aws re/start

AWS Trusted Advisor

Security Fundamentals

This module introduces AWS Trusted Advisor.

What you will learn

At the core of the lesson

You will learn how to:

- Describe AWS Trusted Advisor
- Explore the five categories of recommendations that Trusted Advisor produces
- List the security features of Trusted Advisor
- Interpret Trusted Advisor recommendations

aws re/start

You will learn how to:

- Describe AWS Trusted Advisor
- Explore the five categories of recommendations that Trusted Advisor produces
- List the security features of Trusted Advisor
- Interpret Trusted Advisor recommendations

Trusted Advisor

You'll begin with an overview of Trusted Advisor.

Introduction to Trusted Advisor

Trusted Advisor provides best practices or checks in five categories:

- Cost optimization
- Performance
- Security
- Fault tolerance
- Service limits

Checks have a status:

Green: No problem detected

Yellow: Investigation recommended

Red: Action recommended

aws re/start

Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. It provides best practices (or checks) in five categories:

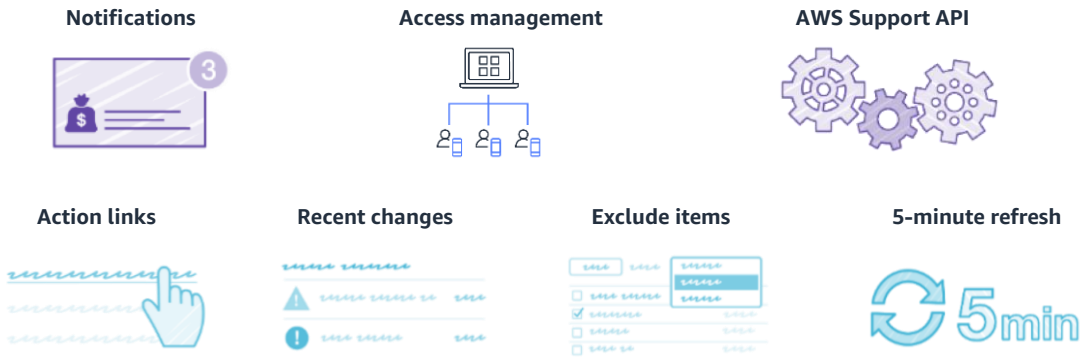
1. **Cost Optimization** – Save money on AWS by reducing unused and idle resources or making commitments to reserved capacity.
2. **Performance** – Improve the performance of your service by checking your service limits, ensuring that you take advantage of provisioned throughput, and monitoring for overutilized instances.
3. **Security** – Improve the security of your application by closing gaps, activating various AWS security features, and examining your permissions.
4. **Fault Tolerance** – Increase the availability and redundancy of your AWS application by taking advantage of automatic scaling, health checks, multiple Availability Zones, and backup capabilities.
5. **Service Limits** – Check for service usage that is more than 80 percent of the service limit.

The status of the check is shown by using color coding on the dashboard page:

- **Red** (red exclamation mark) – Action is recommended.
- **Yellow** (yellow exclamation mark) – Investigation is recommended.
- **Green** (green checkmark) – No problem has been detected.

Trusted Advisor features

Trusted Advisor provides a suite of features for you to customize recommendations and to proactively monitor your Amazon Web Services (AWS) resources.



aws re/start

Trusted Advisor provides a suite of features so that you can customize recommendations and proactively monitor your Amazon Web Services (AWS) resources:

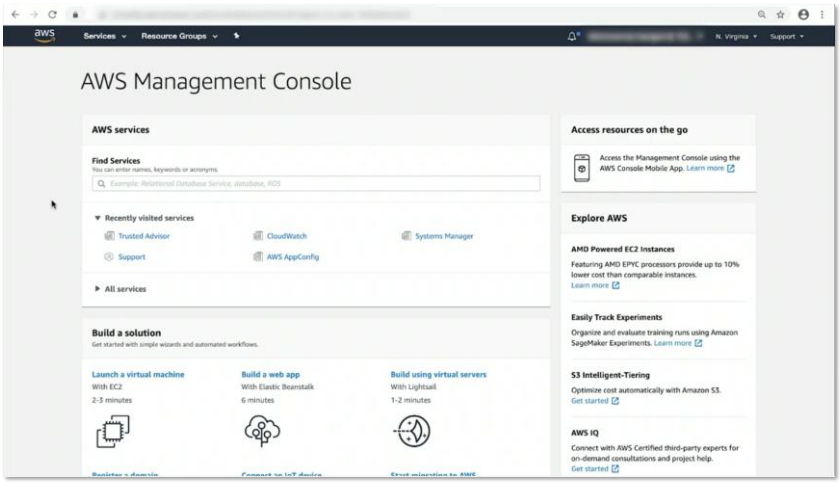
- **Trusted Advisor notifications** – Stay up to date with your AWS resource deployment. You will receive a weekly notification email message when you opt in for this service.
- **Access management** – Control access to specific checks or check categories.
- **AWS Support application programming interface (API)** – Retrieve and refresh Trusted Advisor results programmatically.
- **Action links** – Access items in a Trusted Advisor report from hyperlinks that take you directly to the console. From the console, you can implement the Trusted Advisor recommendations.
- **Recent changes** – Track recent changes of check status on the console dashboard. The most recent changes appear at the top of the list to bring them to your attention.
- **Exclude items** – Customize the Trusted Advisor report. You can exclude items from the check result if they are not relevant.
- **Refresh all** – Refresh individual checks or refresh all the checks at once by choosing Refresh All in the upper-right corner of the summary dashboard. A check is eligible for **5-Minute Refresh** after it was last refreshed.

For more information about Trusted Advisor, see the AWS Trusted Advisor product webpage at https://aws.amazon.com/premiumsupport/technology/trusted-advisor/.

Trusted Advisor walkthrough (1 of 4)

How do I start using Trusted Advisor?

Sign in to the AWS Management Console, and navigate to Trusted Advisor.



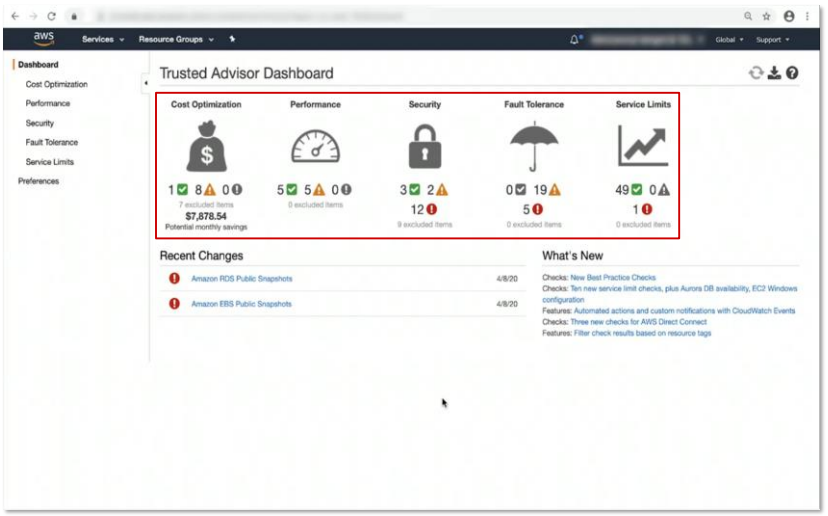
aws re/start

Sign in to the AWS Management Console, and navigate to Trusted Advisor. This action opens the Trusted Advisor Dashboard.

Trusted Advisor walkthrough (2 of 4)

Trusted Advisor Dashboard

- The Trusted Advisor Dashboard provides a summary of findings for each of the five check categories.
- You can refresh all checks in your account.
- You can also export all of the results to an .xls file.
- Select a category icon to see a list of the checks performed for that category.



aws re/start

Trusted Advisor inspects your AWS infrastructure for opportunities to save money, improve system availability and performance, or help close security gaps. The checks are based on best practices identified by experts in each AWS service and on information from customers over time.

The results are summarized in the Trusted Advisor Dashboard for each of the five check categories. For each category, the count of recommendations is grouped by check status:

- Red – Action recommended
- Yellow – Investigation recommended
- Green – No problem detected

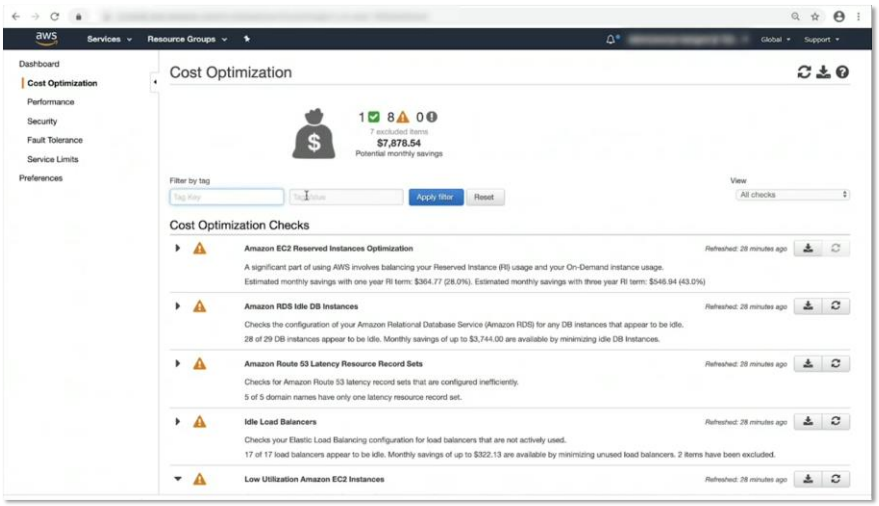
The dashboard displays a *What's New* section that lists new and improved features of Trusted Advisor. It also displays a *Recent Changes* section that highlights recent check status changes.

You can choose a category icon to display the list of checks performed for that category.

Trusted Advisor walkthrough (3 of 4)

Category checklist

- The list of checks for a category is grouped by check status.
- You can filter the list to show only the checks that have a given status.
- You can export the details of an individual check to an .xls file.
- Expand a check to see its details.



aws re/start

The list of checks for a category groups each check by status and provides a summarized description of the check. You can filter the list to show only the checks that have have a given status by using the *View* dropdown menu. You can also export the details of an individual check to an .xls file.

This slide shows an example of the list of checks for the Cost Optimization category.

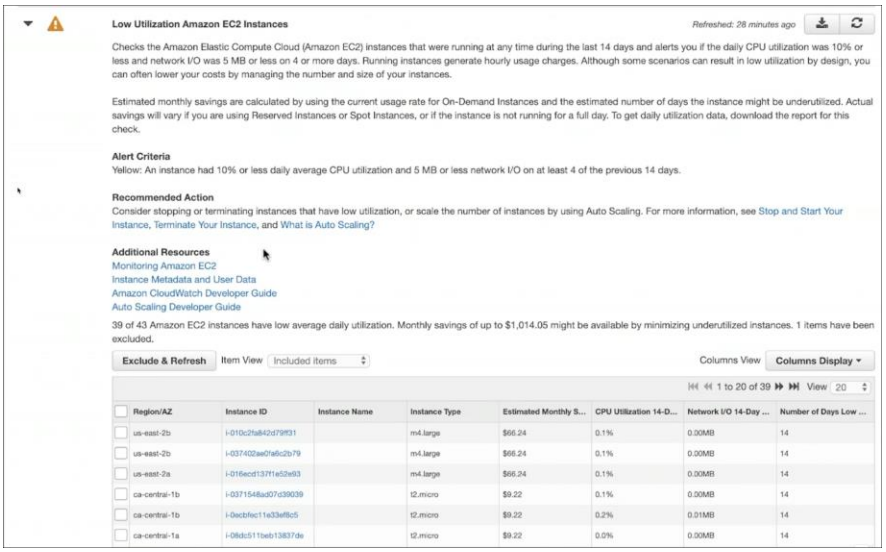
Expand a check to see its details.

Trusted Advisor walkthrough (4 of 4)

Check details

The details for the check include the following:

- Detailed description
- Alert Criteria
- Recommended Action
- Additional Resources
- A table that lists the affected items in your account



aws re/start

When you expand a check, you see the following details:

- **Detailed description**
- **Alert Criteria** – Describes the status of the check and the threshold conditions that it evaluates.
- **Recommended Action** – Describes the recommended actions for the 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.

This slide shows an example screen capture of the details for a **Low Utilization Amazon EC2 Instances** check. The table at the bottom lists the affected instances in the account. This check identifies 39 EC2 instances that have low usage and recommends that you stop or terminate the resources.

Trusted Advisor security checks

Trusted advisor provides the following security checks to all customers at no cost:

1. AWS Identity and Access Management (IAM) use
2. Multi-factor authentication (MFA) on root account
3. Security groups – Specific ports unrestricted
4. Amazon Simple Storage Service (Amazon S3) bucket permissions
5. Amazon Elastic Block Store (Amazon EBS) public snapshots
6. Amazon Relational Database Service (Amazon RDS) public snapshots

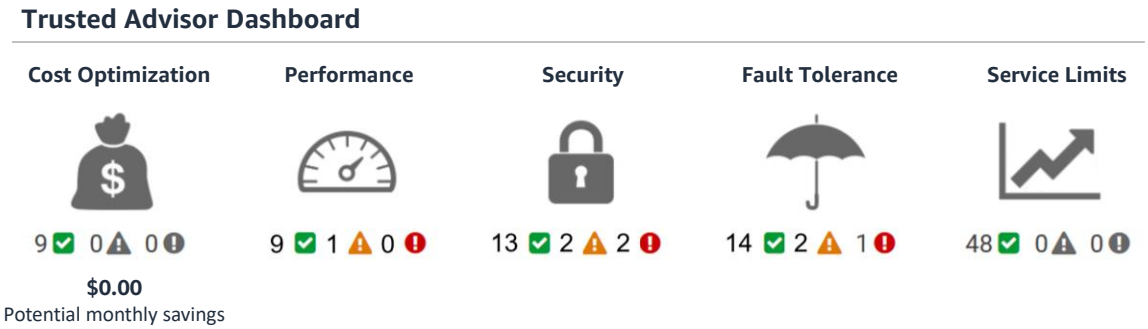
Trusted Advisor provides popular performance and security recommendations to all AWS customers. The following Trusted Advisor checks are available to all customers at no cost:

1. **AWS Identity and Access Management (IAM) use**: Checks for the existence of at least one IAM user to discourage the use of root access
2. **Multi-factor authentication (MFA) on root account:** Checks the root account and warns you if MFA is not activated
3. **Security groups** – Specific ports unrestricted: Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports
4. **Amazon Simple Storage Service (Amazon S3) bucket permissions:** Checks buckets in Amazon S3 that have open access permissions or that allow access to any authenticated AWS user.
5. **Amazon Elastic Block Store (Amazon EBS) public snapshots:** Checks the permission settings for your Amazon EBS volume snapshots and alerts you if any snapshots are marked as public
6. **Amazon Relational Database Service (Amazon RDS) public snapshots:** Checks the permission settings for your Amazon RDS database (DB) snapshots and alerts you if any snapshots are marked as public

Activity

Next, you'll learn more about Trusted Advisor through an activity.

Activity: Interpret Trusted Advisor recommendations



aws re/start

You have a friend who used Trusted Advisor for the first time. Your friend is trying to interpret its recommendations to improve their cloud environment and needs your help.

The dashboard shown on the slide is your friend's dashboard. In the *Security* category, you notice that a few recommendations are indicated. You want to examine these recommendations to help your friend improve their security.

Help your friend interpret the following recommendations, which are on the next few slides.

Activity: Recommendation 1

MFA on the root account

Description: Checks the root account and warns when 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.

Alert criteria: MFA is not enabled on the root account.

Recommended action: Log in to your root account and activate an MFA device.

aws re/start

For this recommendation, answer the following questions:

- What is the status?
- What is the problem?
- What specific environment details are you given?
- What is the best practice?
- What is the recommended action?

Activity: Recommendation 2

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.

Alert Criteria: A password policy is enabled, but at least one content requirement is not 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.

aws re/start

For this recommendation, answer the following questions:

- What is the status?
- What is the problem?
- What specific environment details are you given?
- What is the best practice?
- What is the recommended action?

Activity: Recommendation 3

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).

Alert Criteria: 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.

Region	Security Group Name	Security Group ID	Protocol	Port	Status	IP Range
us-east-1	WebServerSG	sg-xxxxxxx1 (vpc-xxxxxxx1)	tcp	22	Red	0.0.0.0/0
us-west-2	DatabaseServerSG	sg-xxxxxxx2 (vpc-xxxxxxx2)	Tcp	8080	Red	0.0.0.0/0

aws re/start

For this recommendation, answer the following questions:

- What is the status?
- What is the problem?
- What specific environment details are you given?
- What is the best practice?
- What is the recommended action?

Activity: Recommendation No. 4

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.

Alert Criteria:

Yellow: The bucket does not have server access logging enabled.
Yellow: The target bucket permissions do not include the owner account. Trusted Advisor cannot check it.

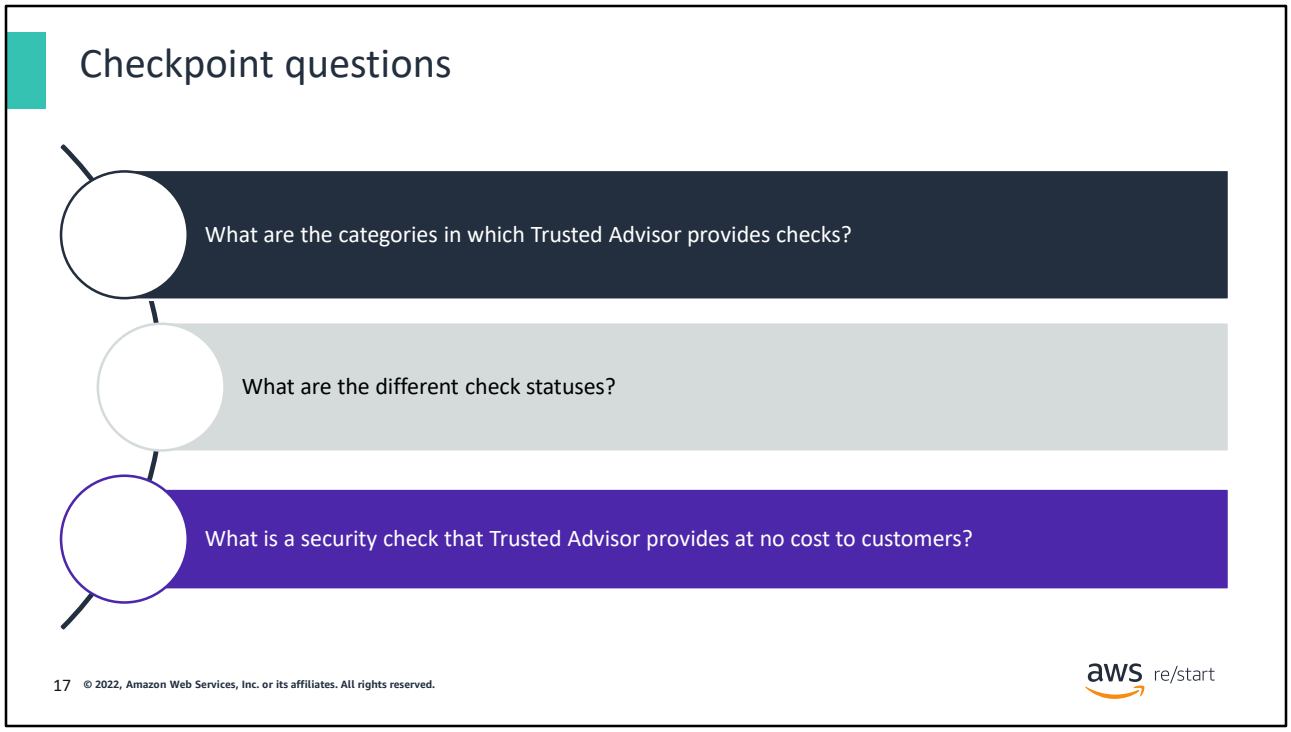
Recommended Action: Enable bucket logging for most buckets. If the target bucket permissions do not include the owner account and you want Trusted Advisor to check the logging status, add the owner account as a grantee.

Region	Bucket Name	Target Name	Target Exists	Same Owner	Write Enabled	Reason
us-east-1	My-hello-world-bucket		No	No	No	Logging not enabled

aws re/start

For this recommendation, answer the following questions:

- What is the status?
- What is the problem?
- What specific environment details are you given?
- What is the best practice?
- What is the recommended action?



Q1: What are the categories in which Trusted Advisor provide checks?

- Cost optimization
- Performance
- Security
- Fault tolerance
- Service limits

Q2: What are the different check statuses?

- Action recommended (red)
- Investigation recommended (yellow)
- No problems detected (green)

Q3: What is a security check that Trusted Advisor provides at no cost to customers?

Any one of the following:

- IAM use
- MFA on the root account

- Security groups – Specific ports unrestricted
- S3 bucket permissions
- Amazon EBS public snapshots
- Amazon RDS public snapshots

Key takeaways

- Trusted Advisor is an online tool that provides real-time guidance to help you **provision**, **optimize**, and **secure** your resources by following AWS best practices.
- Examples of Trusted Advisor **security checks and advice** include the following:
  - Making sure that **security groups** do not keep ports open with unrestricted access
  - Checking for your use of **IAM permissions** to control access to AWS resources
  - Checking the root account and warning **if MFA** is not activated
  - Checking that **S3 buckets do not have open access permissions**

aws re/start

This module includes the following key takeaways:

- Trusted Advisor is an online tool that provides real-time guidance to help you provision, optimize, and secure your resources by following AWS best practices.
- Examples of Trusted Advisor security checks and advice include the following:
  - Making sure that security groups do not keep ports open with unrestricted access
  - Checking for your use of IAM permissions to control access to AWS resources
  - Checking the root account and warning you if MFA is not activated
  - Checking that S3 buckets do not have open access permissions

Thank you

Thank you for completing this module.