Auditing Your Security with AWS Trusted Advisor

**SPL-75 - Version 2.0.17**

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at [*AWS Training and Certification*](https://support.aws.amazon.com/#/contacts/aws-training).

**Lab overview**

This lab guides you through the steps to audit your AWS resources to ensure your configuration complies with basic **security best practices**. This lab makes use of AWS Trusted Advisor as it applies to security. The topics covered include working with security groups, Multi-factor Authentication (MFA), and AWS Identity and Access Management (IAM).

**Note:** If you are attending *AWS re:Inforce 2023* and would like to follow along with the instructor for this spotlight lab, you can use the following presentation:

OBJECTIVES

By the end of this lab, you will be able to do the following:

* Use Trusted Advisor to perform a basic audit of your AWS resources
* Modify Amazon Elastic Compute Cloud (Amazon EC2) Security Groups to meet best practices
* Configure Multi-factor Authentication (MFA) (Optional, requiring installation of software on a mobile device)

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should be familiar with AWS services, including Amazon EC2 and have a basic understanding of security groups. You should be comfortable logging into and using the AWS Management Console and have familiarity with IAM.

DURATION

This lab will require *90* minutes to complete.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

* A sample output that you can use to verify the output of a step/task that you perform.
* A hint, tip, or important guidance.
* **Additional information:** Where to find more information.

**AWS Security Best Practices**

SHARED RESPONSIBILITY MODEL

The AWS Security Model is that of **shared responsibility**, which requires both AWS and customers to work together towards security objectives. AWS provides a highly secure and available underlying infrastructure on which all AWS services operate. The AWS layers of security includes security of physical hardware, facilities, network infrastructure, and the virtualization infrastructure.

Layers beyond AWS direct control require the customer take responsibility of properly securing the resources they use in the cloud infrastructure.

SECURING CLOUD RESOURCES

AWS has provided a number of controls that customers can use to protect their information assets in the cloud. These include IAM, Amazon Virtual Private Clouds (VPCs), security groups, network ACLs and certificates.

It is important when building and maintaining a cloud-based infrastructure in AWS to follow best practices in order to keep your data and resources secure.

The [Best Practices for Security, Identity, & Compliance](https://aws.amazon.com/architecture/security-identity-compliance) is a valuable reference guide to understanding security best practices in Amazon Web Services.

**AWS Trusted Advisor**

**AWS Trusted Advisor** provides best practices in five categories:

* Cost optimization
* Security
* Fault tolerance
* Performance improvement
* Service limits

You can use over 60 AWS Trusted Advisor checks to monitor and improve the deployment of Amazon EC2, Elastic Load Balancing (ELB), Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon EC2 Auto Scaling, AWS Identity and Access Management (IAM), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, and other services. You can view the overall status of your AWS resources and savings estimations on the AWS Trusted Advisor Recommendations page.

AWS Trusted Advisor is particularly useful in making sure you are following security best practices. In this lab you use AWS Trusted Advisor’s free security checks.

AWS TRUSTED ADVISOR PRICING

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 category and the following checks in the security category:

**Security Groups – Specific Ports Unrestricted:** 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.

**IAM Use:** Checks for your use of IAM. You can use IAM to create users, groups, and roles in AWS, and you can use permissions to control access to AWS resources.

**MFA on Root Account:** Checks the root account and warns if multi-factor authentication (MFA) is not enabled. For increased security, AWS recommends 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 console and associated websites.

**Amazon EBS Public Snapshots:** Checks the permission settings for your 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 with particular users or accounts, mark the snapshot as private, and then specify the user or accounts you want to share the snapshot data with.

**Amazon RDS Public Snapshots:** Checks the permission settings for your 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 with particular users or accounts, mark the snapshot as private, and then specify the user or accounts you want to share the snapshot data with.

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

Some of these checks can be used as a very basic audit of your security configuration. To have full access to all 60+ checks, you must upgrade your account to either the Business or Enterprise support plan.

More information on AWS Support pricing can be found at [AWS Support Plans](https://aws.amazon.com/premiumsupport/signup/)

MFA DEVICES

**Multi-Factor Authentication (MFA) devices** can be either virtual or physical. Physical MFA requires purchase of a Gemalto hardware keyfob or display card. Alternatively, you can use one of several free supported virtual MFA applications available for Android, iPhone, Windows, and Blackberry mobile devices. In this lab, you walk-through setting up a virtual MFA app on a mobile device. If you are uncomfortable with this step, you can bypass it.

Please consult this list of supported virtual MFA applications, to see if there is an option for your mobile device: [Multi-Factor Authentication (MFA) for IAM](https://aws.amazon.com/iam/details/mfa/#Virtual_MFA_Applications)

**Start lab**

1. To launch the lab, at the top of the page, choose **Start lab**.

 You must wait for the provisioned AWS services to be ready before you can continue.

1. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

**Error: You must first sign out**



If you see the message, **You must first log out before logging into a different AWS account:**

* Choose the **click here** link.
* Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
* Choose **Open Console** again.

**Error: Choosing Start Lab has no effect**

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

**Task 1: Check recommended actions with Trusted Advisor**

In this task, you analyze the basic checks performed by Trusted Advisor.

1. At the top of the **AWS Management Console**, use the search bar to search for

Trusted Advisor

 and then, in the list of results, choose the service.

The Trusted Advisor Recommendations page displays a **Checks summary** and a list of **Recommended Actions** based on pre-defined checks on the AWS account. Each recommended action will be indicated by one of three icons:

 (Red) Critical – Action recommended

 (Orange) Investigation recommended

 (Green) No issues or concerns found

1. If Trusted Advisor Recommendations page does not display any of the above icons or displays a question mark, choose **Refresh all checks** at the top-right of the page to update Trusted Advisor recommendations page status.

**Note:** If you encounter a notice at the top of the screen that says *Checks have been refreshed*, you can close the notice.

1. Wait for few seconds, for **Recommended Actions** section to appear.
2. Expand each AWS Trusted Advisor check and explore the details. Any items which are not green will list the criteria for the status and provide a *Recommended Action*.

**Note:** If you cannot see an **Refresh all checks** enabled at the top-right of the page item,  Try refreshing the Security Groups - Specific Ports Unrestricted item using  button.

**Congratulations!** You analyzed the basic checks performed by Trusted Advisor.

**Task 2: Modify security groups with unrestricted ports**

As part of the lab setup, some security best practices and settings have been intentionally created contrary to best practice. In this task, you identify and resolve an incorrectly opened port on a security group.

1. In the **Trusted Advisor** navigation pane to the left of the page, choose **Security** under **Recommendations** menu.
2. Under **Checks**, expand  **Security Groups - Specific Ports Unrestricted**.
3. In the **Security Groups** table at the bottom of this section, identify the Security Group(s) that are marked as **Red**  in the **Status** column.

One of the items listed shows that there is a protocol/port that is unrestricted in the security group (tcp/port 21). Your security staff inform you that this port is not currently needed and should be removed from the rules.

**Note:** If you cannot see an item which has (tcp/port 21), try refreshing the **Security Groups - Specific Ports Unrestricted** item using the  button.

1. Find the item that contains **tcp** in the **Protocol** column and **21** in the **From Port** column.
2. Choose the **WordPress Security Group** link to open the **Security Groups** page.
3. Choose the **Inbound rules** tab.
4. Choose **Edit inbound rules**, then:

* For the rule for port 21, select **Delete** to the right of the rule
* Select **Save rules**

**Expected output:**

**Inbound security group rules successfully modified on security group**

**Congratulations!** You have used the **Trusted Advisor** findings to detect security groups in you account that has unnecessary unrestricted ports and remediated them.

**Task 3: Modify Security Groups to Restrict Access**

In this task, you tighten the access on a security group to only allow inbound traffic from a specific Amazon EC2 instance.

1. Go back to the **Trusted Advisor** console page.
2. In the navigation pane to the left, choose **Security** under the **Recommendations** menu.
3. Under **Checks**, expand  **Security Groups - Specific Ports Unrestricted**
4. Identify the **tcp/port 3306** security group that was also flagged as Red  by Trusted Advisor.

This group is allowing unrestricted access to an Amazon RDS MySQL database (port 3306/tcp).

1. Choose the **MySQL Security Group** link to open the **Security Groups** page.
2. Choose the **Inbound rules** tab.
3. Choose **Edit inbound rules**, then:

Notice that the rule is permitting incoming traffic to port 3306 from **0.0.0.0/0**, which means traffic will be permitted from **any computer on the Internet**. This is poor security practice for a database, which should only permit access from an application such as a Web Server.

1. Remove the rule for **port 3306** by choosing **Delete** to the right of the rule.
2. Choose **Add rule**, and then:

* For **Type**, choose **MySQL/Aurora**. Notice the **Protocol** and **Port range** fields are populated with **TCP 3306** automatically.
* For **Source**, choose **Custom**. In the search field, enter

sg

 and then choose the **Web Security Group**.

This rule now permits access to the RDS database only from members of the Web Security Group. Computers on the Internet will no longer be able to make contact with the database server.

1. Choose **Save rules**.

**Expected output:**

**Inbound security group rules successfully modified on security group**

1. Return back to the **Trusted Advisor** page and choose **Recommendations** from the navigation pane to the left of the page.
2. At the top-right of the page, choose the **Refresh all checks** to force Trusted Advisor to re-evaluate all the checks. This might take some time. During this time, you can remediate another issue in the next task.

**Note:** If you cannot see **Refresh all checks** enabled at the top-right of the page item,  Expand each AWS Trusted Advisor check and explore the details. Any items which are not green will list the criteria for the status and provide a *Recommended Action*, try refreshing the Security Groups - Specific Ports Unrestricted item using  button and try refreshing the MFA on Root Account item using  button.

**Congratulations!** You have used the **Trusted Advisor** findings to detect security groups in you account that has unrestricted access to required ports and remediated them.

**Task 4: Configure multi-factor authentication (MFA)**

In this task, you configure multi-factor authentication for your *user-1* IAM User using a virtual device.

TASK 4.1: SETUP YOUR MFA VIRTUAL DEVICE

1. In the **Trusted Advisor** navigation pane to the left of the page, choose **Security** under **Recommendations** menu.
2. Under **Checks**, expand  **MFA on Root Account**.
3. Under **Alert Criteria**, note that the status is **Red**  and that MFA is not currently enabled on the root account.

**Note:** The check by AWS Trusted Advisor recommends enabling MFA for the **root account**. For the purposes of this lab, you only configure MFA for *user-1*. The process for root is identical.

1. Install one of the [supported virtual MFA applications](https://aws.amazon.com/iam/details/mfa/#Virtual_MFA_Applications) onto the mobile device of your choice.
2. At the top of the **AWS Management Console**, use the search bar to search for

IAM

 and then, in the list of results, choose the service.

1. In the left navigation pane, choose **Users**, under **Access management** menu.
2. Under the **User name** column, choose the **user-1** link to open the summary page of user-1.
3. Choose the **Security credentials** tab.

This tab shows several ways that this IAM User can authenticate to AWS. Note that **Multi-factor authentication (MFA)** has no assigned MFA device.

1. In **Multi-factor authentication (MFA)**, choose **Assign MFA device**

* For **Device name**, enter

MyMFAdevice

.

* Choose  **Authenticator app**, then choose **Next**

1. In the **Set up your authenticator app**, choose **Show QR code**

This code is used to configure a mobile device-based virtual MFA. If your virtual MFA app and device are able to scan the QR code, do that now. If not, choose **Show secret key** and configure your app manually.

1. For **MFA code 1**, enter the 6-digit code displayed in your MFA app.
2. Wait 30 seconds for the next code to appear on your mobile device.
3. For **MFA code 2**, enter the 6-digit code displayed in your MFA app.
4. Choose **Add MFA**.

**Expected output:**

 MFA device assigned.

TASK 4.2: VERIFY AUTHENTICATION USING MFA TOKEN

To verify MFA authentication, you need to login to the AWS Management Console as **user-1**. This requires that you use a new private window in your browser. This allows you to login to the AWS Management Console with a different user while stay logged in as the original lab user.

1. In your preferred browser, open a new Private, Incognito, or InPrivate window.
2. From the **Resources** pane to the left of these instructions, copy the **LoginURL** and paste it into your new private browser window to open the AWS Management Console login page.
3. In the AWS Management Console login page, for **IAM user name**, enter

user-1

1. From the **Resources** pane to the left of these instructions, copy the **AdministratorPassword** value and paste it in the **Password** field.
2. Choose **Sign in**
3. The **Multi-factor Authentication** page will be opened. For the **MFA Code**, enter the 6-digit code displayed in your MFA app.
4. Choose **Submit**

If you can login to the AWS Management Console, then the MFA virtual device have been integrated with IAM for authenticating *user-1*.

1. Close the browser private window and return back to the original AWS Management Console page to continue the lab.

**Congratulations!** You have successfully configured MFA authentication for *user-1*.

**Task 5: Exclude Security Groups if Unrestricted Access is Required**

In this task, you configure Trusted Advisor to exclude ports that you intentionally wish to be opened.

1. If you are not already on the **Trusted Advisor** page, use the AWS Management Console search bar to search for

Trusted Advisor

 and then, in the list of results, choose the service.

1. Scroll down to the **Recommended Actions** section and locate the **Security Groups - Specific Ports Unrestricted** check.
2. Expand the  **Security Groups - Specific Ports Unrestricted** check.

 If you must allow unrestricted access to any port, it is vital to have other controls such as a firewall and/or secure authentication.

1. Examine the remaining security groups.

* Port 3389 grants RDP (Remote Desktop Protocol) access to Windows-based instances
* Port 22 grants SSH access to Linux-based instances

In some situations, you want to approve having such ports open. You can therefore configure Trusted Advisor to skip over these warnings.

1. In the **Security Groups - Specific Ports Unrestricted** section:

* Select  the security group for port **tcp/22**
* Select  the security group for port **tcp/3389**
* Select **Exclude & Refresh**.

**Note:** If the **Exclude & Refresh** button is greyed out, then you need to wait for the Trusted Advisor checks to be updated.

The lines should now disappear from the list. (They are accessible by changing the Item View from **Included items** to **Excluded items**).

**Congratulations!** You have successfully configured Trusted Advisor to exclude ports that you intentionally wish to be opened.

**Conclusion**

 Congratulations! You now have successfully:

* Used AWS Trusted Advisor to perform a basic audit of your AWS resources
* Modified Amazon EC2 Security Groups to meet best practices
* Configured Multi-factor Authentication (MFA)

**End lab**

Follow these steps to close the console and end your lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
3. Choose **End lab** and then confirm that you want to end your lab.

For more information about AWS Training and Certification, see [*https://aws.amazon.com/training/*](https://aws.amazon.com/training/).

*Your feedback is welcome and appreciated.*  
If you would like to share any feedback, suggestions, or corrections, please provide the details in our [*AWS Training and Certification Contact Form*](https://support.aws.amazon.com/#/contacts/aws-training).

* [Best Practices for Security, Identity, & Compliance](https://aws.amazon.com/architecture/security-identity-compliance)
* [AWS Support Plans](https://aws.amazon.com/premiumsupport/signup/)
* [List of supported virtual MFA applications](http://aws.amazon.com/iam/details/mfa/)
* [IAM Best Practices](http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html)
* [Amazon Trusted Advisor](https://aws.amazon.com/premiumsupport/trustedadvisor/)
* [Using a Virtual MFA](http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_VirtualMFA.html)