Module 8. Resources for Security Support

This module covers the following subjects:

- **Tools for Security Support**: This module section details various essential tools for security support in AWS.
- **Additional Security Support Resources**: This module section provides even more security support resource ideas available to you as an AWS or potential customer.

Greater security than ever before in your infrastructure and architectures is possible within AWS. To achieve the highest levels of security and the lowest levels of risk, you should be ready to take advantage of the tremendous resources available for security support. This module is critical in this regard.

TOOLS FOR SECURITY SUPPORT

When you have a topic as critical as security, you need many tools to assist you. With AWS, that is precisely what you get.

Certifications and Attestations

The number of security certifications and attestations for AWS is staggering—and this list is constantly growing! These certifications and attestations help you ensure that you meet the security levels you might be required to provide.

Assurance programs in this category include the following:

- DoD SRG
- FedRAMP
- FIPS
- IRAP
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MLPS Level 3
- MTCS
- PCI DSS Level 1
- SEC Rule 17a-4(f)
- SOC 1
- SOC 2
- SOC 3

There are many laws and regulations you might need to meet. Fortunately, AWS allows for the following requirements:

- EU Model Clauses
- FERPA
- HIPAA
- IRS-1075
- ITAR
- My Number Act (Japan)
- VPAT / Section 508
- EU Data Protection Directive

Finally, AWS adheres to many frameworks recommended for security, including the following:

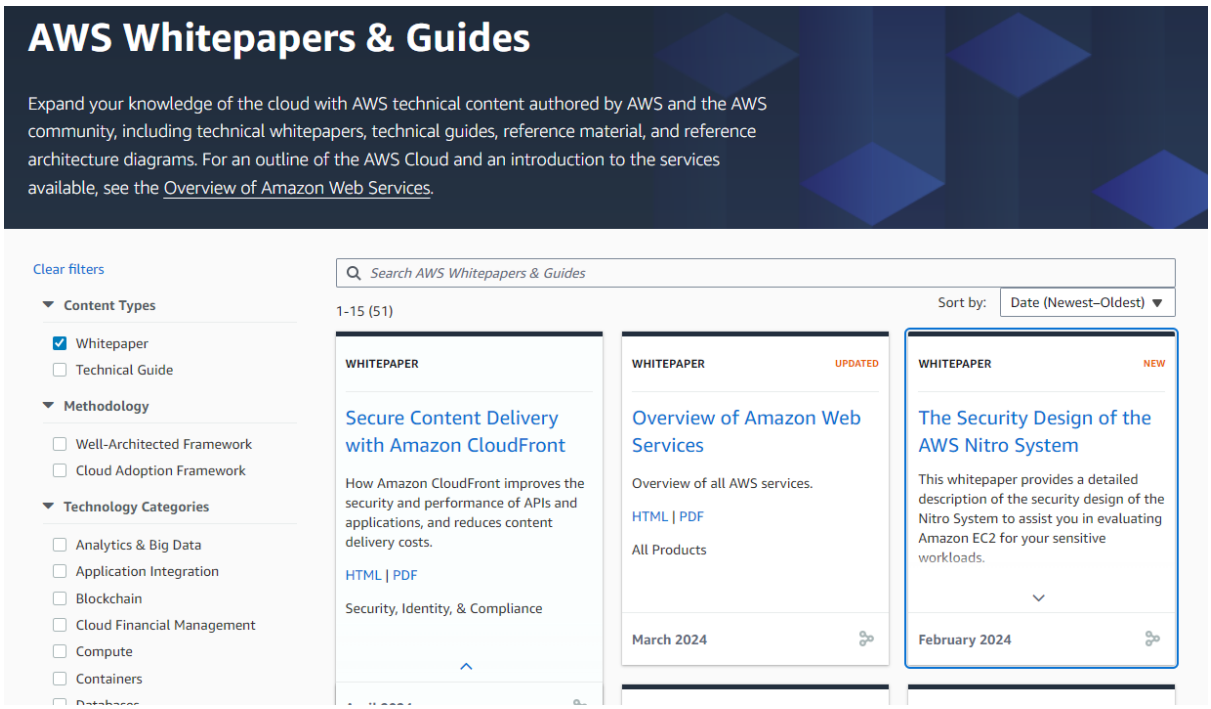
- CJIS
- FedRAMP TIC
- FISC
- FISMA
- GxP (FDA 21 CFR Part 11)
- IT-Grundschutz
- MPAA
- NERC
- NIST
- UK Cyber Essentials

Whitepapers

Reading AWS whitepapers for assistance is commonplace. However, it is a crucial step in security. AWS understands this and provides many essential whitepapers related directly to security.

Want to get excited over just some of these titles? Check out Table 8-2 for a screenshot of some of the many whitepapers available. As an AWS engineer or user, you should keep current on these.

Table 8-2 AWS Security Related Whitepapers (check for more recent ones)



AWS Artifact

AWS Artifact is your go-to central resource for compliance-related information that matters to you. It provides on-demand access to AWS's security and compliance reports and select online agreements. Reports available in AWS Artifact include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

AWS Trusted Advisor

Wouldn't it be nice if we had our own cloud expert working for us at AWS? This is the concept behind the Trusted Advisor tool. This management tool ensures you are following security best practices and helps you close security gaps.

LAB: Using the Trusted Advisor

This lab walks you through the steps of using the Trusted Advisor to learn of security issues and improvements you might be able to make to enhance your AWS security.

Note

This lab assumes you have an AWS Free Tier account.

Follow these steps to use Trusted Advisor:

Step 1. In the AWS Management Console, search for **Trusted Advisor**. Select the **Trusted Advisor** link that appears.

Step 2. In the dashboard on the left side of the page, click **Security**.

Step 3. Note the security checks that have been performed and the results. Notice also the other security checks that may be purchased. Figure 8-1 shows the security checks.

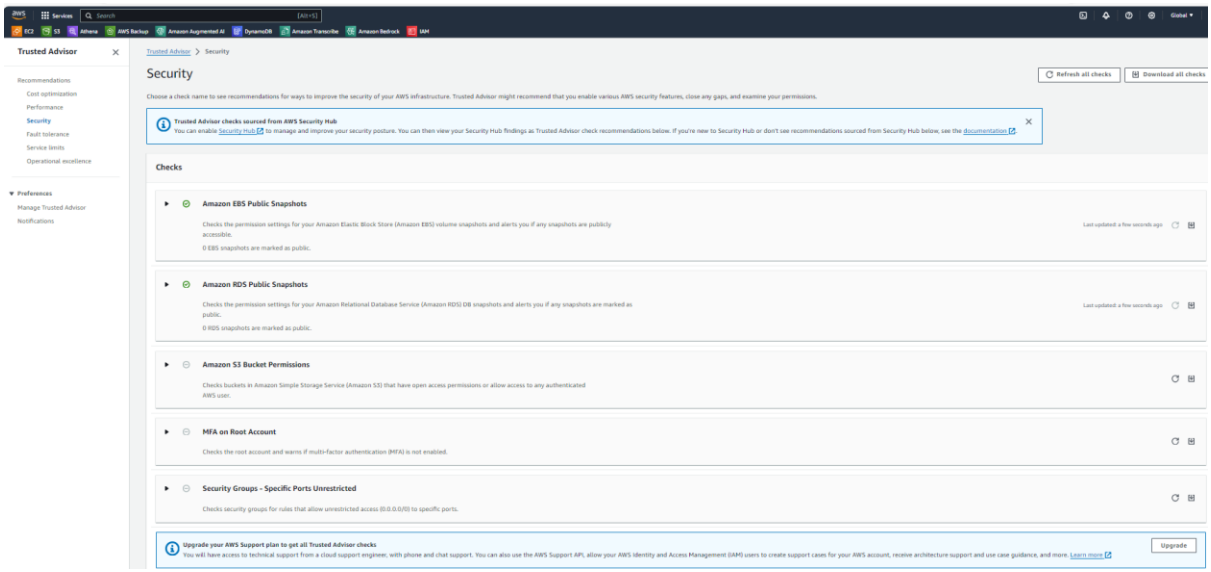


Figure 8-1 Using the Trusted Advisor for Security Guidance

Cloud Associates and Engineers

AWS offers a range of support plans to cater to the varying needs of organisations, from essential guidance for startups and individual developers to advanced technical support for mission-critical applications. AWS Support Plans provide access to resources and technical support to help users manage, monitor, and optimise their AWS infrastructure. Here's an overview of the different AWS support plans:

1. Basic Support

- **Overview:** Basic Support is included with all AWS accounts at no additional cost. It provides access to AWS customer service, documentation, whitepapers, and support forums.
- **Key Features:**
    - **AWS Support Dashboard:** Access to a personal support dashboard for managing support cases.
    - **24/7 Access to Customer Service:** Assistance with account and billing-related inquiries.
    - **Service Health Dashboard:** Real-time information on the status of AWS services.
    - **AWS Trusted Advisor:** Access to seven core Trusted Advisor checks for best practices on security, fault tolerance, and service limits.

2. Developer Support

- **Overview:** Developer Support is designed for users experimenting with AWS and needing guidance in their development and testing environments. This plan offers enhanced technical support and resources to help with early-stage projects.
- **Pricing:** Starts at $29 per month.
- **Key Features:**
    - **Business Hours Support:** Access to cloud support engineers via email during business hours.
    - **General Guidance:** Response time of < 24 hours for general guidance.
    - **System Impaired Issues:** Response time of < 12 hours for system-impaired issues.

- **Best Practice Recommendations:** Access to architectural best practices for building on AWS.
- **Case Severity Levels:** Ability to open cases with low to moderate severity levels.

3. Business Support

- **Overview:** Business Support is tailored for production workloads and provides access to AWS support engineers 24/7, with faster response times and architectural guidance.
- **Pricing:** Starts at $100 per month or 10% of monthly AWS usage, whichever is greater.
- **Key Features:**
  - **24/7 Technical Support:** Access to support engineers via email, chat, and phone.
  - **Use Case Guidance:** Provides architectural guidance and best practices for specific use cases.
  - **IAM Support:** Enables using AWS Identity and Access Management (IAM) for managing support cases.
  - **AWS Trusted Advisor:** Full access to all Trusted Advisor checks, including cost optimisation, security, and performance.
  - **Response Times:** < 1 hour for production system impaired and < 4 hours for production system down issues.
  - **Third-Party Software Support:** Assistance with standard third-party software running on AWS.

4. Enterprise Support

- **Overview:** Enterprise Support is designed for large-scale enterprises running business-critical workloads on AWS. It offers the highest level of support, including a dedicated Technical Account Manager (TAM) and proactive guidance from AWS experts.
- **Pricing:** Starts at $15,000 per month or a percentage of monthly AWS usage.
- **Key Features:**
  - **Dedicated TAM:** Provides proactive guidance and advocacy, including personalised insights into account health and cost optimisation.

- **Access to AWS Experts:** Priority access to AWS subject matter experts and support engineers.
- **24/7 Support with Fast Response Times:** Response time of < 15 minutes for business-critical system down issues.
- **Operational Reviews:** Regular reviews of your infrastructure to identify risks and provide recommendations.
- **Proactive Services:** Includes architectural reviews, account management, and workshops.
- **Incident Management:** Access to AWS Incident Management for large-scale issues impacting critical systems.
- **Event Management:** Support for planning and operating events such as product launches, migrations, and seasonal promotions.

Choosing the Right Support Plan:

- **Basic Support** suits users who need minimal support and are comfortable relying on self-service resources.
- **Developer Support** is ideal for developers or small teams working on non-production environments who need more guidance and best practices.
- **Business Support** is best for organisations with production workloads that require 24/7 support, faster response times, and more comprehensive best practice guidance.
- **Enterprise Support** is designed for enterprises with critical applications that demand proactive support, fast response times, and dedicated resources to ensure the smooth operation of their AWS environment.

AWS Support Plans are designed to meet the diverse needs of AWS customers, offering varying levels of support, guidance, and hands-on assistance to help ensure the success of cloud operations.

See https://aws.amazon.com/premiumsupport/plans

ADDITIONAL SECURITY SUPPORT RESOURCES

Believe it or not, there are even more security support resources than we have mentioned thus far in the module. This section explores even more of them.

Professional Services Consultants

The AWS Professional Services organisation is a global team of experts that can help you realise your desired business outcomes when using the AWS Cloud. Amazon works with your team and your chosen AWS Partner Network (APN) member to execute your enterprise cloud computing initiatives.

The AWS Professional Services organisation provides assistance through a collection of offerings that help you achieve specific outcomes related to enterprise cloud adoption. AWS Professional Services also deliver focused guidance through their global specialty practices, which cover a variety of solutions, technologies, and industries. In addition to working alongside AWS customers, AWS Professional Services share their experience through tech talk webinars, whitepapers, and blog posts that are available to anyone.

AWS Partner Network

The AWS Partner Network (APN) is the global partner program for AWS. It is focused on helping APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support.

APN Partners receive business, technical, sales, and marketing resources to help you to grow your business and better support your customers. You can join the APN and take advantage of numerous APN programs to differentiate your business and connect with customers on AWS.

The AWS Partner Network strives to ensure customers take full advantage of all the business benefits that AWS has to offer. With their deep expertise in AWS, APN Partners are uniquely positioned to help your company at any stage of your cloud adoption journey and to help you achieve your business objectives.

Advisories and Bulletins (Check the site for the latest)

No matter how carefully engineered the AWS services are, from time to time, it may be necessary to notify customers of security and privacy events with AWS services. As a result, Amazon publishes security bulletins that are publicly accessible via their website. You can also subscribe to the Security Bulletin RSS Feed to keep abreast of security announcements.

Here is a sample AWS Security bulletin

Issue with Amazon EC2 VM Import Export Service

Publication Date: 2024/06/11 10:30 AM PDT

AWS is aware of an issue with the Amazon Elastic Compute Cloud (Amazon EC2) VM Import Export Service (VMIE). On April 12, 2024, we addressed this issue and can confirm new Windows OS imports are not affected.

When using the EC2 VMIE service to import a VM using Windows OS, customers can optionally use their own Sysprep answer file. Before April 12, 2024, the EC2 VMIE service had an issue where, if a customer imported a VM using Windows OS to use as an AMI or instance, then an identical backup copy of the answer file would be created without sensitive data being removed if included in the file. This backup file is only accessible to on-instance Windows users who had permission to access the customer-provided answer file.

For customers who used the EC2 VMIE service in this manner, we recommend checking for a file name ending with .vmimport in the following locations, which are associated with Sysprep:

- C:\
- C:\Windows\Panther\
- C:\Windows\Panther\Unattend\
- C:\Windows\system32\
- C:\Windows\system32\sysprep\Panther\Unattend\

Once you identify the .vmimport file, restrict access to necessary user accounts or remove the backup file completely on the imported EC2

instance(s) or instance(s) launched from an affected AMI. Completing either of these actions will not affect the functionality of the EC2 instance. Because new EC2 instances launched using an affected AMI will be affected by this issue, we recommend customers delete the affected AMI and create a new AMI using the EC2 VM Import Export (VMIE) Service to re-import the virtual machine, or use the EC2 API/Console to create a new AMI from the EC2 instance where the fix has been applied.

No action is required for users who had scoped down access to the Sysprep answer file before using EC2 VMIE Service to import the Windows OS or have used EC2 VMIE Service after April 12, 2024, to import Windows OS with/without Sysprep answer file in any AWS region.

We would like to thank Immersive Labs for responsibly disclosing this issue to AWS.

Security-related questions or concerns can be brought to our attention via aws-security@amazon.com.

More Bulletins can be found here:

https://aws.amazon.com/security/security-bulletins/

Auditor Learning Path

The *AWS Auditor Learning Path of the AWS Cloud Audit Academy* is designed for those in auditor, compliance, and legal roles who want to learn how their internal operations can demonstrate compliance using AWS's platform. Thanks to this Learning Path, you can build the skills necessary to understand how to audit solutions on the AWS Cloud.

Compliance Solution Guide

The AWS Compliance Solution Guide is designed to provide you with a repository of frequently used resources and processes for performing your compliance responsibilities on AWS.

AWS protects millions of active customers worldwide—from large enterprises and government organisations to startups and nonprofits. Through these relationships, Amazon has developed best-in-class resources to allow customers from any industry to understand how to achieve compliance in the AWS Cloud quickly. Customers inherit all of the benefits of the vast experience of the AWS staff, including best practices for security policies, architecture, and operational processes validated against external assurance frameworks.

See https://aws.amazon.com/compliance/solutions-guide/

Services in Scope by Compliance Program

AWS also includes services in the scope of their compliance efforts based on the expected use case, feedback, and demand. If a service is not currently listed as in the scope of the most recent assessment, it does not mean you cannot use it. It is part of your organisation's shared responsibility to determine the nature of the data. Based on the nature of what you are building on AWS, you should decide if the service will process or store customer data and how it will or will not impact the compliance of your customer data environment.

Amazon encourages you to discuss your workload objectives and goals with your AWS account team; they will be able to evaluate your proposed use case and architecture and how the AWS security and compliance processes overlay that architecture.

See https://aws.amazon.com/compliance/services-in-scope/

Security Blog

Amazon also provides a security-centric blog site that is continuously updated with the latest essential announcements and training opportunities on security-related developments.

See **https://aws.amazon.com/blogs/security/**

Case Studies

Amazon also does an excellent job of maintaining case studies and testimonials on security best practices. These case studies are available online and can even be selected based on topic. Read a few of them.

https://aws.amazon.com/solutions/case-studies/

FAQs

Another excellent resource is the Frequently Asked Questions (FAQs) area of the AWS documentation. Here, you can visit those FAQs regarding security. These present an excellent learning opportunity. These FAQs are also valuable certification exam prep resources, as Amazon derives many exam questions from these very robust and detailed FAQs.

https://aws.amazon.com/faqs/

EXAM PREPARATION TASKS

- **REVIEW ALL TOPICS**

- **DEFINE ALL KEY TERMS AND CHECK ANSWERS IN THE GLOSSARY.**

- **DO THE QUIZ – REPEAT UNTIL YOU PASS IT (100% PASSMARK).**

DEFINE KEY TERMS

Define the following key terms from this module and check your answers in the Glossary:

Whitepapers

AWS Artifact

Trusted Advisor

AWS Professional Services

AWS Partner Network

AWS Auditor Learning Path

Q&A

1. Provide at least three examples of security frameworks to which AWS adheres.

2. What level of technical support provides 24×7 access to Senior Cloud Support Engineers via email, chat, and phone?