set Name
- Resource Record Set Type
- Reason

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

Alert Criteria

- Yellow: A resource record set whose routing policy is Failover has a TTL greater than 60 seconds.
- Yellow: A resource record set with an associated health check has a TTL greater than 60 seconds.

Recommended Action

Enter a TTL value of 60 seconds for the listed resource record sets. For more information, see Working with Resource Record Sets.

Additional Resources

Amazon Route 53 Health Checks and DNS Failover

Report columns

- Status
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

Alert Criteria

Yellow: A hosted zone for which the registrar for your domain does not use all four of the Route 53 name servers in the delegation set.

Recommended Action

Add or update name server records with your registrar or with the current DNS service for your domain to include all four of the name servers in your Route 53 delegation set. To find these values, see Getting the Name Servers for a Hosted Zone. For information about adding or updating name server records, see Creating and Migrating Domains and Subdomains to Amazon Route 53.

Additional Resources

- Working with Hosted Zones

Report columns

- Hosted Zone Name
- Hosted Zone ID
- Number of Name Server Delegations Used

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**

BueAdJ7NzP

**Alert Criteria**

- **Yellow**: The bucket does not have server access logging enabled.
- **Yellow**: The target bucket permissions do not include the root account, so Trusted Advisor cannot check it.
- **Red**: The target bucket does not exist.
- **Red**: The target bucket and the source bucket have different owners.
- **Red**: The log deliverer does not have write permissions for the target bucket.

**Recommended Action**

Enable bucket logging for most buckets. See [Enabling Logging Using the Console](#) and [Enabling Logging Programmatically](#).

If the target bucket permissions do not include the root account and you want Trusted Advisor to check the logging status, add the root account as a grantee. See [Editing Bucket Permissions](#).

If the target bucket does not exist, select an existing bucket as a target or create a new one and select it. See [Managing Bucket Logging](#).

If the target and source have different owners, change the target bucket to one that has the same owner as the source bucket. See [Managing Bucket Logging](#).

If the log deliverer does not have write permissions for the target (write not enabled), grant Upload/Delete permissions to the Log Delivery group. See [Editing Bucket Permissions](#).

**Additional Resources**

- [Working with Buckets](#)
- [Server Access Logging](#)
- [Server Access Log Format](#)
- [Deleting Log Files](#)

**Report columns**

- Status
- Region
- Bucket Name
- Target Name
- Target Exists
- Same Owner
- Write Enabled
- Reason

**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

**Alert Criteria**

- Green: Versioning is enabled for the bucket.
- Yellow: Versioning is not enabled for the bucket.
- Yellow: Versioning is suspended for the bucket.

**Recommended Action**

Enable bucket versioning on most buckets to prevent accidental deletion or overwriting. See Using Versioning and Enabling Versioning Programatically.

If bucket versioning is suspended, consider re-enabling versioning. For information on working with objects in a versioning-suspended bucket, see Managing Objects in a Versioning-Suspended Bucket.

When versioning is enabled or suspended, you can define lifecycle configuration rules to mark certain object versions as expired or to permanently remove unneeded object versions. For more information, see Object Lifecycle Management.

MFA Delete requires additional authentication when the versioning status of the bucket is changed or when versions of an object are deleted. It requires the user to enter credentials and a code from an approved authentication device. For more information, see MFA Delete.

**Additional Resources**

Working with Buckets

**Report columns**

- Status
- Region
- Bucket Name
- Versioning
- MFA Delete Enabled

**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**

CLOG40CDO8
Alert Criteria

- Yellow: An Auto Scaling group has an associated load balancer, but the Elastic Load Balancing health check is not enabled.
- Yellow: An Auto Scaling group does not have an associated load balancer, but the Elastic Load Balancing health check is enabled.

Recommended Action

If the Auto Scaling group has an associated load balancer, but the Elastic Load Balancing health check is not enabled, see Add an Elastic Load Balancing Health Check to your Auto Scaling Group.

If the Elastic Load Balancing health check is enabled, but no load balancer is associated with the Auto Scaling group, see Set Up an Auto-Scaled and Load-Balanced Application.

Additional Resources

Amazon EC2 Auto Scaling User Guide

Report columns

- Status
- Region
- Auto Scaling Group Name
- Load Balancer Associated
- Health Check

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

Alert Criteria

- Red: An Auto Scaling group is associated with a deleted load balancer.
- Red: A launch configuration is associated with a deleted Amazon Machine Image (AMI).

Recommended Action

If the load balancer has been deleted, either create a new load balancer and then create a new Auto Scaling group with the new load balancer, or create a new Auto Scaling group without the load balancer. For information about creating a new Auto Scaling group with a new load balancer, see Set Up an Auto-Scaled and Load-Balanced Application. For information about creating a new Auto Scaling group without a load balancer, see Create Auto Scaling Group in Getting Started With Auto Scaling Using the Console.

If the AMI has been deleted, create a new launch configuration using a valid AMI and associate it with an Auto Scaling group. See Create Launch Configuration in Getting Started With Auto Scaling Using the Console.
Additional Resources

- Troubleshooting Auto Scaling: Amazon EC2 AMIs
- Troubleshooting Auto Scaling: Load Balancer Configuration
- Amazon EC2 Auto Scaling User Guide

Report columns

- Status
- Region
- Auto Scaling Group Name
- Launch Type
- Resource Type
- Resource Name

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

Alert Criteria

Yellow: The AWS Region has only one AWS Direct Connect connection.

Recommended Action

Configure an additional Direct Connect connection in this AWS Region to protect against device unavailability. For more information, see Configure Redundant Connections with AWS Direct Connect. To protect against site unavailability and add location redundancy, configure the additional Direct Connect connection to a different Direct Connect location.

Additional Resources

- Getting Started with AWS Direct Connect
- AWS Direct Connect FAQs

Report columns

- Status
- Region
- Time Stamp
- Location
- Connection ID

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

Alert Criteria
Yellow: The Direct Connect connections in the AWS Region are not configured to different locations.

Recommended Action
Configure a Direct Connect connection that uses a different Direct Connect location to protect against location unavailability. For more information, see Getting Started with AWS Direct Connect.

Additional Resources
• Getting Started with AWS Direct Connect
• AWS Direct Connect FAQs

Report columns
• Status
• Region
• Time Stamp
• Location
• Connection Details

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

Alert Criteria
Yellow: A virtual private gateway has less than two virtual interfaces, or the interfaces are not configured to multiple Direct Connect connections.

Recommended Action
Configure at least two virtual interfaces that are configured to two Direct Connect connections to protect against device or location unavailability. See Create a Virtual Interface.

Additional Resources
• Getting Started with AWS Direct Connect
• AWS Direct Connect FAQs
• Working With AWS Direct Connect Virtual Interfaces

Report columns
  • Status
  • Region
  • Time Stamp
  • Gateway ID
  • Location for VIF
  • Connection ID for VIF

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. Currently, you can’t exclude resources from this check.

Check ID
  L4dfs2Q4C6

Alert Criteria
  Yellow: A VPC-enabled Lambda function connected to subnets in a single Availability Zone.

Recommended Action
  When configuring functions for access to your VPC, choose subnets in multiple Availability Zones to ensure high availability.

Additional Resources
  • Configuring a Lambda function to access resources in a VPC
  • Resilience in AWS Lambda

Report columns
  • Status
  • Region
  • Function ARN
  • VPC ID
  • Average daily Invokes
  • Last Updated Time

AWS Well-Architected high risk issues for reliability

Description
  Checks for high risk issues (HRIs) for your workloads in the reliability pillar. This check is based on your AWS-Well Architected reviews. Your check results depend on whether you completed the workload evaluation with AWS Well-Architected.
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. Currently, you can’t exclude resources from this check.

Check ID
Wxdfp4B1L4

Alert Criteria
- Red: At least one active high risk issue was identified in the reliability pillar for AWS Well-Architected.
- Green: No active high risk issues were detected in the reliability pillar for AWS Well-Architected.

Recommended Action
AWS Well-Architected detected high risk issues during your workload evaluation. These issues present opportunities to reduce risk and save money. Sign in to the AWS Well-Architected tool to review your answers and take action to resolve your active issues.

Report columns
- Status
- Region
- Workload ARN
- Workload Name
- Reviewer Name
- Workload Type
- Workload Started Date
- Workload Last Modified Date
- Number of identified HRIs for Reliability
- Number of HRIs resolved for Reliability
- Number of questions answered for Reliability
- Total number of questions in Reliability pillar
- Last Updated Time

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
7qGx6Kluw

Alert Criteria
Yellow: Connection draining is not enabled for a load balancer.

Recommended Action
Enable connection draining for the load balancer. For more information, see Connection Draining and Enable or Disable Connection Draining for Your Load Balancer.
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

Alert Criteria

Yellow: Cross-zone load balancing is not enabled for a load balancer.

Recommended Action

Confirm that the Amazon EC2 instances registered with the load balancer are launched in multiple
Availability Zones, and then enable cross-zone load balancing for the load balancer. For more
information, see Availability Zones and Regions and Enable or Disable Cross-Zone Load Balancing for
Your Load Balancer.

Additional Resources

- Request Routing
- Elastic Load Balancing Concepts

Report columns

- Status
- Region
- Load Balancer Name
- Reason

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
Alert Criteria

- Yellow: A load balancer is enabled for a single Availability Zone.
- Yellow: A load balancer is enabled for an Availability Zone that has no active instances.
- Yellow: The Amazon EC2 instances that are registered with a load balancer are unevenly distributed across Availability Zones. (The difference between the highest and lowest instance counts in utilized Availability Zones is more than 1, and the difference is more than 20% of the highest count.)

Recommended Action

Ensure that your load balancer points to active and healthy instances in at least two Availability Zones. For more information, see Add Availability Zone.

If your load balancer is configured for an Availability Zone with no healthy instances, or if there is an imbalance of instances across the Availability Zones, determine if all the Availability Zones are necessary. Omit any unnecessary Availability Zones and ensure there is a balanced distribution of instances across the remaining Availability Zones. For more information, see Remove Availability Zone.

Additional Resources

- Availability Zones and Regions
- Managing Load Balancers
- Best Practices in Evaluating Elastic Load Balancing

Report columns

- Status
- Region
- Load Balancer Name
- # of Zones
- Zone a Instances
- Zone b Instances
- Zone c Instances
- Zone d Instances
- Zone e Instances
- Zone f Instances
- Reason

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

Alert Criteria

- Yellow: A VPN has one active tunnel (this is normal for some hardware).
Service limits

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

All checks in this category have the following descriptions:

**Alert Criteria**
- Yellow: 80% of limit reached.
- Red: 100% of limit reached.
- Blue: Trusted Advisor was unable to retrieve utilization or limits in one or more AWS Regions.

**Recommended Action**
- If you expect to exceed a service limit, request an increase directly from the Service Quotas console.
- If Service Quotas doesn't support your service yet, you can create an open a support case in Support Center.

**Report columns**
- Status
- Service
- Region
- Limit Amount
- Current Usage

**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. 135)
• Auto Scaling Launch Configurations (p. 135)
• CloudFormation Stacks (p. 135)
• DynamoDB Read Capacity (p. 135)
• DynamoDB Write Capacity (p. 136)
• EBS Active Snapshots (p. 136)
• EBS Cold HDD (sc1) Volume Storage (p. 136)
• EBS General Purpose SSD (gp2) Volume Storage (p. 136)
• EBS General Purpose SSD (gp3) Volume Storage (p. 137)
• EBS Magnetic (standard) Volume Storage (p. 137)
• EBS Provisioned IOPS (SSD) Volume Aggregate IOPS (p. 137)
• EBS Provisioned IOPS SSD (io1) Volume Storage (p. 137)
• EBS Provisioned IOPS SSD (io2) Volume Storage (p. 138)
• EBS Throughput Optimized HDD (st1) Volume Storage (p. 138)
• EC2 On-Demand Instances (p. 138)
• EC2 Reserved Instance Leases (p. 138)
• EC2-Classic Elastic IP Addresses (p. 139)
• EC2-VPC Elastic IP Address (p. 139)
• ELB Application Load Balancers (p. 139)
• ELB Classic Load Balancers (p. 139)
• ELB Network Load Balancers (p. 139)
• IAM Group (p. 140)
• IAM Instance Profiles (p. 140)
• IAM Policies (p. 140)
• IAM Roles (p. 140)
• IAM Server Certificates (p. 141)
• IAM Users (p. 141)
• Kinesis Shards per Region (p. 141)
• RDS Cluster Parameter Groups (p. 141)
• RDS Cluster Roles (p. 141)
• RDS Clusters (p. 142)
• RDS DB Instances (p. 142)
• RDS DB Manual Snapshots (p. 142)
• RDS DB Parameter Groups (p. 142)
• RDS DB Security Groups (p. 143)
• RDS Event Subscriptions (p. 143)
• RDS Max Auths per Security Group (p. 143)
• RDS Option Groups (p. 143)
• RDS Read Replicas per Master (p. 143)
• RDS Reserved Instances (p. 144)
• RDS Subnet Groups (p. 144)
• RDS Subnets per Subnet Group (p. 144)
• RDS Total Storage Quota (p. 144)
• Route 53 Hosted Zones (p. 145)
Service limits

- Route 53 Max Health Checks (p. 145)
- Route 53 Reusable Delegation Sets (p. 145)
- Route 53 Traffic Policies (p. 145)
- Route 53 Traffic Policy Instances (p. 145)
- SES Daily Sending Quota (p. 146)
- VPC (p. 146)
- VPC Internet Gateways (p. 146)

Auto Scaling Groups

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

Check ID
fW7HH0l7J9

Additional Resources
Auto Scaling quotas

Auto Scaling Launch Configurations

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

Check ID
aW7HH0l7J9

Additional Resources
Auto Scaling quotas

CloudFormation Stacks

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

Check ID
gW7HH0l7J9

Additional Resources
AWS CloudFormation quotas

DynamoDB Read Capacity

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

Additional Resources
DynamoDB quotas

EBS Active Snapshots

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

Check ID
eI7KK0l7J9

Additional Resources
Amazon EBS limits

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

Additional Resources
Amazon EBS limits

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
Additional Resources

Amazon EBS limits

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

Additional Resources

Amazon EBS limits

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

Additional Resources

Amazon EBS limits

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

Additional Resources

Amazon EBS limits

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
Additional Resources

Amazon EBS limits

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

Additional Resources
Amazon EBS limits

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

Additional Resources
Amazon EBS limits

EC2 On-Demand Instances

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

Check ID
0Xc6LMYG8P

Additional Resources
Amazon EC2 quotas

EC2 Reserved Instance Leases

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

Check ID
iH7PP017J9

Additional Resources
Amazon EC2 quotas
EC2-Classic Elastic IP Addresses

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

Check ID
aW9HH0l8J6

Additional Resources
Amazon EC2 quotas

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

Additional Resources
VPC Elastic IP quotas

ELB Application Load Balancers

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

Check ID
EM8b3yLRTr

Additional Resources
Elastic Load Balancing quotas

ELB Classic Load Balancers

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

Check ID
iK700017J9

Additional Resources
Elastic Load Balancing quotas

ELB Network Load Balancers

Description
Checks for usage that is more than 80% of the ELB Network Load Balancers quota.
Check ID
8wIqYSt25K
Additional Resources
Elastic Load Balancing quotas

IAM Group
Description
Checks for usage that is more than 80% of the IAM group quota.
Check ID
sU7XX017J9
Additional Resources
IAM quotas

IAM Instance Profiles
Description
Checks for usage that is more than 80% of the IAM instance profiles quota.
Check ID
n07SS017J9
Additional Resources
IAM quotas

IAM Policies
Description
Checks for usage that is more than 80% of the IAM policies quota.
Check ID
pR7UU017J9
Additional Resources
IAM quotas

IAM Roles
Description
Checks for usage that is more than 80% of the IAM roles quota.
Check ID
oQ7TT017J9
Additional Resources
IAM quotas
IAM Server Certificates

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

**Check ID**
rt7WW017J9

**Additional Resources**
IAM quotas

IAM Users

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

**Check ID**
qS7VV017J9

**Additional Resources**
IAM quotas

Kinesis Shards per Region

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

**Check ID**
bW7HH017J9

**Additional Resources**
Kinesis quotas

RDS Cluster Parameter Groups

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

**Check ID**
jt1IMO3g2M

**Additional Resources**
Amazon RDS quotas

RDS Cluster Roles

**Description**
Checks for usage that is more than 80% of the RDS cluster roles quota.
Check ID
7fuccf1Mx7

Additional Resources
Amazon RDS quotas

RDS Clusters

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

Check ID
gjqMBn6pjz

Additional Resources
Amazon RDS quotas

RDS DB Instances

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

Check ID
XG0aXHpIEt

Additional Resources
Amazon RDS quotas

RDS DB Manual Snapshots

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

Check ID
dV84wpqRU5

Additional Resources
Amazon RDS quotas

RDS DB Parameter Groups

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

Check ID
jEECYg2YVU

Additional Resources
Amazon RDS quotas
RDS DB Security Groups

Description

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

Check ID
gf2An3W7w1

Additional Resources
Amazon RDS quotas

RDS Event Subscriptions

Description

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

Check ID
keAhfbH5yb

Additional Resources
Amazon RDS quotas

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

Additional Resources
Amazon RDS quotas

RDS Option Groups

Description

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

Check ID
3Njm0DJQ09

Additional Resources
Amazon RDS quotas

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
Additional Resources
Amazon RDS quotas

RDS Reserved Instances

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

Check ID
UUDvOa5r34
Additional Resources
Amazon RDS quotas

RDS Subnet Groups

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

Check ID
dYWbaXaaMM
Additional Resources
Amazon RDS quotas

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
Additional Resources
Amazon RDS quotas

RDS Total Storage Quota

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

Check ID
P1jhKWEmLa
Additional Resources
Amazon RDS quotas
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

Additional Resources
Route 53 quotas

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

Additional Resources
Route 53 quotas

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

Additional Resources
Route 53 quotas

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

Additional Resources
Route 53 quotas

Route 53 Traffic Policy Instances

Description
Checks for usage that is more than 80% of the Route 53 traffic policy instances quota per account.
AWS Support User Guide
Change log for AWS Trusted Advisor checks

Check ID
dx8afcdMr
Additional Resources
Route 53 quotas

SES Daily Sending Quota
Description
Checks for usage that is more than 80% of the Amazon SES daily sending quota.
Check ID
hJ7NN017J9
Additional Resources
Amazon SES quotas

VPC
Description
Checks for usage that is more than 80% of the VPC quota.
Check ID
jL7PP017J9
Additional Resources
VPC quotas

VPC Internet Gateways
Description
Checks for usage that is more than 80% of the VPC Internet gateways quota.
Check ID
kM7QQ017J9
Additional Resources
VPC quotas

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. 71).
Added Security Hub checks to Trusted Advisor

As of June 23, 2022, Trusted Advisor only supports Security Hub controls available through April 7, 2022. This release supports all controls in the AWS Foundational Security Best Practices security standard except for controls in the Category: Recover > Resilience. For more information, see Viewing AWS Security Hub controls in AWS Trusted Advisor (p. 57).

For a list of supported controls, see AWS Foundational Security Best Practices controls in the AWS Security Hub User Guide.

Added checks from AWS Compute Optimizer

Trusted Advisor added the following checks on May 4, 2022.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EBS over-provisioned volumes</td>
<td>Cost optimization</td>
<td>Cor6dfpM03</td>
</tr>
<tr>
<td>Amazon EBS under-provisioned volumes</td>
<td>Performance</td>
<td>Cor6dfpM04</td>
</tr>
<tr>
<td>AWS Lambda over-provisioned functions for memory size</td>
<td>Cost optimization</td>
<td>Cor6dfpM05</td>
</tr>
<tr>
<td>AWS Lambda under-provisioned functions for memory size</td>
<td>Performance</td>
<td>Cor6dfpM06</td>
</tr>
</tbody>
</table>

You must opt in your AWS account for Compute Optimizer so that these checks can receive data from your Lambda and Amazon EBS resources. For more information, see Opt in AWS Compute Optimizer for Trusted Advisor checks (p. 62).

Updates to the Exposed Access Keys check

Trusted Advisor updated the following check on April 25, 2022.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposed Access Keys</td>
<td>Security</td>
<td>12Fnkpl8Y5</td>
</tr>
</tbody>
</table>

Trusted Advisor now refreshes this check for you automatically. This check can't be refreshed manually from the Trusted Advisor console or the AWS Support API. If your application or code refreshes this check for your AWS account, we recommend that you update it to no longer refresh this check. Otherwise, you will receive the InvalidParameterValue error.

Any access keys that you excluded before this update will no longer be excluded and will appear as affected resources. You can't exclude access keys from your check results. For more information, see Exposed Access Keys (p. 111).

Note
If you created your AWS account after April 25, 2022, the check results for Exposed Access Keys initially shows the gray icon (:none) even for unexposed access keys. This means that Trusted Advisor hasn't identified any changes to the check.
If Trusted Advisor identifies a resource at risk, the status changes to the action recommended icon (⚠️). After you fix or delete the resource, the check result shows the check mark icon (✔️).

Updated checks for AWS Direct Connect

Trusted Advisor updated the following checks on March 29, 2022.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Direct Connect Connection Redundancy</td>
<td>Fault tolerance</td>
<td>0t121N1Ty3</td>
</tr>
<tr>
<td>AWS Direct Connect Location Redundancy</td>
<td>Fault tolerance</td>
<td>8M012Ph3U5</td>
</tr>
<tr>
<td>AWS Direct Connect Virtual Interface Redundancy</td>
<td>Fault tolerance</td>
<td>4g3Nt5M1Th</td>
</tr>
</tbody>
</table>

- The value for the **Region** column now shows the AWS Region code instead of the full name. For example, resources in US East (N. Virginia) will now have the `us-east-1` value.
- The value for the **Time Stamp** column now appears in the RFC 3339 format, such as `2022-03-30T01:02:27.000Z`.
- Resources that don’t have any detected problems will now appear in the check table. These resources will have a check mark icon (✔️) next to them.

Previously, only resources that Trusted Advisor recommended that you investigate appeared in the table. These resources have a warning icon (⚠️) next to them.

AWS Security Hub controls added to the AWS Trusted Advisor console

AWS Trusted Advisor added 111 Security Hub controls to the **Security** category on January 18, 2022.

You can view your findings for Security Hub controls from the AWS Foundational Security Best Practices security standard. This integration doesn't include controls that have the **Category: Recover > Resilience**.

For more information about this feature, see Viewing AWS Security Hub controls in AWS Trusted Advisor (p. 57).

New checks for Amazon EC2 and AWS Well-Architected

Trusted Advisor added the following checks on December 20, 2021.

- Amazon EC2 instances consolidation for Microsoft SQL Server
- Amazon EC2 instances over-provisioned for Microsoft SQL Server
- Amazon EC2 instances with Microsoft SQL Server end of support
- AWS Well-Architected high risk issues for cost optimization
- AWS Well-Architected high risk issues for performance
- AWS Well-Architected high risk issues for security
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.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon OpenSearch Service Reserved Instance Optimization</td>
<td>Cost optimization</td>
<td>7ujm6yhn5t</td>
</tr>
</tbody>
</table>

**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. 198).

Added checks for Amazon Elastic Block Store volume storage

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

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBS General Purpose SSD (gp3) Volume Storage</td>
<td>Service limits</td>
<td>dH7RR016J3</td>
</tr>
<tr>
<td>EBS Provisioned IOPS SSD (io2) Volume Storage</td>
<td>Service limits</td>
<td>gI7MM017J2</td>
</tr>
</tbody>
</table>

Added checks for AWS Lambda

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

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Lambda Functions with Excessive Timeouts</td>
<td>Cost optimization</td>
<td>L4dfs2Q3C3</td>
</tr>
<tr>
<td>AWS Lambda Functions with High Error Rates</td>
<td>Cost optimization</td>
<td>L4dfs2Q3C2</td>
</tr>
<tr>
<td>AWS Lambda Functions Using Deprecated Runtimes</td>
<td>Security</td>
<td>L4dfs2Q4C5</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Lambda VPC-enabled Functions without Multi-AZ Redundancy</td>
<td>Fault tolerance</td>
<td>L4dfs2Q4C6</td>
</tr>
</tbody>
</table>

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. 198).

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
<th>Updated CloudWatch metric for ServiceLimit</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBS Cold HDD (sc1) Volume Storage</td>
<td>Service limits</td>
<td>gH5CC0e3J9</td>
<td>Cold HDD (sc1) volume storage (TiB)</td>
</tr>
<tr>
<td>EBS General Purpose SSD (gp2) Volume Storage</td>
<td>Service limits</td>
<td>dH7RR016J9</td>
<td>General Purpose SSD (gp2) volume storage (TiB)</td>
</tr>
<tr>
<td>EBS Magnetic (standard) Volume Storage</td>
<td>Service limits</td>
<td>cG7HH017J9</td>
<td>Magnetic (standard) volume storage (TiB)</td>
</tr>
<tr>
<td>EBS Provisioned IOPS SSD (io1) Volume Storage</td>
<td>Service limits</td>
<td>gI7MM017J9</td>
<td>Provisioned IOPS (SSD) storage (TiB)</td>
</tr>
<tr>
<td>EBS Throughput Optimized HDD (st1) Volume Storage</td>
<td>Service limits</td>
<td>wH7DD013J9</td>
<td>Throughput Optimized HDD (st1) volume storage (TiB)</td>
</tr>
</tbody>
</table>

### Trusted Advisor check removal

**Note**

Trusted Advisor removed the following checks on November 18, 2020.
<table>
<thead>
<tr>
<th>Checks removed on November 18, 2020</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2Config Service for EC2 Windows Instances</td>
<td>Fault tolerance</td>
<td>V77iO1Bqz</td>
</tr>
<tr>
<td>ENA Driver Version for EC2 Windows Instances</td>
<td>Fault tolerance</td>
<td>TyfdMXG69d</td>
</tr>
<tr>
<td>NVMe Driver Version for EC2 Windows Instances</td>
<td>Fault tolerance</td>
<td>yHAGQJV9K5</td>
</tr>
<tr>
<td>PV Driver Version for EC2 Windows Instances</td>
<td>Fault tolerance</td>
<td>Wnwm9I5bG</td>
</tr>
<tr>
<td>EBS Active Volumes</td>
<td>Service limits</td>
<td>fH7L017J9</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Check category</th>
<th>Check ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Limits</td>
<td>Performance</td>
<td>eW7HH017J9</td>
</tr>
</tbody>
</table>
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. 152)
- Identity and access management for AWS Support (p. 153)
- Incident response (p. 184)
- Logging and monitoring in AWS Support and AWS Trusted Advisor (p. 185)
- Compliance validation for AWS Support (p. 185)
- Resilience in AWS Support (p. 186)
- Infrastructure security in AWS Support (p. 186)
- Configuration and vulnerability analysis in AWS Support (p. 186)

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. 153)
• Authenticating with identities (p. 154)
• Managing access using policies (p. 155)
• How AWS Support works with IAM (p. 157)
• AWS Support identity-based policy examples (p. 158)
• Using service-linked roles (p. 160)
• AWS managed policies for AWS Support and AWS Trusted Advisor (p. 164)
• Manage access for AWS Trusted Advisor (p. 177)
• Troubleshooting AWS Support identity and access (p. 183)

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. 183).

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 service users 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. 157).

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. 158).
Authenticating with identities

Authenticating 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 create an AWS account, you begin with one 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. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the AWS General Reference.

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 AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. 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. 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. 157)
- AWS Support IAM roles (p. 157)

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. 158).

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. 160).

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. 158)
- Using the AWS Support console (p. 159)
- Allow users to view their own permissions (p. 159)

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. 160)
- Using service-linked roles for Trusted Advisor (p. 161)

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. We use AWS KMS keys to encrypt sensitive fields. These fields are redacted in the API response and aren't visible to AWS Support agents.

**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. 161).

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
Using service-linked roles

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. 164).

### 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](p. 160).

### 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](p. 160) 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](p. 160).

### 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. 160).

For information about other services that support service-linked roles, see [AWS services that work with IAM](p. 160). 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.
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. 173).

- **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. 176).

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. 39).

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.

```json
{
    "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.

```json
{
   "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.

```json
{
   "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

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 policies for AWS Support (p. 165)
  - AWS managed policy: AWSSupportServiceRolePolicy (p. 165)
  - AWS Support updates to AWS managed policies (p. 165)
  - Permission changes for AWSSupportServiceRolePolicy (p. 170)
- AWS managed policies for AWS Trusted Advisor (p. 170)
  - AWS managed policy: AWSTrustedAdvisorPriorityFullAccess (p. 171)
  - AWS managed policy: AWSTrustedAdvisorPriorityReadOnlyAccess (p. 172)
  - AWS managed policy: AWSTrustedAdvisorServiceRolePolicy (p. 173)
  - AWS managed policy: AWSTrustedAdvisorReportingServiceRolePolicy (p. 176)
  - Trusted Advisor updates to AWS managed policies (p. 176)

AWS managed policies for AWS Support

AWS Support has the following managed policies.

Contents

- AWS managed policy: AWSSupportServiceRolePolicy (p. 165)
- AWS Support updates to AWS managed policies (p. 165)
- Permission changes for AWSSupportServiceRolePolicy (p. 170)

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. 160).

For a list of changes to the policy, see AWS Support updates to AWS managed policies (p. 165) and Permission changes for AWSSupportServiceRolePolicy (p. 170).

AWS Support updates to AWS managed policies

View details about updates to AWS managed policies for AWS Support 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. 214) page.

The following table describes important updates to the AWS Support managed policies since February 17, 2022.
## AWS Support

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| AWSSupportServiceRolePolicy (p. 165) – Update to an existing policy | Added 46 new permissions to the following services to perform actions that help troubleshoot customer issues related to billing, administrative, and technical support:  
  - Amazon Managed Streaming for Apache Kafka – To troubleshoot issues related to Amazon MSK.  
  - AWS DataSync – To troubleshoot issues related to DataSync.  
  - AWS Elastic Disaster Recovery – To troubleshoot replication and launch issues.  
  - Amazon GameSparks – To troubleshoot issues related to GameSparks.  
  - AWS IoT TwinMaker – To debug issues related to AWS IoT TwinMaker.  
  - AWS Lambda – To view the configuration of a function URL to troubleshooting issues.  
  - Amazon Lookout for Equipment – To troubleshoot issues related to Lookout for Equipment.  
  - Amazon Route 53 and Amazon Route 53 Resolver – To get resolver configurations so that AWS Support can check the DNS resolution behavior of a VPC. | August 17, 2022 |
| AWSSupportServiceRolePolicy (p. 165) – Update to an existing policy | Added new permissions to the following services to perform actions that help troubleshoot customer issues related to billing, administrative, and technical support:  
  - Amazon CloudWatch Logs – To help troubleshoot CloudWatch Logs related issues.  
  - Amazon Interactive Video Service – To help AWS Support check existing Amazon IVS resources for support | June 23, 2022 |
### AWS Support User Guide

### AWS managed policies

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>cases regarding fraud or compromised accounts.</td>
<td>• Amazon Inspector – To troubleshoot Amazon Inspector related issues.</td>
<td></td>
</tr>
<tr>
<td>Removed permissions for services, such as Amazon WorkLink. Amazon WorkLink was deprecated on April 19, 2022.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **AWSSupportServiceRolePolicy (p. 165)** – Update to an existing policy | Added 25 new permissions to the following services to perform actions that help troubleshoot customer issues related to billing, administrative, and technical support:  
  • AWS Amplify UI Builder – To troubleshoot issues related to component and theme generation.  
  • Amazon AppStream – To troubleshoot issues by retrieving resources for features that launched recently.  
  • AWS Backup – To troubleshoot issues related to backup jobs.  
  • AWS CloudFormation – To perform diagnostics on issues related to IAM, extension, and versioning.  
  • Amazon Kinesis – To troubleshoot issues related to Kinesis.  
  • AWS Transfer Family – To troubleshoot issues related to Transfer Family. | April 27, 2022     |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| AWSManagedPolicyName (p. 165) – Update to an existing policy | Added 54 new permissions to the following services to perform actions that help troubleshoot customer issues related to billing, administrative, and technical support:  
  - Amazon Elastic Compute Cloud  
  - To troubleshoot issues related to customer and AWS-managed prefixed lists.  
  - To troubleshoot issues related to Amazon VPC IP Address Manager (IPAM).  
  - AWS Network Manager – To troubleshoot issues related to Network Manager.  
  - Savings Plans – To get metadata about outstanding Savings Plan commitments.  
  - AWS Serverless Application Repository – To improve and support response actions as part of researching and resolving support cases.  
  - Amazon WorkSpaces Web – To debug and troubleshoot issues with WorkSpaces Web services. | March 14, 2022 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| **AWSSupportServiceRolePolicy (p. 165)** – Update to an existing policy | Added 74 new permissions to the following services to perform actions that help troubleshoot customer issues related to billing, administrative, and technical support:  
  - AWS Application Migration Service – To support agentless replication in the Application Migration Service.  
  - AWS CloudFormation – To perform diagnostics on IAM, extension, and versioning related issues.  
  - Amazon CloudWatch Logs – To validate resource policies.  
  - Amazon EC2 Recycle Bin – To get metadata about Recycle Bin retention rules.  
  - AWS Elastic Disaster Recovery – To troubleshoot replication and launch problems in customer accounts.  
  - Amazon FSx – To view the description of Amazon FSx snapshots.  
  - Amazon Lightsail – To view metadata and configurations details for Lightsail buckets.  
  - Amazon Macie – To view Macie configurations, such as classification jobs, custom data identifiers, regular expressions and findings.  
  - Amazon S3 – To gather metadata and configurations for Amazon S3 buckets.  
  - AWS Storage Gateway – To view metadata about customers' automatic tape creation policies.  
  - Elastic Load Balancing – To view the description of resource limits when using the Service Quotas console.  
  For more information, see [Permission changes for AWSSupportServiceRolePolicy (p. 170)](https://docs.aws.amazon.com/IAM/latest/UserGuide/permissions-managed-policies.html). | February 17, 2022 |
Permission changes for AWSSupportServiceRolePolicy

Most permissions added to AWSSupportServiceRolePolicy allow AWS Support to call an API operation with the same name. However, some API operations require permissions that have a different name.

The following table only lists the API operations that require permissions with a different name. This table describes these differences beginning on February 17, 2022.

<table>
<thead>
<tr>
<th>Date</th>
<th>API operation name</th>
<th>Required policy permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added permissions on February 17, 2022</td>
<td>s3.GetBucketAnalyticsConfiguration</td>
<td>s3:DescribeAnalyticsConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.ListBucketAnalyticsConfiguration</td>
<td>s3:ListAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketNotificationConfiguration</td>
<td>s3:GetBucketNotification</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketEncryption</td>
<td>s3:GetEncryptionConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketIntelligentTieringConfiguration</td>
<td>s3:GetIntelligentTieringConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.ListBucketIntelligentTieringConfiguration</td>
<td>s3:ListIntelligentTieringConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketInventoryConfiguration</td>
<td>s3:DescribeInventoryConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.ListBucketInventoryConfiguration</td>
<td>s3:listAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketLifecycleConfiguration</td>
<td>s3:getLifecycleConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketMetricsConfiguration</td>
<td>s3:GetMetricConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.ListBucketMetricsConfiguration</td>
<td>s3:listBucketMetricsConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.GetBucketReplication</td>
<td>s3:GetReplicationConfiguration</td>
</tr>
<tr>
<td></td>
<td>s3.HeadBucket</td>
<td>s3:ListBucket</td>
</tr>
<tr>
<td></td>
<td>s3.ListObjects</td>
<td>s3:listObjects</td>
</tr>
<tr>
<td></td>
<td>s3.ListBuckets</td>
<td>s3:listAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3.ListMultipartUploads</td>
<td>s3:ListBucketMultipartUploads</td>
</tr>
<tr>
<td></td>
<td>s3.ListObjectVersions</td>
<td>s3:ListBucketVersions</td>
</tr>
<tr>
<td></td>
<td>s3.ListParts</td>
<td>s3:ListMultipartUploadParts</td>
</tr>
</tbody>
</table>

AWS managed policies for AWS Trusted Advisor

Trusted Advisor has the following AWS managed policies.

Contents
- AWS managed policy: AWSTrustedAdvisorPriorityFullAccess (p. 171)
AWS managed policy: AWSTrustedAdvisorPriorityFullAccess

The AWSTrustedAdvisorPriorityFullAccess policy grants full access to Trusted Advisor Priority. This policy also enables the user to add Trusted Advisor as a trusted service with AWS Organizations and to specify the delegated administrator accounts for Trusted Advisor Priority.

Permissions details

In the first statement, the policy includes the following permissions for trustedadvisor:

- Describes your account and organization.
- Describes identified risks from Trusted Advisor Priority. The permissions allow you to download and update the risk status.
- Describes your configurations for Trusted Advisor Priority email notifications. The permissions allow you to configure the email notifications and disable them for your delegated administrators.
- Sets up Trusted Advisor so that your account can enable AWS Organizations.

In the second statement, the policy includes the following permissions for organizations:

- Describes your Trusted Advisor account and organization.
- Lists the AWS services that you enabled to use Organizations.

In the third statement, the policy includes the following permissions for organizations:

- Lists the delegated administrators for Trusted Advisor Priority.
- Enables and disables trusted access with Organizations.

In the fourth statement, the policy includes the following permissions for iam:

- Creates the AWSServiceRoleForTrustedAdvisorReporting service-linked role.

In the fifth statement, the policy includes the following permissions for organizations:

- Allows you to register and deregister delegated administrators for Trusted Advisor Priority.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "trustedadvisor:DescribeAccount*",
            "trustedadvisor:DescribeOrganization",
            "trustedadvisor:DescribeRisk*",
            "trustedadvisor:DownloadRisk",
            "trustedadvisor:UpdateRiskStatus",
            "trustedadvisor:DescribeNotificationConfigurations",
            "trustedadvisor:UpdateNotificationConfigurations"
         ]
      }]
}
```
The `AWSTrustedAdvisorPriorityReadOnlyAccess` policy grants read-only permissions to Trusted Advisor Priority. This includes permission to view the delegated administrator accounts.

**Permissions details**
In the first statement, the policy includes the following permissions for trustedadvisor:

- Describes your Trusted Advisor account and organization.
- Describes the identified risks from Trusted Advisor Priority and allows you to download them.
- Describes the configurations for Trusted Advisor Priority email notifications.

In the second and third statement, the policy includes the following permissions for organizations:

- Describes your organization with Organizations.
- Lists the AWS services that you enabled to use Organizations.
- Lists the delegated administrators for Trusted Advisor Priority

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "trustedadvisor:DescribeAccount*",
            "trustedadvisor:DescribeOrganization",
            "trustedadvisor:DescribeRisk*",
            "trustedadvisor:DownloadRisk",
            "trustedadvisor:DescribeNotificationConfigurations"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "organizations:DescribeOrganization",
            "organizations:ListAWSServiceAccessForOrganization"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "organizations:ServicePrincipal": [
                  "reporting.trustedadvisor.amazonaws.com"
               ]
            }
         }
      }
   ]
}
```

**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 AWS Identity and Access Management (IAM) entities. For more information, see Using service-linked roles for Trusted Advisor (p. 161).
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.

- Auto Scaling – 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 (ELB) 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",
        "cloudwatch:GetMetricStatistics"
      ]
    }
  ]
}
"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",
"sgs: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. 161).

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

```json
{
  "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": "*"
    }
  ]
}
```

**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. 214) page.

The following table describes important updates to the Trusted Advisor managed policies since August 10, 2021.
Trusted Advisor

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added</td>
<td>Trusted Advisor added two new managed policies that you can use to control access to Trusted Advisor Priority.</td>
<td>August 17, 2022</td>
</tr>
<tr>
<td></td>
<td>New AWS managed policies for the Trusted Advisor</td>
<td></td>
</tr>
<tr>
<td>Added</td>
<td>Trusted Advisor added new actions to grant the DescribeTargetGroups and GetAccountPublicAccessBlock permissions.</td>
<td>August 10, 2021</td>
</tr>
<tr>
<td></td>
<td>The DescribeTargetGroup permission is required for the Auto Scaling Group Health Check to retrieve non-Classic Load Balancers that are attached to an Auto Scaling group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The GetAccountPublicAccessBlock permission is required for the Amazon S3 Bucket Permissions check to retrieve the block public access settings for an AWS account.</td>
<td></td>
</tr>
<tr>
<td>Change log published</td>
<td>Change log for the Trusted Advisor managed policies.</td>
<td>August 10, 2021</td>
</tr>
</tbody>
</table>

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, Enterprise On-Ramp, or Enterprise Support plan, you can access all checks. For more information, see AWS Trusted Advisor check reference (p. 71).

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

Topics
- Permissions for the Trusted Advisor console (p. 178)
- Trusted Advisor actions (p. 178)
- IAM policy examples (p. 180)
- See also (p. 183)
Permissions for the Trusted Advisor console

To access the Trusted Advisor console, a user must have a minimum set of permissions. These permissions must allow the user 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 Trusted Advisor console’s tag filter feature. 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 Controlling access to and for IAM users and roles using tags.

- Create an IAM policy with the trustedadvisor namespace. You can use this policy to specify permissions for 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. However, you can’t use the trustedadvisor namespace to allow or deny Trusted Advisor API operations in the AWS Support API. You must use the support namespace for AWS Support instead.

Note

If you have permissions to the AWS Support API, the Trusted Advisor widget in the AWS Management Console will show a summary view of your Trusted Advisor results. To view your results in the Trusted Advisor console, you must have permission to the trustedadvisor namespace.

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeAccount</td>
<td>Grants permission to view the AWS Support plan and various Trusted Advisor preferences.</td>
</tr>
<tr>
<td>DescribeAccountAccess</td>
<td>Grants permission to view if the AWS account has enabled or disabled Trusted Advisor.</td>
</tr>
<tr>
<td>DescribeCheckItems</td>
<td>Grants permission to view details for the check items.</td>
</tr>
<tr>
<td>DescribeCheckRefreshStatuses</td>
<td>Grants permission to view the refresh statuses for Trusted Advisor checks.</td>
</tr>
<tr>
<td>DescribeCheckSummaries</td>
<td>Grants permission to view Trusted Advisor check summaries.</td>
</tr>
<tr>
<td>DescribeChecks</td>
<td>Grants permission to view details for Trusted Advisor checks.</td>
</tr>
<tr>
<td>DescribeNotificationPreferences</td>
<td>Grants permission to view the notification preferences for the AWS account.</td>
</tr>
<tr>
<td>ExcludeCheckItems</td>
<td>Grants permission to exclude recommendations for Trusted Advisor checks.</td>
</tr>
</tbody>
</table>
### Action

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IncludeCheckItems</td>
<td>Grants permission to include recommendations for Trusted Advisor checks.</td>
</tr>
<tr>
<td>RefreshCheck</td>
<td>Grants permission to refresh a Trusted Advisor check.</td>
</tr>
<tr>
<td>SetAccountAccess</td>
<td>Grants permission to enable or disable Trusted Advisor for the account.</td>
</tr>
<tr>
<td>UpdateNotificationPreferences</td>
<td>Grants permission to update notification preferences for Trusted Advisor.</td>
</tr>
</tbody>
</table>

### Trusted Advisor actions for organizational view

The following Trusted Advisor actions are for the organizational view feature. For more information, see [Organizational view for AWS Trusted Advisor](#p. 39).

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

You can perform the following Trusted Advisor actions in the console if you have Trusted Advisor Priority enabled for your account. You can also add these Trusted Advisor actions in an IAM policy to allow or deny specific actions. For more information, see Example IAM policies for Trusted Advisor Priority (p. 183).

**Note**
The risks that appear in Trusted Advisor Priority are recommendations that your technical account manager (TAM) has identified for your account. Recommendations from a service, such as a Trusted Advisor check, are created for you automatically. Recommendations from your TAM are created for you manually. Next, your TAM sends these recommendations so that they appear in Trusted Advisor Priority for your account.

For more information, see Get started with AWS Trusted Advisor Priority (p. 63).

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeRisks</td>
<td>Grants permission to view risks in Trusted Advisor Priority.</td>
</tr>
<tr>
<td>DescribeRisk</td>
<td>Grants permission to view risk details in Trusted Advisor Priority.</td>
</tr>
<tr>
<td>DescribeRiskResources</td>
<td>Grants permission to view affected resources for a risk in Trusted Advisor Priority.</td>
</tr>
<tr>
<td>DownloadRisk</td>
<td>Grants permission to download a file that contains details about the risk in Trusted Advisor Priority.</td>
</tr>
<tr>
<td>UpdateRiskStatus</td>
<td>Grants permission to update the risk status in Trusted Advisor Priority.</td>
</tr>
<tr>
<td>DescribeNotificationConfigurations</td>
<td>Grants permission to get your email notification preferences for Trusted Advisor Priority.</td>
</tr>
<tr>
<td>UpdateNotificationConfigurations</td>
<td>Grants permission to create or update your email notification preferences for Trusted Advisor Priority.</td>
</tr>
<tr>
<td>DeleteNotificationConfigurationForDelegatedAdmin</td>
<td>Grants permission to the organization management account to delete email notification preferences from a delegated administrator account for Trusted Advisor Priority.</td>
</tr>
</tbody>
</table>

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. 181)
- Read-only access to Trusted Advisor (p. 181)
• Deny access to Trusted Advisor (p. 181)
• Allow and deny specific actions (p. 181)
• Control access to the AWS Support API operations for Trusted Advisor (p. 182)
• Example IAM policies for Trusted Advisor Priority (p. 183)

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.
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.

```json
{
  "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",
      ],
      "Resource": "*"
    }
  ]
}
```
For more information about how IAM works with AWS Support and Trusted Advisor, see Actions (p. 157).

Example IAM policies for Trusted Advisor Priority

You can use the following AWS managed policies to control access to Trusted Advisor Priority. For more information, see AWS managed policies for AWS Trusted Advisor (p. 170) and Get started with AWS Trusted Advisor Priority (p. 63).

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. 183)
- I want to view my access keys (p. 184)
- I'm an administrator and want to allow others to access AWS Support (p. 184)
- I want to allow people outside of my AWS account to access my AWS Support resources (p. 184)

I’m not authorized to perform iam:PassRole

If you receive an error that you’re not authorized to perform the iam:PassRole action, your policies must be updated 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 that are 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’s policies must be updated to allow her to perform the iam:PassRole action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.
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. 157).
- 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 Health Dashboard. For example, events that affect services or resources in your account. For more information, see Getting started with the AWS Health Dashboard in the AWS Health User Guide.

Logging and monitoring in AWS Support and AWS Trusted Advisor

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

- **Amazon CloudWatch** monitors your AWS resources and the applications that 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 Elastic Compute Cloud (Amazon EC2) instances and automatically launch new instances when needed. For more information, see the Amazon CloudWatch User Guide.

- **Amazon EventBridge** delivers a near real-time stream of system events that describe changes in AWS resources. EventBridge 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 EventBridge 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 Simple Storage Service (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.

For more information, see Monitoring and logging for AWS Support (p. 187) and Monitoring and logging for AWS Trusted Advisor (p. 196).

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 or other AWS services are within the 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.
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.
Monitoring and logging for 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 EventBridge** delivers a near real-time stream of system events that describe changes in AWS resources. EventBridge 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 EventBridge 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**
- Monitoring AWS Support cases with Amazon EventBridge (p. 187)
- Logging AWS Support API calls with AWS CloudTrail (p. 190)

Monitoring AWS Support cases with Amazon EventBridge

You can use Amazon EventBridge to detect and react to changes for your AWS Support cases. Then, based on the rules that you create, EventBridge invokes one or more target actions when an event matches the values that you specify in a rule.

Depending on the event, you can send notifications, capture event information, take corrective action, initiate events, or take other actions. For example, you can get notified whenever the following actions occur in your account:

- Create a support case
- Add a case correspondence to an existing support case
- Resolve a support case
- Reopen a support case

**Note**
AWS Support delivers events on a best effort basis. Events are not always guaranteed to be delivered to EventBridge.

Creating an EventBridge rule for AWS Support cases

You can create an EventBridge rule to get notified for AWS Support case events. The rule will monitor updates for support cases in your account, including actions that you, your IAM users, or support agents perform. Before you create a rule for AWS Support case events, do the following:
AWS Support User Guide
Example AWS Support events

• Familiarize yourself with events, rules, and targets in EventBridge. For more information, see What is Amazon EventBridge? in the Amazon EventBridge User Guide.

• Create the target to use in your event rule. For example, you can create an Amazon Simple Notification Service (Amazon SNS) topic so that whenever a support case is updated, you will receive a text message or email. For more information, see EventBridge targets.

Note
AWS Support is a global service and doesn't use separate Regions. To receive updates for your support cases, use the US East (N. Virginia) Region.

To create an EventBridge rule for AWS Support case events

1. Open the Amazon EventBridge console at https://console.aws.amazon.com/events/.
2. If you haven't already, use the Region selector in the upper-right corner of the page and choose US East (N. Virginia).
3. In the navigation pane, choose Rules.
4. Choose Create rule.
5. On the Define rule detail page, enter a name and description for your rule.
6. Keep the default values for Event bus and Rule type, and then choose Next.
7. On the Build event pattern page, for Event source, choose AWS events or EventBridge partner events.
8. Under Event pattern, keep the default value for AWS services.
9. For AWS service, choose Support.
10. For Event type, choose Support Case Update.
11. Choose Next.
12. In the Select target(s) section, choose the target that you created for this rule, and then configure any additional options that are required for that type. For example, if you choose Amazon SNS, make sure that your SNS topic is configured correctly so that you will be notified by email or SMS.
13. Choose Next.
14. (Optional) On the Configure tags page, add any tags and then choose Next.
15. On the Review and create page, review your rule setup and ensure that it meets your event monitoring requirements.
16. Choose Create rule. Your rule will now monitor for AWS Support case events and then send them to the target that you specified.

Notes

• When you receive an event, you can use the origin parameter to determine whether you or an AWS Support agent added a case correspondence to a support case. The value for origin can be either CUSTOMER or AWS.

Currently, only events for the AddCommunicationToCase action will have this value.

• For more information about creating event patterns, see Event patterns in the Amazon EventBridge User Guide.

• You can also create another rule for the AWS API Call via CloudTrail event type. This rule will monitor AWS CloudTrail logs for AWS Support API calls in your account.

Example AWS Support events

The following events are created when support actions occur in your account.
Example: Create support case

The following event is created when a support case is created.

```
{
  "version": "0",
  "id": "343df007-9285-55a3-f6d1-536944be45d7",
  "detail-type": "Support Case Update",
  "source": "aws.support",
  "account": "111122223333",
  "time": "2022-02-21T15:51:19Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "case-id": "case-111122223333-muen-2022-7118885805350839",
    "display-id": "1234563851",
    "communication-id": "",
    "event-name": "CreateCase",
    "origin": ""
  }
}
```

Example: Update support case

The following event is created when AWS Support replies to a support case.

```
{
  "version": "0",
  "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
  "detail-type": "Support Case Update",
  "source": "aws.support",
  "account": "111122223333",
  "time": "2022-02-21T15:51:31Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "case-id": "case-111122223333-muen-2022-7118885805350839",
    "display-id": "1234563851",
    "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
    "event-name": "AddCommunicationToCase",
    "origin": "AWS"
  }
}
```

Example: Resolve support case

The following event is created when a support case is resolved.

```
{
  "version": "0",
  "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
  "detail-type": "Support Case Update",
  "source": "aws.support",
  "account": "111122223333",
  "time": "2022-02-21T15:51:31Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "case-id": "case-111122223333-muen-2022-7118885805350839",
    "display-id": "1234563851",
    "communication-id": "",
    "event-name": "ResolveCase"
  }
}
```
Example: Reopen support case

The following event is created when a support case is reopened.

```json
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

See also

For more information about how to use EventBridge with AWS Support, see the following resources:

- How to automate AWS Support API with Amazon EventBridge
- AWS Support case activity notifier on GitHub

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. 207).

**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.

```json
{
  "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.

```json
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/Admin",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Admin",
    "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"
}
```
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. 17).
- 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.

```json
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
            }
        }
    },
    "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.metal1.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 console actions for changes to your AWS Support plan

"creationDate": "2021-01-07T22:08:05Z"
}

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": "2021-01-07T22:08:07Z",
  "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": "eleeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "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"
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "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": "eleeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
AWS Support User Guide
Logging console actions for changes to your AWS Support plan

"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"}
Monitoring and logging for AWS Trusted Advisor

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

- **Amazon EventBridge** delivers a near real-time stream of system events that describe changes in AWS resources. EventBridge 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 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. EventBridge detects this event and then sends you a notification so that you can take action. For more information, see the [Amazon EventBridge User Guide](https://docs.aws.amazon.com/monitoring/latest/page_eventbridge.html).

- **AWS Trusted Advisor checks** identify ways for you to reduce cost, increase performance, and improve security for your AWS account. You can use EventBridge 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.

- **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](https://docs.aws.amazon.com/monitoring/latest/page_cloudtrail.html).

### Topics
- Monitoring AWS Trusted Advisor check results with Amazon EventBridge (p. 196)
- Creating Amazon CloudWatch alarms to monitor AWS Trusted Advisor metrics (p. 198)
- Logging AWS Trusted Advisor console actions with AWS CloudTrail (p. 207)

### Monitoring AWS Trusted Advisor check results with Amazon EventBridge

You can use EventBridge to detect when your checks for Trusted Advisor change status. Then, based on the rules that you create, EventBridge invokes one or more target actions when the status changes to a value that you specify in a rule.

Depending on the status change, you can send notifications, capture status information, take corrective action, initiate events, or take other actions. For example, you can specify the following target types if a check changes status from no problems detected (green) to recommended action (red):

- Use an AWS Lambda function to pass a notification to a Slack channel.
- Push data about the check to an Amazon Kinesis stream to support comprehensive and real-time status monitoring.
- Send an Amazon Simple Notification Service topic to your email.
• Get notified with an Amazon CloudWatch alarm action.

For more information about on how to use EventBridge and Lambda functions to automate responses for Trusted Advisor, see Trusted Advisor tools in GitHub.

Notes
• Trusted Advisor delivers events on a best effort basis. Events are not always guaranteed to be delivered to EventBridge.
• You must have an AWS Support plan to create a rule for Trusted Advisor checks. For more information, see Changing your AWS Support plan (p. 17).

Follow this procedure to create an EventBridge rule for Trusted Advisor. Before you create event rules, do the following:
• Familiarize yourself with events, rules, and targets in EventBridge. For more information, see What is Amazon EventBridge? in the Amazon EventBridge User Guide.
• Create the target that you will use in your event rule.

To create an EventBridge rule for Trusted Advisor
1. Open the Amazon EventBridge console at https://console.aws.amazon.com/events/.
2. To change the Region, use the Region selector in the upper-right corner of the page and choose US East (N. Virginia).
3. In the navigation pane, choose Rules.
4. Choose Create rule.
5. On the Define rule detail page, enter a name and description for your rule.
6. Keep the default values for Event bus and Rule type, and then choose Next.
7. On the Build event pattern page, for Event source, choose AWS events or EventBridge partner events.
8. Under Event pattern, keep the default value for AWS services.
9. For AWS service, choose Trusted Advisor.
10. For Event type, choose Check Item Refresh Status.
11. Choose one of the following options for check statuses:
   • Choose Any status to create a rule that monitors for any status change.
   • Choose Specific status(es), and then choose the values that you want your rule to monitor.
     • ERROR – Trusted Advisor recommends an action for the check.
     • INFO – Trusted Advisor can't determine the status of the check.
     • OK – Trusted Advisor doesn't detect an issue for the check.
     • WARN – Trusted Advisor detects a possible issue for the check and recommends investigation.
12. Choose one of the following options for your checks:
   • Choose Any check.
   • Choose Specific check(s), and then choose one or more check names from the list.
13. Choose one of the following options for AWS resources:
   • Choose Any resource ID to create a rule that monitors all resources.
   • Choose Specific resource ID(s) by ARN, and then enter the Amazon Resource Names (ARNs) that you want.
15. In the **Select target(s)** page, choose the target type that you created for this rule, and then configure any additional options that are required for that type. For example, you might send the event to an Amazon SQS queue or an Amazon SNS topic.

16. Choose **Next**.

17. (Optional) On the **Configure tags** page, add any tags and then choose **Next**.

18. On the **Review and create** page, review your rule setup and ensure that it meets your event monitoring requirements.

19. Choose **Create rule**. Your rule will now monitor for Trusted Advisor checks and then send the event to the target that you specified.

---

**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. 198)
- CloudWatch metrics for Trusted Advisor (p. 201)
- Trusted Advisor metrics and dimensions (p. 206)

**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. 34).

**To create a CloudWatch alarm for Trusted Advisor metrics**

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.
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**.

<table>
<thead>
<tr>
<th>Check Name</th>
<th>Metric Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM Access Key Rotation</td>
<td>YellowResources</td>
</tr>
</tbody>
</table>

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.
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).
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)

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 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.

```bash
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```
Your output might look like the following.

```json
{
  "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"
        }
      ]
    }
  ]
}
```
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"
                },
            ],
            "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"
    }
  ]
}
```
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.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RedResources</td>
<td>The number of resources that are in a red state (action recommended).</td>
</tr>
<tr>
<td>YellowResources</td>
<td>The number of resources that are in a yellow state (investigation recommended).</td>
</tr>
</tbody>
</table>

**Trusted Advisor category-level metrics**

You can use the following metrics for Trusted Advisor categories.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GreenChecks</td>
<td>The number of Trusted Advisor checks that are in a green state (no issues detected).</td>
</tr>
<tr>
<td>RedChecks</td>
<td>The number of Trusted Advisor checks that are in a red state (action recommended).</td>
</tr>
<tr>
<td>YellowChecks</td>
<td>The number of Trusted Advisor checks that are in a yellow state (investigation recommended).</td>
</tr>
</tbody>
</table>

**Trusted Advisor service quota-level metrics**

You can use the following metrics for AWS service quotas.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceLimitUsage</td>
<td>The percentage of resource usage against a service quota (formerly referred to as limits).</td>
</tr>
</tbody>
</table>

**Dimensions for check-level metrics**

You can use the following dimension for Trusted Advisor checks.

API Version 2013-04-15

206
Dimensions for category-level metrics

You can use the following dimension for Trusted Advisor check categories.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>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. 31) page.</td>
</tr>
</tbody>
</table>

Dimensions for service quota metrics

You can use the following dimensions for Trusted Advisor service quota metrics.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>The AWS Region for a service quota.</td>
</tr>
<tr>
<td>ServiceName</td>
<td>The name of the AWS service.</td>
</tr>
<tr>
<td>ServiceLimit</td>
<td>The name of the service quota. For more information about service quotas, see AWS service quotas in the AWS General Reference.</td>
</tr>
</tbody>
</table>

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
- DescribeRisk
- DescribeRisks
- DescribeRiskResources
- DescribeServiceMetadata
- DownloadRisk
- ExcludeCheckItems
- GenerateReport
- IncludeCheckItems
- ListAccountsForParent
- ListRoots
- ListOrganizationalUnitsForParent
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
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": "AIDACKCEVSQ6CJEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/janedoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIATOPDDNN7EXAMPLE",
        "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": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "R365s2Qddf"
    },
    "responseElements": {
```
Example: Trusted Advisor Log File Entries

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

```json
{
    "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":"signin.amazonaws.com",
    "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":"f5b923d8-d210-4037-bd32-997c6EXAMPLE",
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```
Example: Trusted Advisor Log File Entries

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": "signin.amazonaws.com",
  "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"
}
```
Troubleshooting resources

For answers to common troubleshooting questions, see the AWS Support Knowledge Center.

For Windows, Amazon EC2 offers EC2Rescue, which customers can use 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.

<table>
<thead>
<tr>
<th>Service</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services</td>
<td>Troubleshooting AWS Signature Version 4 errors</td>
</tr>
<tr>
<td>Amazon AppStream</td>
<td>Troubleshoot Amazon AppStream</td>
</tr>
<tr>
<td>Amazon EC2 Auto Scaling</td>
<td>Troubleshooting Auto Scaling</td>
</tr>
<tr>
<td>AWS Certificate Manager (ACM)</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>Troubleshooting AWS CloudFormation</td>
</tr>
<tr>
<td>Amazon CloudFront</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>Amazon CloudSearch</td>
<td>Troubleshooting Amazon CloudSearch</td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td>Troubleshooting AWS CodeDeploy</td>
</tr>
<tr>
<td>AWS Data Pipeline</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>Troubleshooting AWS Direct Connect</td>
</tr>
<tr>
<td>AWS Directory Service</td>
<td>Troubleshooting AWS Directory Service administration issues</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>Troubleshooting instances</td>
</tr>
<tr>
<td>Amazon Elastic Container Service (Amazon ECS)</td>
<td>Amazon ECS troubleshooting</td>
</tr>
<tr>
<td>Service</td>
<td>Link</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>Troubleshoot your application load balancers</td>
</tr>
<tr>
<td>Amazon EMR (Amazon EMR)</td>
<td>Troubleshoot a cluster</td>
</tr>
<tr>
<td>Amazon ElastiCache for Memcached</td>
<td>Troubleshooting applications</td>
</tr>
<tr>
<td>Amazon ElastiCache for Redis</td>
<td>Troubleshooting applications</td>
</tr>
<tr>
<td>AWS Flow Framework</td>
<td>Troubleshooting and debugging tips</td>
</tr>
<tr>
<td>AWS GovCloud (US)</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>AWS Identity and Access Management (IAM)</td>
<td>Troubleshooting IAM</td>
</tr>
<tr>
<td>Kinesis</td>
<td>Troubleshooting Kinesis producers</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>Troubleshooting and monitoring AWS Lambda functions with CloudWatch</td>
</tr>
<tr>
<td>AWS OpsWorks</td>
<td>Debugging and troubleshooting guide</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>Troubleshooting queries</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>Troubleshooting Amazon Route 53</td>
</tr>
<tr>
<td>Amazon Silk</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>Amazon Simple Email Service (Amazon SES)</td>
<td>Troubleshooting Amazon SES</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>Troubleshooting CORS issues</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service (Amazon SWF)</td>
<td>AWS flow framework for Java: Troubleshooting and debugging tips</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>Troubleshooting your gateway</td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud (Amazon VPC)</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>Amazon WorkMail</td>
<td>Troubleshooting the Amazon WorkMail web application</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>Troubleshooting Amazon WorkSpaces administration issues</td>
</tr>
<tr>
<td>Amazon WorkSpaces Application Manager (Amazon WAM)</td>
<td>Troubleshooting Amazon WAM application issues</td>
</tr>
</tbody>
</table>
# 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

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.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added documentation for Trusted Advisor Priority (p. 214)</td>
<td>Trusted Advisor Priority adds support for the following features:</td>
<td>August 17, 2022</td>
</tr>
<tr>
<td></td>
<td>• Delegated administrators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Daily and weekly email notifications for recommendation summaries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reopen resolved or rejected recommendations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS managed policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see Getting started with Trusted Advisor Priority.</td>
<td></td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>The Preferences page in the Trusted Advisor console has been updated. For more information, see Getting started with AWS Trusted Advisor.</td>
<td>July 15, 2022</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>Updated the checks to include the following information:</td>
<td>July 7, 2022</td>
</tr>
<tr>
<td></td>
<td>• Alert Criteria</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Recommended Action</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Additional Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Report columns</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see the AWS Trusted Advisor check reference.</td>
<td></td>
</tr>
<tr>
<td>Updated documentation for AWS Support (p. 214)</td>
<td>Added documentation that explains how to manage your support cases.</td>
<td>June 28, 2022</td>
</tr>
</tbody>
</table>
### Updated documentation

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated documentation for <strong>AWSSupportServiceRolePolicy</strong></td>
<td>Updated permissions to provide billing, administrative, and support services for the service-linked role. For more information, see AWS managed policy: <strong>AWSSupportServiceRolePolicy</strong>.</td>
<td>June 23, 2022</td>
</tr>
<tr>
<td>Updated documentation for <strong>Trusted Advisor (p. 214)</strong></td>
<td>Trusted Advisor supports additional AWS Foundational Security Best Practices security standard controls that are sourced from AWS Security Hub. For more information, see the Change log for AWS Trusted Advisor checks.</td>
<td>June 23, 2022</td>
</tr>
<tr>
<td>Updated documentation for <strong>Trusted Advisor (p. 214)</strong></td>
<td>Added information about how to request service quota increases. For more information, see Service limits.</td>
<td>June 21, 2022</td>
</tr>
<tr>
<td>Updated documentation for <strong>AWS Support (p. 214)</strong></td>
<td>The create case experience has been updated in the Support Center Console. For more information, see Creating support cases and case management.</td>
<td>May 18, 2022</td>
</tr>
<tr>
<td>Updated documentation for <strong>Trusted Advisor (p. 214)</strong></td>
<td>Added four checks for Amazon EBS and AWS Lambda. For more information, see Opt in AWS Compute Optimizer to add Trusted Advisor checks.</td>
<td>May 4, 2022</td>
</tr>
<tr>
<td>Updated documentation for <strong>AWSSupportServiceRolePolicy</strong></td>
<td>Added new permissions to provide billing, administrative, and support services for the service-linked role. For more information, see AWS managed policy: <strong>AWSSupportServiceRolePolicy</strong>.</td>
<td>April 27, 2022</td>
</tr>
<tr>
<td>Updated documentation for the <strong>Exposed Access Keys check (p. 214)</strong></td>
<td>This check is now automatically refreshed for you. For more information, see Change log for AWS Trusted Advisor checks.</td>
<td>April 25, 2022</td>
</tr>
<tr>
<td>Updated documentation for <strong>Trusted Advisor (p. 214)</strong></td>
<td>The AWS Direct Connect checks in the fault tolerance category are updated. For more information, see Change log for AWS Trusted Advisor checks.</td>
<td>March 29, 2022</td>
</tr>
<tr>
<td>Updated documentation for AWSSupportServiceRolePolicy</td>
<td>Added new permissions to provide billing, administrative, and support services for the service-linked role. For more information, see <a href="https://docs.aws.amazon.com/AWSSupport/latest/APIReference/awssupportservicepolicy.html">AWS managed policy: AWSSupportServiceRolePolicy</a>.</td>
<td>March 14, 2022</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Added documentation for Trusted Advisor Priority (p. 214)</td>
<td>You can use Trusted Advisor Priority to view a list of prioritized recommendations from your technical account manager (TAM). For more information, see <a href="https://docs.aws.amazon.com/trustedadvisor/latest/userguide/what-is-trusted-advisor.html">Getting started with Trusted Advisor Priority</a>.</td>
<td>February 28, 2022</td>
</tr>
<tr>
<td>Updated documentation for using Amazon EventBridge for Trusted Advisor (p. 214)</td>
<td>You can create an EventBridge rule to monitor changes to your Trusted Advisor checks. For more information, see <a href="https://docs.aws.amazon.com/eventbridge/latest/userguide/monitoring-trusted-advisor-check-result-events.html">Monitoring AWS Trusted Advisor check results with EventBridge</a>.</td>
<td>February 21, 2022</td>
</tr>
<tr>
<td>New documentation for using Amazon EventBridge to monitor AWS Support cases (p. 214)</td>
<td>You can create an EventBridge rule to monitor and receive notifications about your support cases. For more information, see <a href="https://docs.aws.amazon.com/eventbridge/latest/userguide/monitoring-support-case-events.html">Monitoring AWS Support cases with EventBridge</a>.</td>
<td>February 21, 2022</td>
</tr>
<tr>
<td>Updated documentation for AWSSupportServiceRolePolicy</td>
<td>Added new permissions to provide billing, administrative, and support services for the service-linked role. For more information, see <a href="https://docs.aws.amazon.com/AWSSupport/latest/APIReference/awssupportservicepolicy.html">AWS managed policy: AWSSupportServiceRolePolicy</a>.</td>
<td>February 17, 2022</td>
</tr>
<tr>
<td>Added documentation for integrating with AWS Security Hub (p. 214)</td>
<td>In the Trusted Advisor console, you can now view the findings for your Security Hub controls that are part of the AWS Foundational Security Best Practices security standard. For more information, see <a href="https://docs.aws.amazon.com/trustedadvisor/latest/userguide/security-hub.html">Viewing AWS Security Hub controls in the AWS Trusted Advisor console</a>.</td>
<td>January 18, 2022</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>Added three new checks for Amazon EC2 instances that are running Microsoft SQL Server.</td>
<td>December 20, 2021</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>• Amazon EC2 instances consolidation for Microsoft SQL Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Amazon EC2 instances over-provisioned for Microsoft SQL Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Amazon EC2 instances with Microsoft SQL Server end of support</td>
<td></td>
</tr>
<tr>
<td>For more information, see the AWS Trusted Advisor check reference.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>Trusted Advisor added four new checks for AWS Well-Architected</td>
<td>December 20, 2021</td>
</tr>
<tr>
<td></td>
<td>• AWS Well-Architected high risk issues for cost optimization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS Well-Architected high risk issues for performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS Well-Architected high risk issues for security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS Well-Architected high risk issues for reliability</td>
<td></td>
</tr>
<tr>
<td>For more information, see the AWS Trusted Advisor check reference.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updated documentation (p. 214)</td>
<td>If you have an Enterprise On-Ramp Support plan, you have access to all Trusted Advisor checks and the AWS Support API.</td>
<td>November 24, 2021</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>Trusted Advisor added two new checks for Amazon Comprehend.</td>
<td>September 29, 2021</td>
</tr>
<tr>
<td></td>
<td>For more information, see the AWS Trusted Advisor check reference.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The check name for Amazon Elasticsearch Reserved Instance Optimization is renamed to Amazon OpenSearch Service Reserved Instance Optimization.</td>
<td>September 8, 2021</td>
</tr>
<tr>
<td></td>
<td>For more information, see Change log for AWS Trusted Advisor checks.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor checks (p. 214)</td>
<td>Added a reference topic for all Trusted Advisor checks. For more information, see AWS Trusted Advisor check reference.</td>
<td>September 1, 2021</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor managed policies (p. 214)</td>
<td>Updated documentation for the Trusted Advisor managed policies. For more information, see AWS managed policies for AWS Support and AWS Trusted Advisor.</td>
<td>August 10, 2021</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>Updated documentation for the Trusted Advisor console. For more information, see Get started with AWS Trusted Advisor.</td>
<td>July 16, 2021</td>
</tr>
<tr>
<td>Updated documentation for creating AWS Support cases (p. 214)</td>
<td>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.</td>
<td>June 8, 2021</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor (p. 214)</td>
<td>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.</td>
<td>June 8, 2021</td>
</tr>
</tbody>
</table>
| Updated documentation (p. 214) | The following topics are updated:  
  • 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 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated documentation about AWS managed policies</td>
<td>Added information about the AWSManagedPolicyServiceRolePolicy AWS managed policy. For more information, see Using service-linked roles for AWS Support (p. 160).</td>
<td>March 16, 2021</td>
</tr>
<tr>
<td>Added checks for AWS Lambda</td>
<td>Added four AWS Trusted Advisor checks for Lambda in the Change log for AWS Trusted Advisor checks (p. 146).</td>
<td>March 8, 2021</td>
</tr>
<tr>
<td>Updated service limit checks for Amazon Elastic Block Store</td>
<td>Updated five AWS Trusted Advisor checks for Amazon EBS in the Change log for AWS Trusted Advisor checks (p. 146).</td>
<td>March 5, 2021</td>
</tr>
<tr>
<td>Updated documentation for CloudTrail logging</td>
<td>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. 193).</td>
<td>February 9, 2021</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor</td>
<td>Updated the Get started with AWS Trusted Advisor (p. 29) topic.</td>
<td>January 29, 2021</td>
</tr>
<tr>
<td>Updated documentation for Trusted Advisor reports</td>
<td>Added a Troubleshooting (p. 56) section for using Trusted Advisor reports with other AWS services.</td>
<td>December 4, 2020</td>
</tr>
<tr>
<td>Added AWS Trusted Advisor support for AWS CloudTrail logging</td>
<td>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. 207).</td>
<td>November 23, 2020</td>
</tr>
<tr>
<td>Added a change log topic</td>
<td>View changes to AWS Trusted Advisor checks and categories in the Change log for AWS Trusted Advisor checks (p. 146).</td>
<td>November 18, 2020</td>
</tr>
<tr>
<td>Added support for organizational units</td>
<td>You can now create reports for Trusted Advisor checks for organizational units (OUs). For more information, see Create organizational view reports (p. 41).</td>
<td>November 17, 2020</td>
</tr>
<tr>
<td>Updated the logging with AWS CloudTrail topic</td>
<td>Added an example log entry for a Trusted Advisor API operation. See AWS Trusted Advisor information in CloudTrail logging (p. 191).</td>
<td>October 22, 2020</td>
</tr>
<tr>
<td>Added AWS Support quotas</td>
<td>Added information about the current quotas and restrictions for AWS Support. See the AWS Support endpoints and quotas in the AWS General Reference.</td>
<td>August 4, 2020</td>
</tr>
<tr>
<td>Organizational view for AWS Trusted Advisor</td>
<td>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. 39).</td>
<td>July 17, 2020</td>
</tr>
</tbody>
</table>
### Earlier updates

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and AWS Support</td>
<td>Updated information about security considerations when using AWS Support and Trusted Advisor. See <a href="#">Security in AWS Support</a>.</td>
<td>May 5, 2020</td>
</tr>
<tr>
<td>Security and AWS Support</td>
<td>Added information about security considerations when using AWS Support.</td>
<td>January 10, 2020</td>
</tr>
<tr>
<td>Using Trusted Advisor as a web service</td>
<td>Added updated instructions to refresh Trusted Advisor data after getting list of Trusted Advisor checks.</td>
<td>November 1, 2018</td>
</tr>
<tr>
<td>Using Service-linked roles</td>
<td>Added new section.</td>
<td>July 11, 2018</td>
</tr>
<tr>
<td>Getting Started: Troubleshooting</td>
<td>Added troubleshooting links for Route 53 and AWS Certificate Manager.</td>
<td>September 1, 2017</td>
</tr>
<tr>
<td>Case Management Example: Creating a Case</td>
<td>Added a note about the CC box for users who have the Basic support plan.</td>
<td>August 1, 2017</td>
</tr>
<tr>
<td>Monitoring Trusted Advisor Check Results with CloudWatch Events</td>
<td>Added new section.</td>
<td>November 18, 2016</td>
</tr>
<tr>
<td>Case Management</td>
<td>Updated the names of case severity levels.</td>
<td>October 27, 2016</td>
</tr>
<tr>
<td>Logging AWS Support Calls with AWS CloudTrail</td>
<td>Added new section.</td>
<td>April 21, 2016</td>
</tr>
<tr>
<td>Getting Started: Troubleshooting</td>
<td>Added more troubleshooting links.</td>
<td>May 19, 2015</td>
</tr>
<tr>
<td>Getting Started: Troubleshooting</td>
<td>Added more troubleshooting links.</td>
<td>November 18, 2014</td>
</tr>
<tr>
<td>Getting Started: Case Management</td>
<td>Updated to reflect AWS Service Catalog in the AWS Management Console.</td>
<td>October 30, 2014</td>
</tr>
<tr>
<td>Programming the Life of an AWS Support Case</td>
<td>Added information about new API elements for adding attachments to cases and for omitting case communications when retrieving case history.</td>
<td>July 16, 2014</td>
</tr>
<tr>
<td>Accessing AWS Support</td>
<td>Removed named support contacts as an access method.</td>
<td>May 28, 2014</td>
</tr>
<tr>
<td>Getting Started</td>
<td>Added the Getting Started section.</td>
<td>December 13, 2013</td>
</tr>
<tr>
<td>Initial publication</td>
<td>New AWS Support service released.</td>
<td>April 30, 2013</td>
</tr>
</tbody>
</table>
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.