


This lesson 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 produced by Trusted Advisor
- Highlight the features of Trusted Advisor
- Interpret Trusted Advisor recommendations



2

aws re/start

This module reviews AWS Trusted Advisor and its checks.



AWS 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** – How you can 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, enabling 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** – Checks 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.



AWS 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:

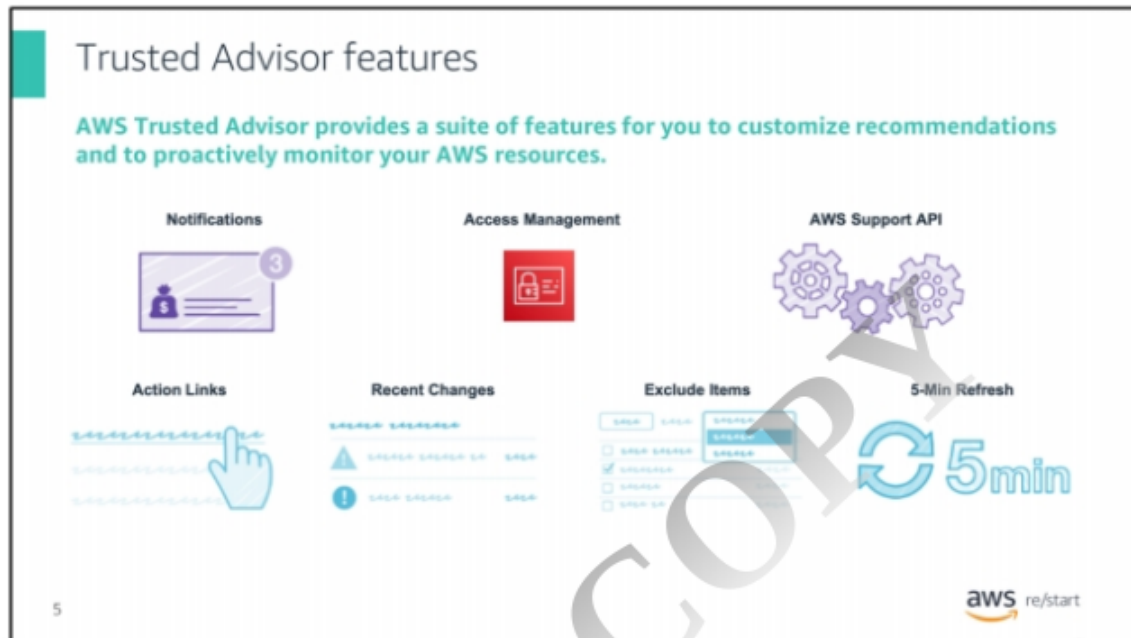
1. Service limits
2. Security groups – Specific ports unrestricted
3. AWS Identity and Access Management (IAM) use
4. Multi-factor authentication (MFA) on root account
5. Amazon Elastic Block Store (Amazon EBS) public snapshots
6. Amazon Relational Database Service (Amazon RDS) public snapshots

The complete set of checks and guidance is available with Business Support and Enterprise Support plans. AWS Trusted Advisor helps you to provision your resources by following best practices. Using this capability, you can improve system performance and reliability, increase security, and look for opportunities to save money.

To learn more about Trusted Advisor best practices, see "AWS Trusted Advisor best practice checklist" on the AWS Support webpage

[\(https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/\)](https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/).

DO NOT COPY
bufetekaye.22@gmail.com



AWS Trusted Advisor provides a suite of features so you can customize recommendations and to proactively monitor your AWS resources:

- **Trusted Advisor Notifications** – Stay up to date with your AWS resource deployment. You will be notified by a weekly email message when you opt in for this service.
- **AWS Identity and Access Management (IAM)** – Control access to specific checks or check categories.
- **AWS Support application programming interface (API)** – Retrieve and refresh Trusted Advisor results programmatically.
- **Action Links** – Hyperlinks on items in a Trusted Advisor report 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 selecting **Refresh All** in the top-right corner of the summary dashboard. A check is eligible for **5-Minute Refresh** after it was last refreshed.

To learn more about Trusted Advisor, see [AWS Trusted Advisor](#) on the AWS

Support webpage.

DO NOT COPY
bufetekaye.22@gmail.com



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

This is your friend's dashboard. Though everything looks OK in the *Cost Optimization* and *Service Limits* categories, 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.

Activity: Recommendation no. 1



MFA on 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.

7

aws re/start

For this recommendation, answer these 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. 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.

8

aws re/start

For this recommendation, answer these 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. 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

For this recommendation, answer these 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



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.

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-2	my-hello-world-bucket		No	No	No	Logging not enabled


10

aws re/start

For this recommendation, answer these 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?

Key takeaways



© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

11

- AWS 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 –
 - Making sure that **security groups** do not keep ports open with unrestricted access.
 - Checking for your use of **AWS Identity and Access Management (IAM) permissions** to control access to AWS resources.
 - Checking the root account and warning if **multi-factor authentication (MFA)** is not enabled.
 - Checking that **logging** is enabled on Amazon Simple Storage Service (Amazon S3) buckets.

aws re/start

Key takeaways from this lesson include:

- AWS 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 –
 - Making sure that security groups do not keep ports open with unrestricted access.
 - Checking for your use of AWS Identity and Access Management (IAM) permissions to control access to AWS resources.
 - Checking the root account and warning if multi-factor authentication (MFA) is not enabled.
 - Checking that logging is enabled on Amazon Simple Storage Service (Amazon S3) buckets.