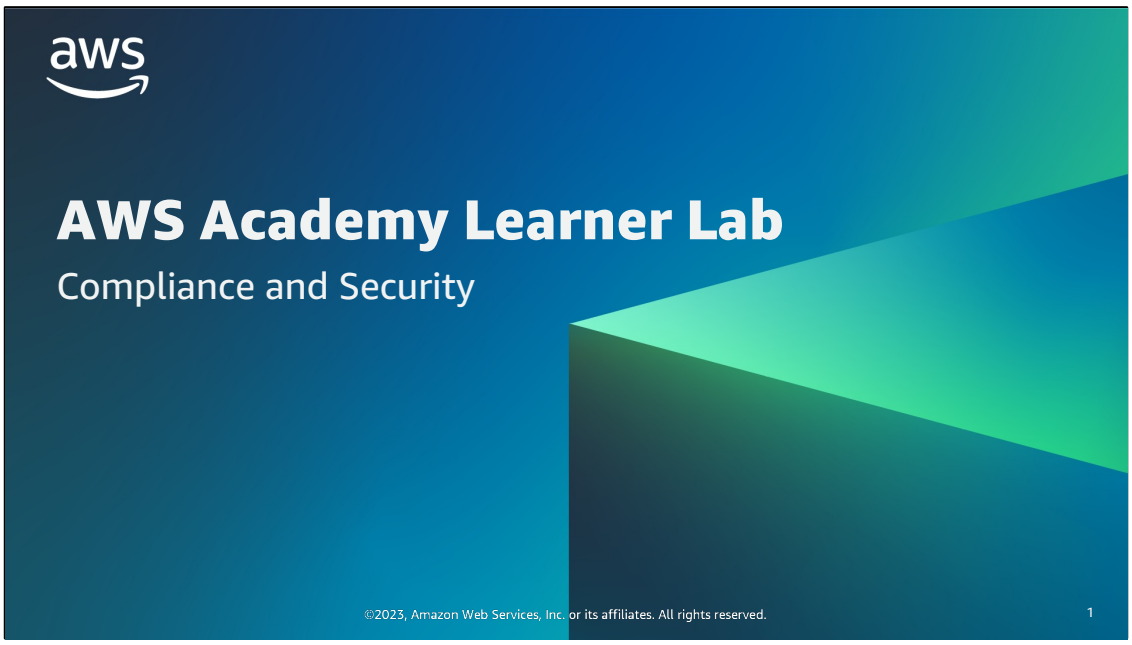
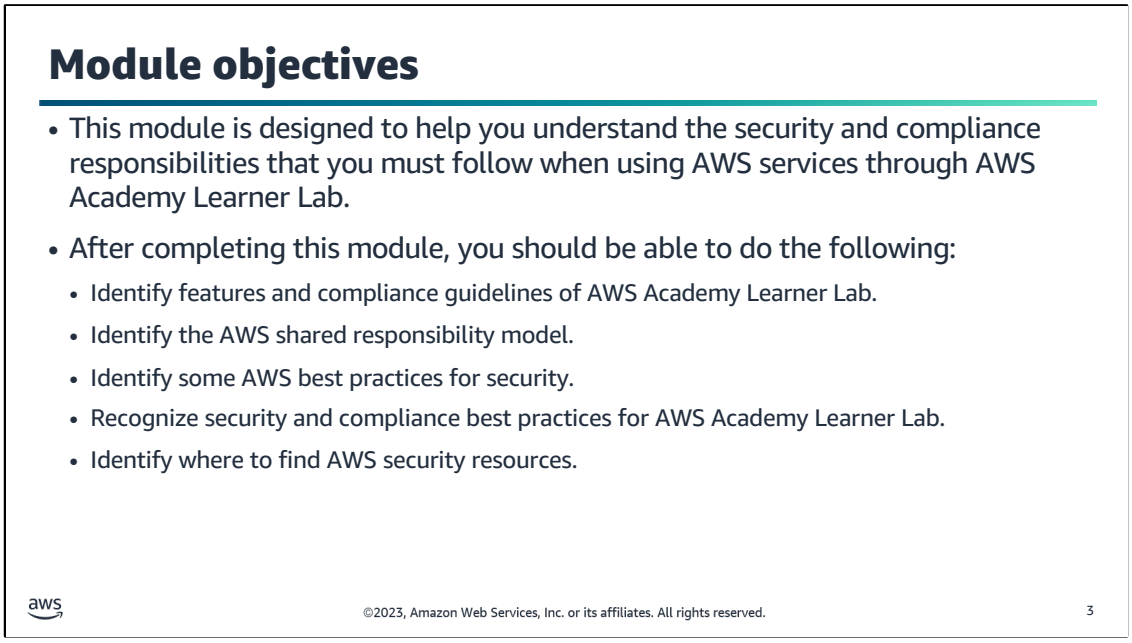


Welcome to the AWS Academy Learner Lab Compliance and Security module.
This module is designed to help you understand the security and compliance responsibilities that you must follow when using AWS services through AWS Academy Learner Lab.

This section provides an overview of the module objectives.



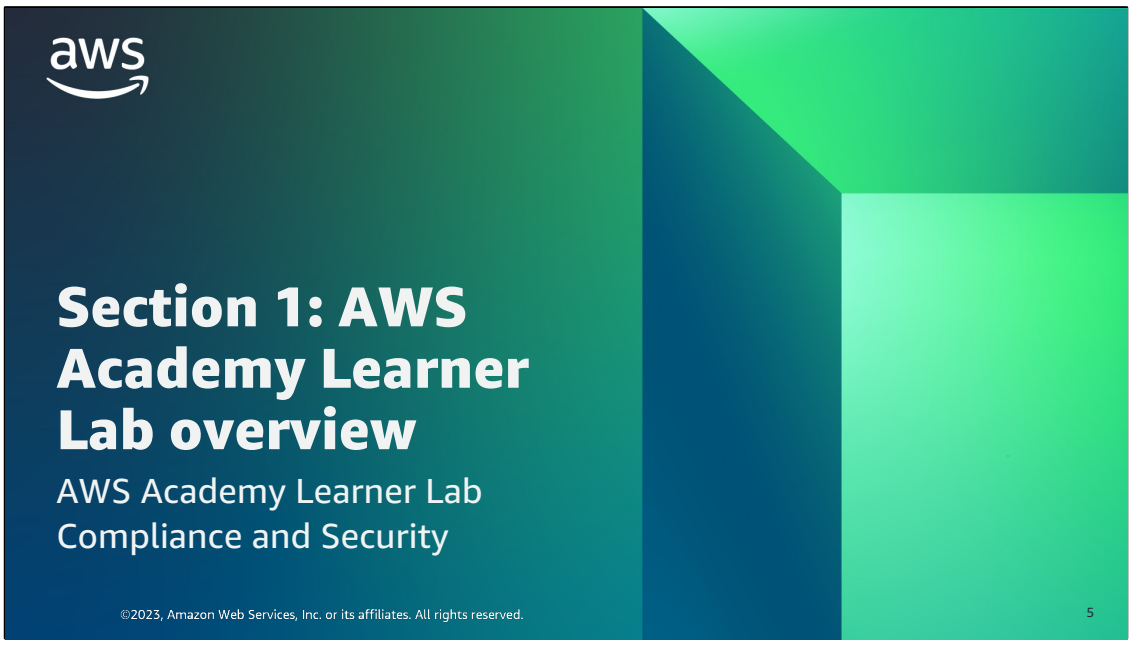
After completing this module, you should be able to do the following:

- Identify features and compliance guidelines of AWS Academy Learner Lab.
- Identify the AWS shared responsibility model.
- Identify some AWS best practices for security.
- Recognize security and compliance best practices for AWS Academy Learner Lab.
- Identify where to find AWS security resources.

Module overview

- Section 1: AWS Academy Learner Lab overview
- Section 2: AWS shared responsibility model
- Section 3: AWS security best practices
- Section 4: AWS Academy Learner Lab best practices
- Section 5: Additional resources

To achieve the module objectives, the module consists of the sections that are listed on the slide.



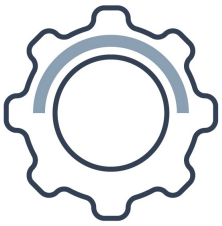
This section provides information about the Academy Learner Lab.

Features of AWS Academy Learner Lab

An AWS Academy Learner Lab provides a long-running sandbox environment to explore AWS services.

The environment has the following features:

- You can access a **restricted set of AWS services**.
- Data and resources that you create in the AWS account will be retained until the class end date.
- Each learner has a budget limit of $50 USD. If you exceed the budget, your lab account will be disabled, and all progress and resources will be lost.
- The session timer is 4 hours by default.



aws

An AWS Academy Learner Lab provides a long-running sandbox environment to explore AWS services. The environment has the following features:

- You can access a **restricted set of AWS services**.
- Data and resources that you create in the AWS account will be retained until the class end date.
- Each learner has a budget limit of $50 USD. If you exceed the budget, your lab account will be disabled, and all progress and resources will be lost.
- The session timer is 4 hours by default.

AWS Academy Learner Lab: Compliance (1 of 2)

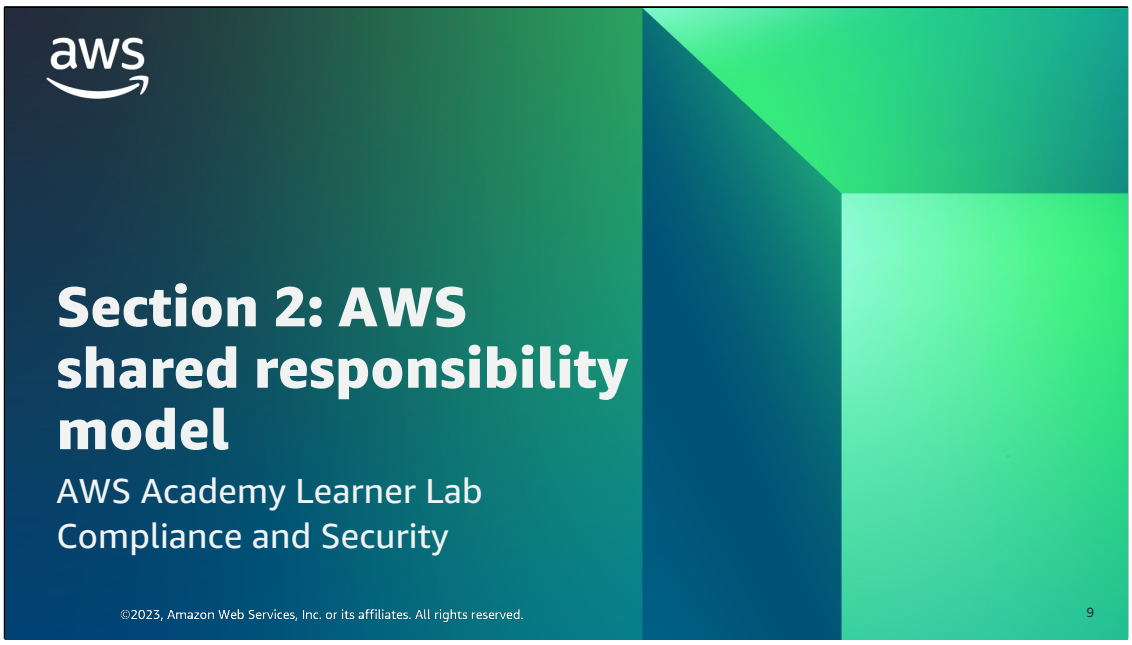
- All use of AWS Academy Learner Lab must comply with the AWS Acceptable Use Policy.
- AWS Academy conducts regular auditing and monitoring of the use of AWS Academy Learner Lab. Any educator or learner who uses AWS Academy Learner Lab and isn't compliant with the AWS Learner Terms and Conditions and the AWS Acceptable Use Policy will be subject to a deactivation notice in the AWS Academy program.

This section describes the features of the AWS Academy Learner Lab and provide information around compliance.

AWS Academy Learner Lab: Compliance (2 of 2)

- Exercise caution to prevent charges that will deplete your budget too quickly. If you exceed your budget, you will lose access to your environment and lose all of your work.
- Educators and learners must follow the AWS Best Practices for Security, Identity, & Compliance when using AWS Academy Learner Lab.
- Before using an AWS Academy Learner Lab, ensure that you do the following:
  - Complete this AWS Academy Learner Lab Compliance and Security module and the module assessment.
  - Read the AWS Academy Learner Lab Readme section.

This section describes the features of the AWS Academy Learner Lab and provide information around compliance.



This section provides information about the AWS shared responsibility model.

Image description: Shared responsibility model listing customer and AWS responsibilities. Customer is responsible for security in the cloud. This includes customer data. Platform, applications, identity and access management. Operating system, network, and firewall configuration. Client-side data encryption and data integrity, authentication. Server-side encryption of file system and data. Networking traffic protection, to include encryption, integrity, and identity. AWS is responsible for security of the cloud. This includes the AWS foundation services for compute, storage, databases, and networking. And the AWS Global Infrastructure, to include Regions, Availability Zones, and Edge Locations. **End of description.**

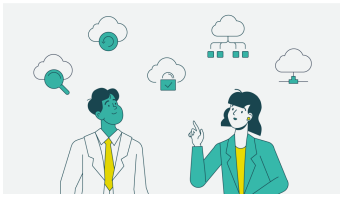
Security and compliance are shared responsibilities between AWS and customers. AWS operates, manages, and controls security *of* the cloud. This responsibility includes securing components, from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. AWS is responsible for protecting the global infrastructure that runs all the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

You assume responsibility and management *in* the cloud. The security steps that you must take depend on the services that you use and the complexity of your system. Customer responsibilities include selecting and securing operating systems that run on EC2 instances, and securing the applications that are launched on AWS resources. Customers must also select and handle security group configurations, firewall configurations, network configurations, and secure account management. Customers are also responsible for managing their data, including encryption options.

To reiterate, AWS secures the hardware, software, facilities, and networks that run all AWS products and services. You are responsible for what you implement by using AWS products and services, and for the applications that you connect to AWS. The security steps that you must take depend on the services that you use and the complexity of your system.

AWS shared responsibility model (2 of 3)

- Security and compliance are shared responsibilities between AWS and customers.
- AWS operates, manages, and controls **security *of* the cloud**. AWS is responsible for protecting the global infrastructure that runs all the services that are offered in the AWS Cloud.
- Customers are responsible for securing everything they put **in the cloud**, what they implement by using AWS products and services, and the applications that they connect to AWS.



Security and compliance are shared responsibilities between AWS and customers. AWS operates, manages, and controls security *of* the cloud. This responsibility includes securing components, from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. AWS is responsible for protecting the global infrastructure that runs all the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

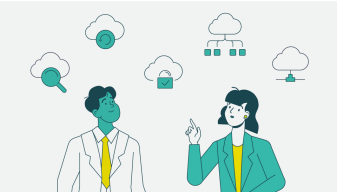
You assume responsibility and management *in* the cloud. The security steps that you must take depend on the services that you use and the complexity of your system. Customer responsibilities include selecting and securing operating systems that run on EC2 instances, and securing the applications that are launched on AWS resources. Customers must also select and handle security group configurations, firewall configurations, network configurations, and secure account management. Customers are also responsible for managing their data, including encryption options.

To reiterate, AWS secures the hardware, software, facilities, and networks that run all AWS products and services. You are responsible for what you implement by using AWS products and services, and for the applications that you connect to AWS. The security steps that you must take depend on the services that you use and the complexity of your system.

AWS shared responsibility model (3 of 3)

Customer responsibilities include the following:

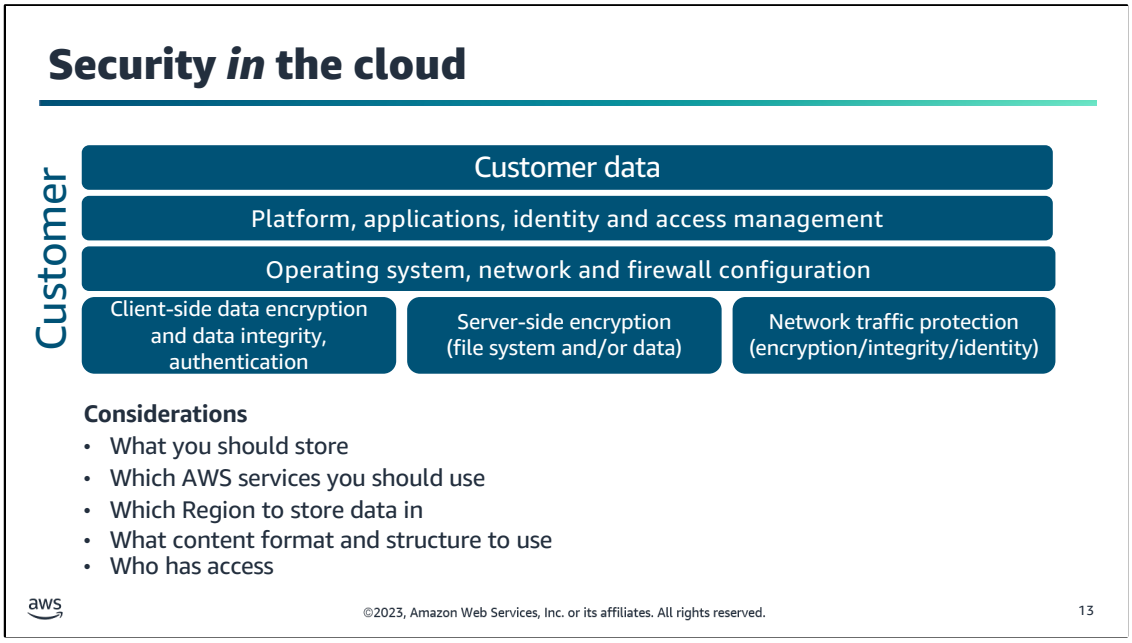
- Selecting and securing operating systems that run on EC2 instances
- Securing the applications that are launched on AWS resources
- Configuring security groups, firewalls, and network settings
- Securely managing accounts
- Managing their data, including encryption options



Security and compliance are shared responsibilities between AWS and customers. AWS operates, manages, and controls security *of* the cloud. This responsibility includes securing components, from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. AWS is responsible for protecting the global infrastructure that runs all the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

You assume responsibility and management *in* the cloud. The security steps that you must take depend on the services that you use and the complexity of your system. Customer responsibilities include selecting and securing operating systems that run on EC2 instances, and securing the applications that are launched on AWS resources. Customers must also select and handle security group configurations, firewall configurations, network configurations, and secure account management. Customers are also responsible for managing their data, including encryption options.

To reiterate, AWS secures the hardware, software, facilities, and networks that run all AWS products and services. You are responsible for what you implement by using AWS products and services, and for the applications that you connect to AWS. The security steps that you must take depend on the services that you use and the complexity of your system.



While AWS secures and maintains the cloud infrastructure, you are responsible for securing everything that you put *IN* the cloud.

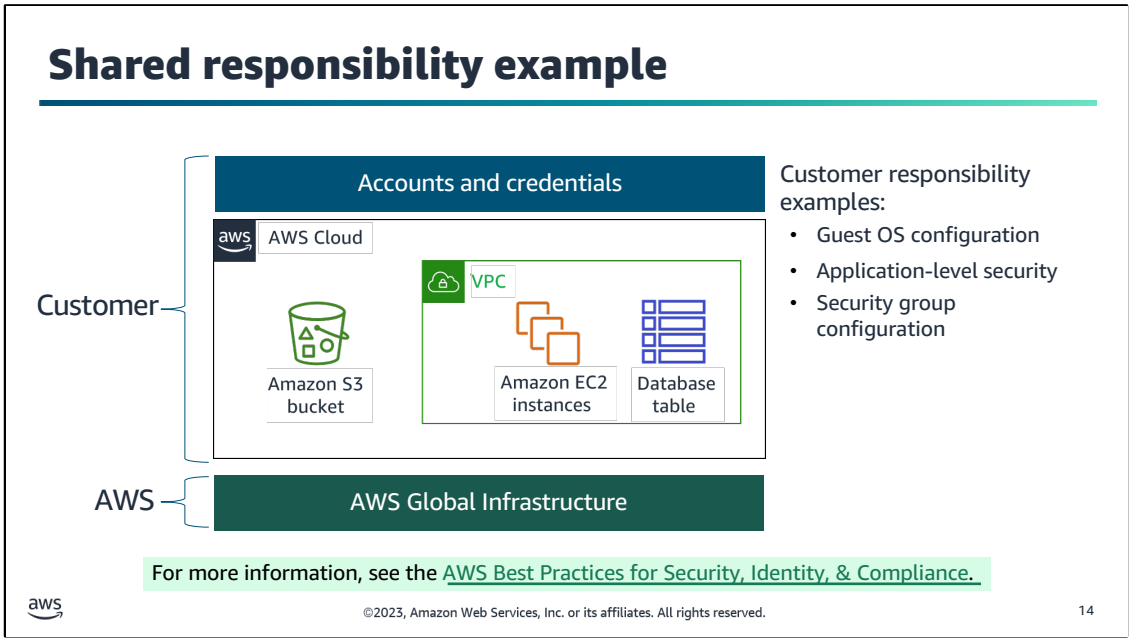
Before you architect any workload, you need to put practices in place that influence security. You will want to control who can do what. In addition, you want to be able to identify security incidents, protect your systems and services, and maintain the confidentiality and integrity of data through data protection. You should have a well-defined and practiced process to respond to security incidents. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

Because AWS physically secures the infrastructure that supports our cloud services, as an AWS customer you can focus on using services to accomplish your goals. The AWS Cloud also provides greater access to security data and an automated approach to respond to security events.

When using AWS services, you maintain complete control over your content and are responsible for managing critical security requirements, including the following:

- The content you choose to store on AWS
- The AWS services that are used with the content
- The country in which that content is stored
- The format and structure of that content, and whether it is masked, anonymized, or encrypted
- Who has access to that content, and how those access rights are granted, managed, and revoked

You retain control of what security you choose to implement to protect your own data, platform, applications, identity and access management, and operating system. This means that the shared responsibility model changes depending on the AWS services that you use.



Consider an example where your company uses Amazon S3 to store data. Your AWS environment also includes EC2 instances and an Amazon Relational Database Service (Amazon RDS) instance. These resources run a MySQL database, which is deployed inside a virtual private cloud (VPC). One EC2 instance hosts a web server, and the web application that runs on it uses the database to store application data.

In this scenario, AWS is responsible for protecting the global infrastructure, which contains the physical servers that host the virtual machines and storage hardware. These virtual machines and storage hardware host your S3 bucket, EC2 instances, and database instance. AWS is responsible for the security of the physical networking infrastructure that ensures that these components can be accessed. AWS is also responsible for the security of the hypervisor layer that hosts the EC2 instances. (The hypervisor is the host OS that runs the EC2 instances, which are virtual machines that run guest operating systems.)

You (the customer) are responsible for managing the guest OS that runs on the EC2 instances (including Microsoft Windows or Linux OS updates and security patches). You are also responsible for managing any application software or utilities that you install. Additionally, you are responsible for the configuration of the security groups that control network access to each EC2 instance and to the RDS database instance. You are also responsible for configuring security on the S3 bucket and the objects that you store in it. For example, you could use one or more of the security features that AWS provides, such as bucket policies, data encryption, and S3 Block Public Access.

For more information, see Shared Responsibility Model at https://aws.amazon.com/compliance/shared-responsibility-model.

This section provides information about some of the AWS security best practices.

Using VPCs to secure resources

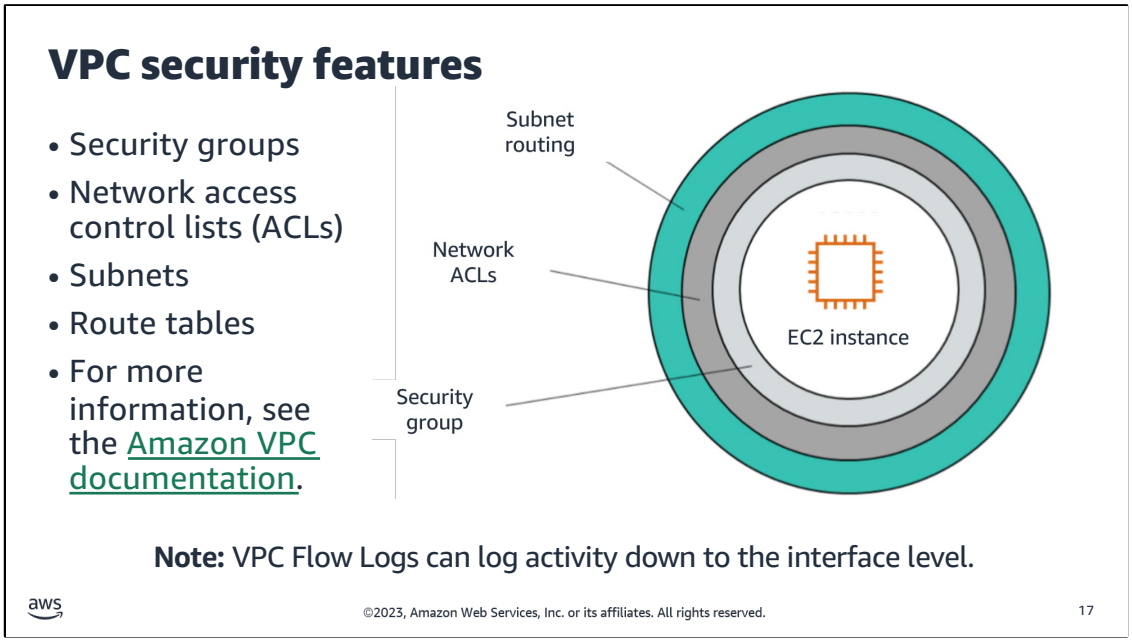


Image description: EC2 instance surrounded by layers of security. The closest layer to the instance is a security group. The next layer is network ACLs. The outside, and farthest layer, is subnet routing. **End of description.**

Virtual private cloud (VPC) security features include the following:

- Security groups act as virtual firewalls for your EC2 instances to control inbound and outbound traffic.
- Network access control lists (ACLs) provide an optional layer of security for your VPC. They act as firewalls to control traffic in and out of one or more subnets.
- Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.
- Route tables control where network traffic is directed.

With the VPC Flow Logs feature, you can capture information about the IP traffic going to and from network interfaces in your VPC. You can publish flow log data to Amazon CloudWatch Logs or Amazon Simple Storage Service (Amazon S3). After you create a flow log, you can retrieve and view its data in the chosen destination.

You can create a flow log for a VPC, subnet, or network interface. If you create a flow log for a subnet or VPC, each network interface in that subnet or VPC is monitored. Flow log data for a monitored network interface is recorded as *flow log records*, which are log events consisting of fields that describe the traffic flow.

For more information, see Logging IP Traffic Using VPC Flow Logs in the *Amazon VPC User Guide* at https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html.

Setting up subnets and route tables

- Public subnets are used when external traffic needs to reach an interface, such as an EC2 instance.
- Private subnets are often used to host database instances that don't need to be accessed through the public internet.
- Route tables determine where traffic is routed in your VPC.

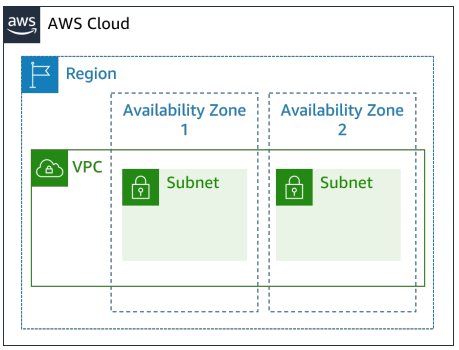


Image description: Diagram of subnets in a VPC. A Region within the AWS Cloud has one VPC, which spreads across two Availability Zones. The VPC has one subnet in each Availability Zone. **End of description.**

Using network ACLs

- A network access control list (ACL) is an optional layer of security for your VPC and acts as a firewall to control traffic at the subnet level.
- Each subnet in your VPC must be associated with a network ACL.
- Network ACLs are stateless, which means that responses to inbound traffic are subject to the rules for outbound traffic (and the reverse).
- Rules are evaluated in number order before a decision is made to allow traffic.
- For more information, see Control Traffic to Subnets Using Network ACLs.

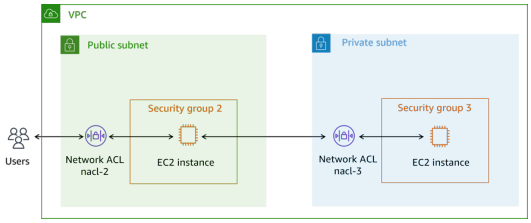


Image description: Diagram showing how network ACLs work. A VPC contains a public subnet and a private subnet. Each subnet contains an EC2 instance. A network ACL in each subnet controls traffic to and from the instances. **End of description.**

Using security groups

- A security group acts as a virtual firewall for an instance to control inbound and outbound traffic.
- Security groups are stateful, which means that state information is kept even after a request is processed.
- All rules are evaluated before a decision is made to allow traffic.

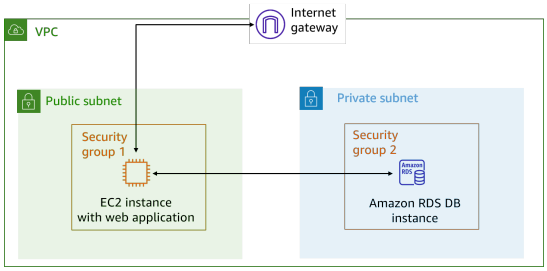


Image description: Diagram of a VPC with a public subnet and a private subnet. The public subnet contains an EC2 instance that is protected by security group 1. The private subnet contains an Amazon Relational Database Service (Amazon RDS) database instance that is protected by security group 2. Communication is allowed between the two security groups, and the internet can communicate with security group 1. **End of description.**

Best practices to protect your network

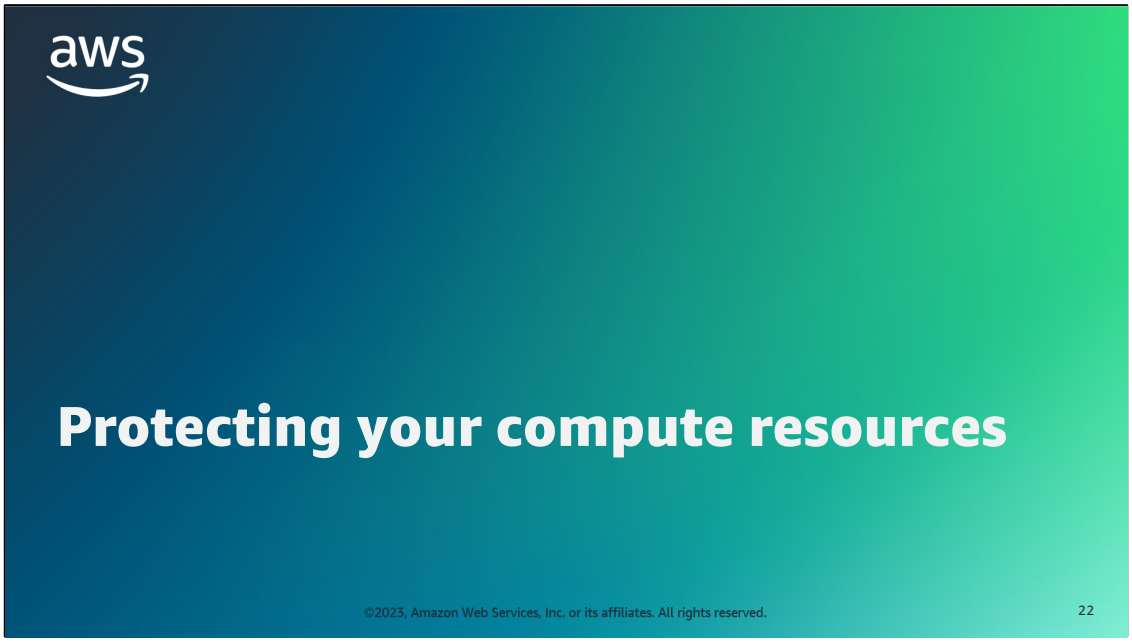
- Apply controls for both inbound and outbound traffic.
- Use subnets in multiple Availability Zones to separate layers of your application.
- Configure security groups and network ACLs to only allow the necessary inbound and outbound traffic.
- Inspect and filter your traffic at the application level.
- Automate network protection.
- Limit exposure by only allowing the minimum required access.
- For more information, see How Do You Protect Your Network Resources?
- Review the AWS Best Practices for Security, Identity, & Compliance.

One of the best practices to protect your network is to apply controls for both inbound and outbound traffic. For a VPC, this includes using security groups, network ACLs, and subnets. Use subnets in multiple Availability Zones to separate layers of your application. Configure security groups and network ACLs to only allow the necessary inbound and outbound traffic.

Another best practice is to inspect and filter network traffic at the application level.

In addition, use threat intelligence and anomaly detection to automate protection mechanisms to provide a self-defending network.

Finally, limit the exposure of the workload to the internet and internal networks by only allowing the minimum required access.



Security in Amazon EC2

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. To learn about the compliance programs that apply to Amazon EC2, see AWS Services in Scope by Compliance Program.
Security *in* the cloud	Your responsibility includes the following: • Controlling network access to your instances, for example, through configuring your VPC and security groups. For more information, see Controlling Network Traffic. • Managing the credentials that are used to connect to your instances. • Managing the guest operating system and software that is deployed to the guest operating system, including updates and security patches. For more information, see Update Management in Amazon EC2. • Configuring the IAM roles that are attached instances and the permissions that are associated with those roles. For more information, see IAM Roles for Amazon EC2.

Authorize inbound traffic for your Windows instances

By using a security group, you can control traffic to an instance, such as specifying the type of traffic that can reach the instance.

Follow these steps:

1. Decide who requires access to your instance; for example, a single host or a specific network that you trust, such as your local computer's public IPv4 address.
2. Follow the AWS documentation to learn how to add a rule for inbound **RDP** traffic to a **Windows** instance.
3. Assign a security group to an instance.

Warning
If you use `0.0.0.0/0`, you enable all IPv4 addresses to access your instance using RDP. If you use `::/0`, you enable all IPv6 addresses to access your instance. You should authorize only a specific IP address or range of addresses to access your instance.

Authorize inbound traffic for your Linux instances

By using a security group, you can control traffic to an instance, such as specifying the type of traffic that can reach the instance.

Follow these steps:

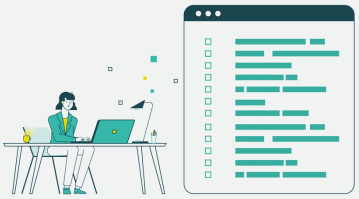
1. Decide who requires access to your instance; for example, a single host or a specific network that you trust, such as your local computer's public IPv4 address.
2. Follow the AWS documentation to learn how to add a rule for inbound **SSH** traffic to a **Linux** instance.
3. Assign a security group to an instance.

Warning
If you use `0.0.0.0/0`, you enable all IPv4 addresses to access your instance using SSH. If you use `::/0`, you enable all IPv6 addresses to access your instance. You should authorize only a specific IP address or range of addresses to access your instance.

Best practices for building AMIs (1 of 2)

Use the following guidelines when you build an Amazon Machine Image (AMI):

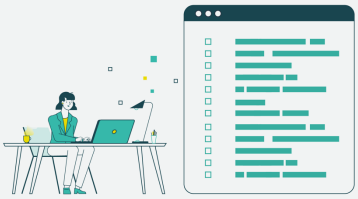
- Ensure that your AMI meets all AWS Marketplace policies, including disabling root login.
- Create your AMI in the US East (N. Virginia) Region.
- Create products from existing, well-maintained AMIs that are backed by Amazon Elastic Block Store (Amazon EBS) with a clearly defined lifecycle and provided by trusted, reputable sources, such as AWS Marketplace.
- Build AMIs using the most up-to-date operating systems, packages, and software.
- Ensure that all AMIs start with a public AMI that uses hardware virtual machine (HVM) virtualization and 64-bit architecture.



For more information, see Best Practices for Building AMIs.

Best practices for building AMIs (2 of 2)

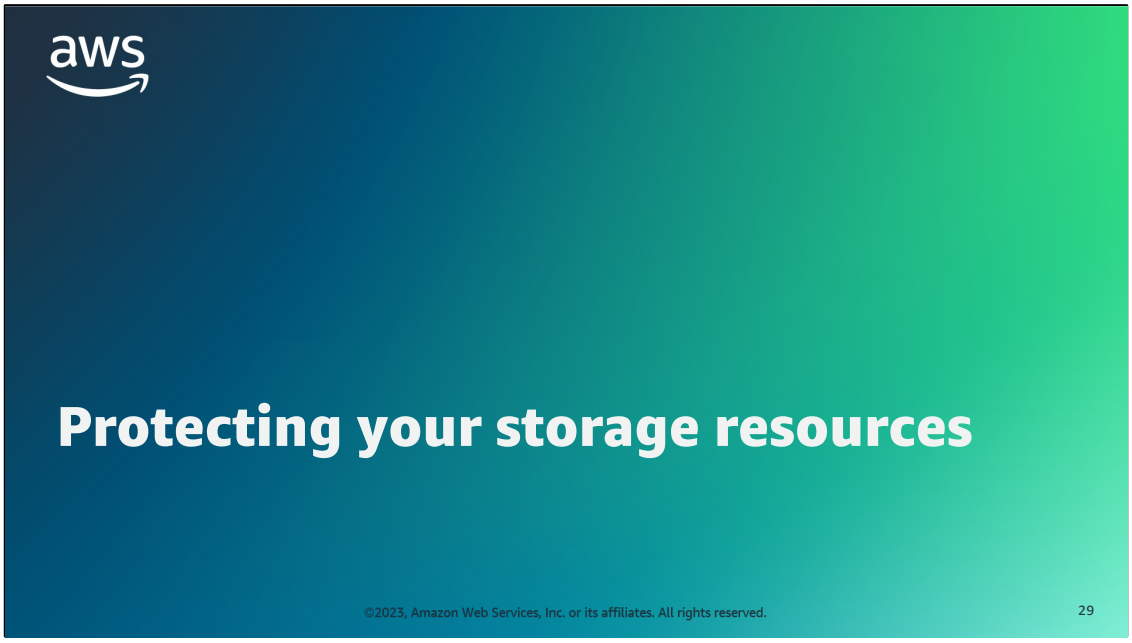
- Develop a repeatable process to build, update, and republish AMIs.
- Use a consistent operating system username across all versions and products. AWS recommends **ec2-user**.
- Configure a running instance from your final AMI to the end-user experience that you want. Test all installation methods, features, and performance before submission to AWS Marketplace.
- Check port settings as follows:
  - Linux-based AMIs: Ensure that a valid SSH port is open. The default SSH port is 22.
  - Windows-based AMIs: Ensure that an RDP port is open. The default RDP port is 3389.

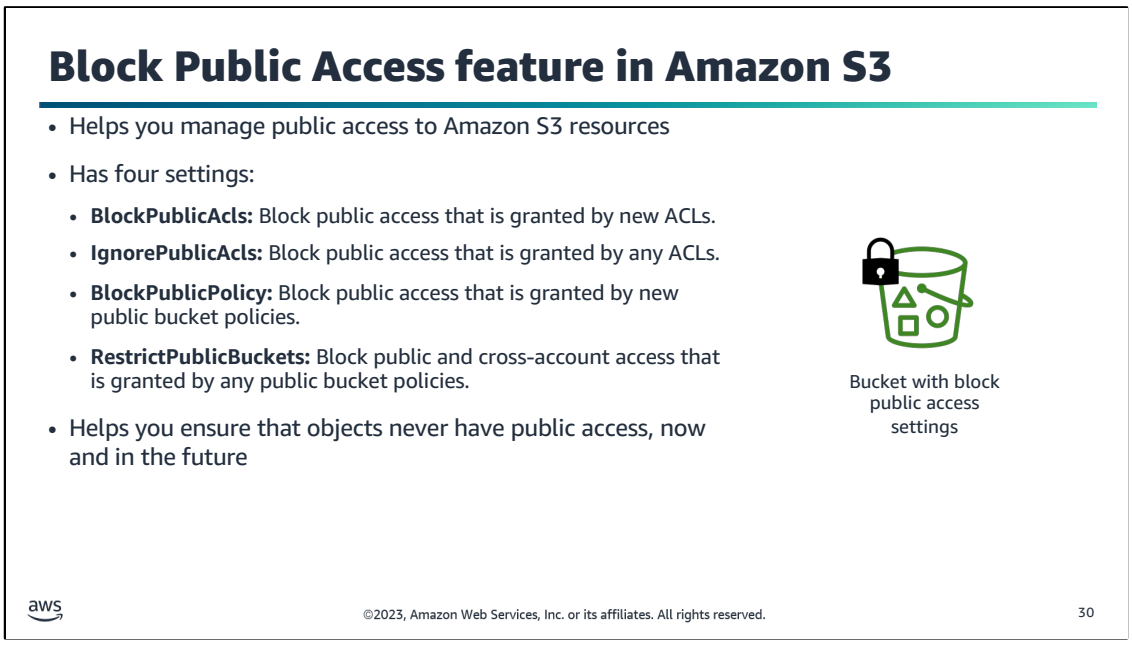


For more information, see Best Practices for Building AMIs.

Best practices to protect your compute resources

- Scan your compute resources regularly for vulnerabilities, and patch them accordingly. You can automate this task by using AWS services such as AWS Lambda and AWS Systems Manager.
- Anyone who possesses your private key can connect to your instances, so it's important that you store your private key in a secure place.
- For more information, see the AWS Best Practices for Security, Identity, & Compliance.





Amazon S3 provides a number of security features to consider as you develop and implement your own security policies. Amazon S3 provides the Block Public Access feature to help you manage public access to S3 resources. By default, new buckets and objects don't allow public access, but users can modify bucket policies or object permissions to allow public access. S3 Block Public Access provides settings that override these policies and permissions so that you can limit public access to these resources.

This feature provides four settings:

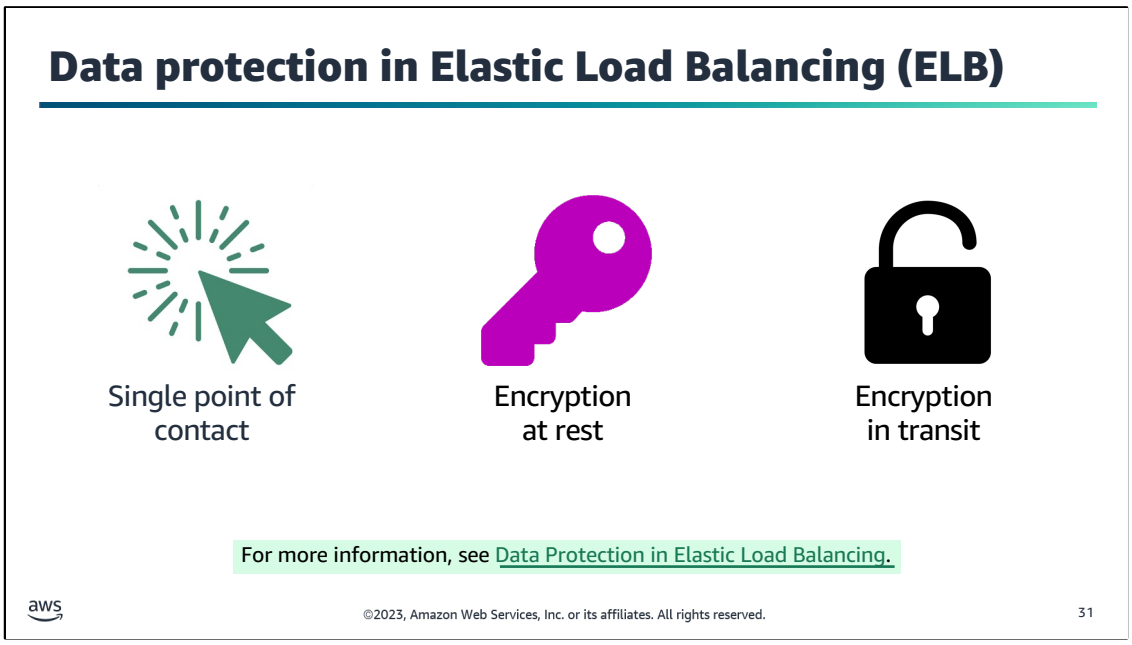
- **BlockPublicAcls:** Prevent any new operations to make buckets or objects public through bucket or object ACLs. Existing policies and ACLs for buckets and objects are not modified.
- **IgnorePublicAcls:** Ignore all public ACLs on a bucket and any objects that it contains.
- **BlockPublicPolicy:** Reject calls to PUT a bucket policy if the specified bucket policy allows public access. (Enabling this setting doesn't affect existing bucket policies.)
- **RestrictPublicBuckets:** Restrict access to a bucket with a public policy to only AWS services and authorized users within the bucket owner's account.

These settings are independent and can be used in any combination. You can apply each setting to an access point, a bucket, or an entire AWS account. You cannot apply these settings on a per-object basis. If the block public access settings for the access point, bucket, or account differ, then Amazon S3 applies the most restrictive combination of the access point, bucket, and account settings.

When Amazon S3 receives a request to access a bucket or an object, the service determines whether the bucket or the bucket owner's account has a block public access setting applied. If an existing block public access setting prohibits the requested access, Amazon S3 rejects the request.

In addition to these settings, the Amazon S3 console highlights your publicly accessible buckets, indicates the source of public accessibility, and also warns you if changes to your bucket policies or bucket ACLs would make your bucket publicly accessible.

For more information, see Blocking Public Access to Your Amazon S3 Storage in the *Amazon Simple Storage Service User Guide* at https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html.



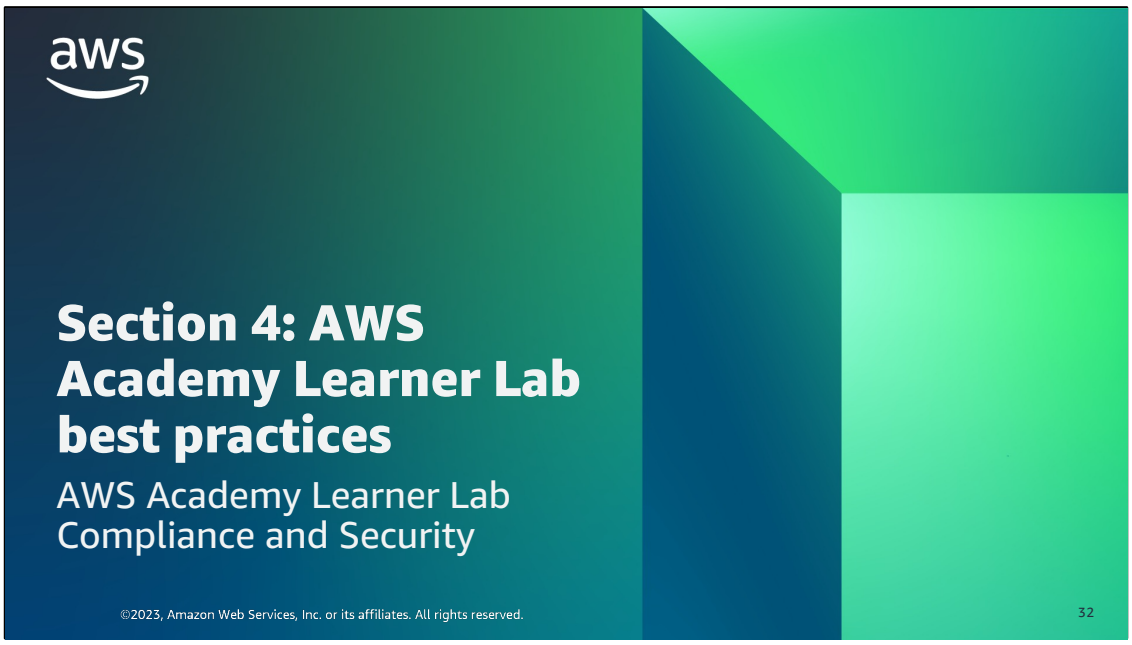
Single point of contact: A load balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application.

An Application Load Balancer can sustain secure HTTPS communication and certificates for communications with clients. It can optionally terminate the SSL connection at the load balancer level so that you don't need to handle certificates in your own application.

Encryption at rest: If you enable server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for your S3 bucket for ELB access logs, ELB automatically encrypts each access log file before it is stored in your S3 bucket. ELB also decrypts the access log files when you access them. Each log file is encrypted with a unique key, which is itself encrypted with a key that is regularly rotated.

Encryption in transit: ELB simplifies the process of building secure web applications by terminating HTTPS and TLS traffic from clients at the load balancer. The load balancer performs the work of encrypting and decrypting the traffic, instead of requiring each EC2 instance to handle the work for TLS termination.

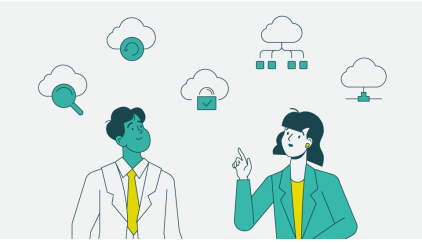
For more information, see Data Protection in Elastic Load Balancing in the ELB User Guide at https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/data-protection.html.



This section provides information about the AWS Academy Learner Lab best practices.

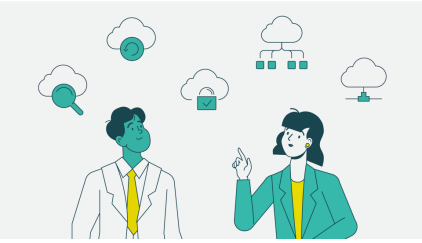
Best practices for AWS Academy Learner Lab

- Use the allowed Regions. All service access is limited to the us-east-1 and us-west-2 Regions, unless mentioned otherwise in the service details.
- A role named **LabRole** has been pre-created for you. This role is designed to be used when you want to attach a role to a resource in an AWS service:
  - The role grants many AWS services access to other AWS services and has permissions that are similar to the permissions that you have as a user in the AWS Management Console.
  - To avoid permissions errors, choose **LabRole** whenever you are prompted to specify a role.

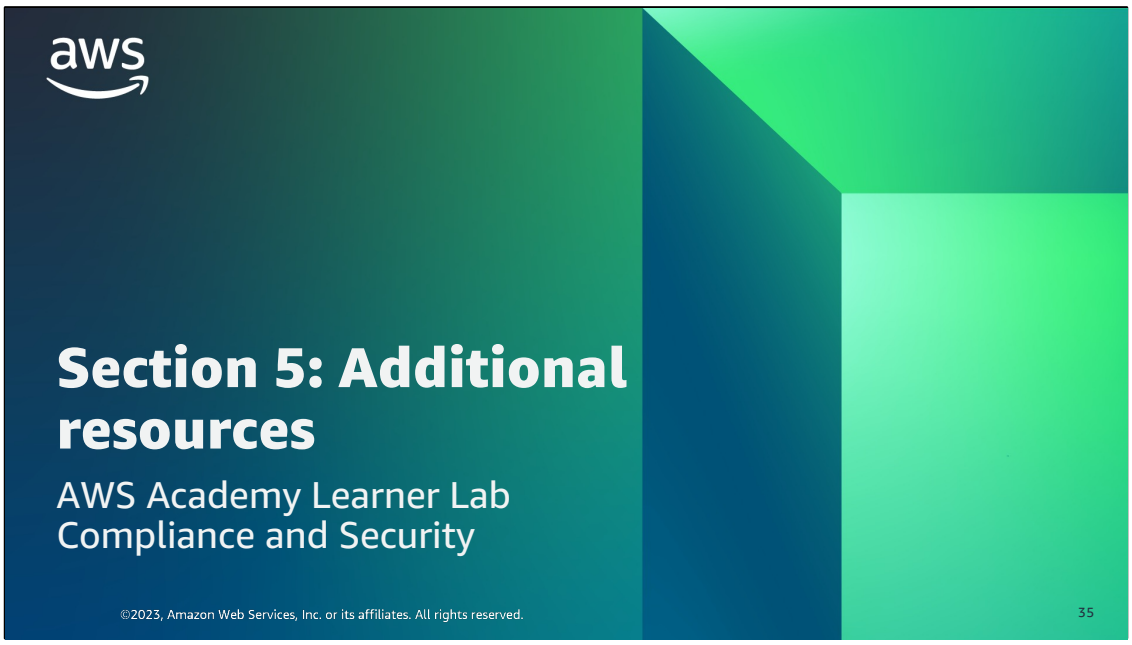


Best practices to preserve your budget

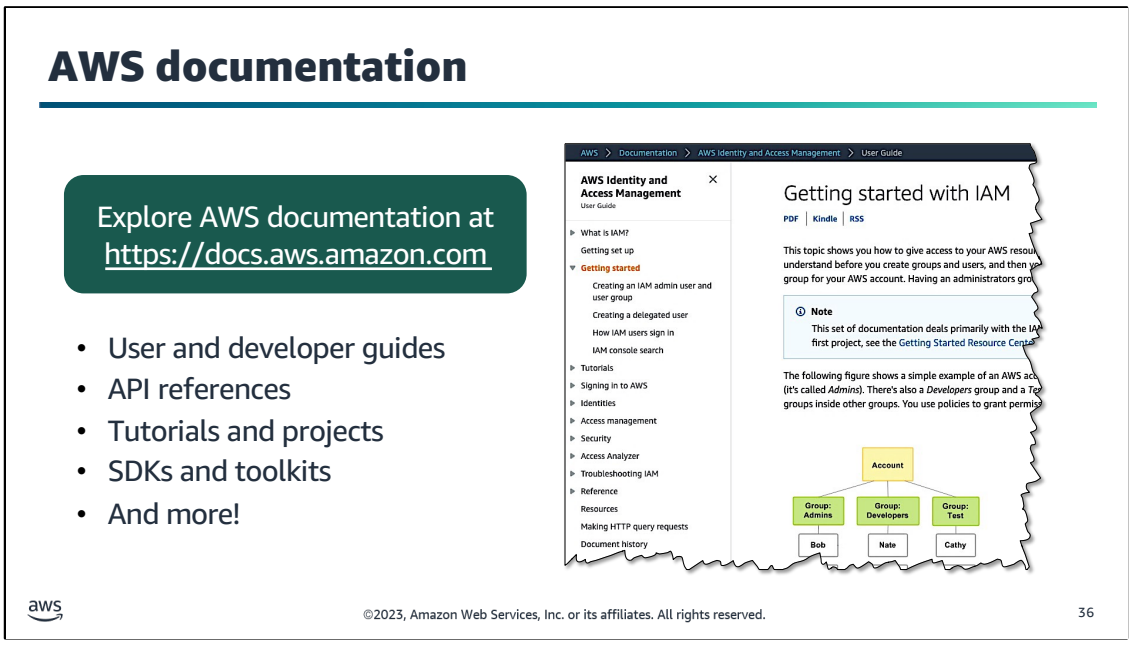
- Launch only the number of instances that you need, and size them to your requirements.
- Turn off or delete compute resources when you no longer need them.
- Use the AWS Pricing Calculator to estimate cost.
- Access AWS Trusted Advisor and review the cost optimization results.
- Check the AWS Academy Learner Lab Readme for more information.



If you exceed your lab budget, your lab account will be disabled, and all progress and resources will be lost.



This section provides information about AWS additional resources.



To access AWS user and developer guides, API references, tutorials and projects, SDKs and toolkits, and other resources, see AWS documentation at https://docs.aws.amazon.com.

Each AWS service developer guide contains a **Getting started** section with step-by-step tutorials that can help to familiarize you with the service.

Security pillar of the AWS Well-Architected Framework

- One of the six pillars of the AWS Well-Architected Framework
- Provides guidance to help you apply best practices and current recommendations to design, deliver, and maintain secure AWS workloads

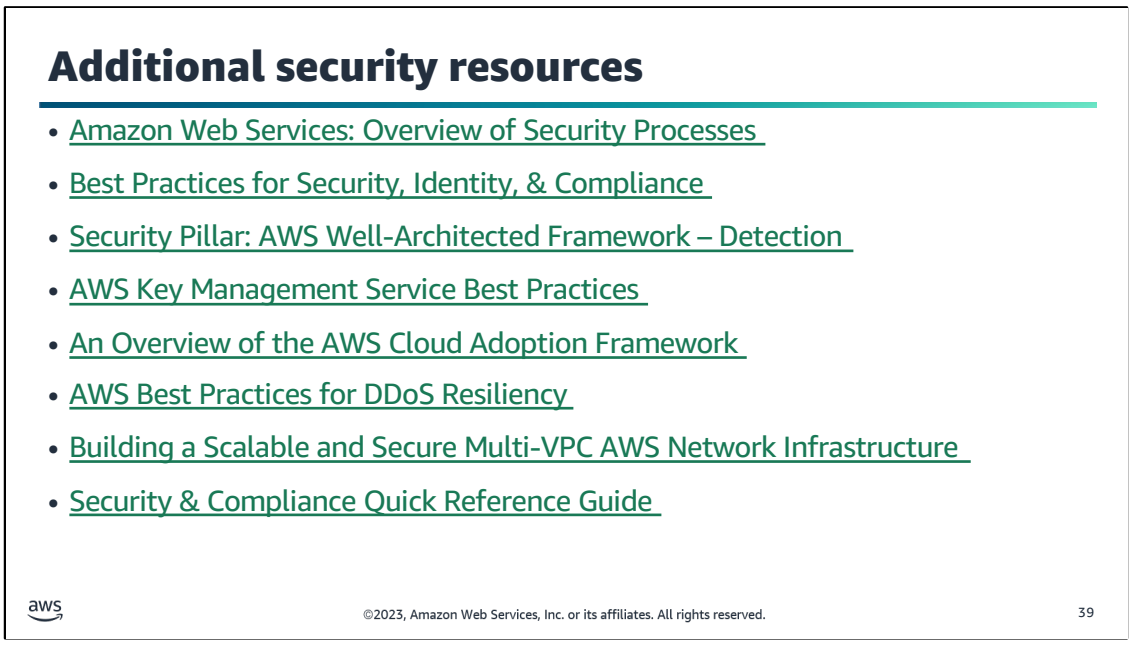
The security pillar of the AWS Well-Architected Framework provides guidance to help you apply best practices and current recommendations in the design, delivery, and maintenance of secure AWS workloads. It will assist you in understanding AWS current recommendations and strategies that you can use when designing cloud architectures with security in mind.

For more information, see Security Pillar: AWS Well-Architected Framework at https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html.

Build your technical skills with the following recommended courses:

- AWS Academy Cloud Security Foundations: https://aws.amazon.com/training/awsacademy
- AWS Security Fundamentals (Digital): https://explore.skillbuilder.aws/learn/course/external/view/elearning/48/aws-security-fundamentals-second-edition
- Getting Started with AWS Security, Identity, and Compliance (Digital): https://explore.skillbuilder.aws/learn/course/external/view/elearning/101/getting-started-with-aws-security-identity-and-compliance
- Introduction to AWS Identity and Access Management (IAM) (Digital): https://explore.skillbuilder.aws/learn/course/external/view/elearning/120/introduction-to-aws-identity-and-access-management-iam
- Introduction to Amazon Virtual Private Cloud (VPC) (Digital): https://explore.skillbuilder.aws/learn/course/external/view/elearning/79/introduction-to-amazon-virtual-private-cloud-vpc
- Securing and Protecting Your Data in Amazon Simple Storage Service (Amazon S3) (Digital): https://explore.skillbuilder.aws/learn/course/external/view/elearning/4892/securing-and-protecting-your-data-in-amazon-simple-storage-service-amazon-s3
- AWS Security Governance at Scale (Classroom): https://aws.amazon.com/training/classroom/aws-security-governance-at-scale
- AWS Security Best Practices: Monitoring and Alerting (Digital): https://explore.skillbuilder.aws/learn/course/external/view/elearning/11264/aws-security-best-practices-monitoring-and-alerting

For more information about AWS training for security professionals, see the security training page at https://aws.amazon.com/training/learn-about/security.



The following additional resources might be helpful for study and review:

- Amazon Web Services: Overview of Security Processes: https://docs.aws.amazon.com/whitepapers/latest/aws-overview-security-processes/aws-overview-security-processes.pdf
- Best Practices for Security, Identity, & Compliance: Security at Scale: https://aws.amazon.com/architecture/security-identity-compliance
- Security Pillar: AWS Well-Architected Framework – Detection: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/detection.html
- AWS Key Management Service Best Practices: https://d1.awsstatic.com/whitepapers/aws-kms-best-practices.pdf
- An Overview of the AWS Cloud Adoption Framework: https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/welcome.html
- AWS Best Practices for DDoS Resiliency: https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
- Building a Scalable and Secure Multi-VPC AWS Network Infrastructure: https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/building-scalable-secure-multi-vpc-network-infrastructure.pdf
- Security & Compliance Quick Reference Guide: https://d1.awsstatic.com/whitepapers/compliance/AWS_Compliance_Quick_Reference.pdf

Complete the knowledge check

It is now time to complete the knowledge check for this module.