Question 21

Which AWS service enables you to view, analyze, and alert on logs, metrics, and events from your infrastructure deployed on AWS?

A. Amazon Logs
B. Amazon Elastic Block Store (EBS)
C. Amazon CloudWatch
D. AWS Identity and Access Management (IAM)

Question 22

Your company utilizes resource tags to properly attribute expenses to specific applications and departments. This data then allows your organization to analyze all AWS spending by these categories. Which pillar of the AWS Well-Architected Framework recommends this approach?

A. Cost Optimization
B. Security
C. Reliability
D. Operational Efficiency

Question 23

What features of Virtual Private Clouds (VPC's) enable you to limit access to your network? (select two)

A. Network Load Balancers
B. AWS CloudFormation
C. Security Groups
D. Network Access Control Lists (ACL's)
E. Amazon EBS Volumes

Question 24

Which service provides a global content delivery network (CDN) that leverages the edge locations in the AWS Global Infrastructure to enable reduced latency when sending content to end users?

A. AWS Content Delivery
B. Amazon CloudFormation
C. Amazon Content Network
D. Amazon CloudFront

Question 25

Which tool would enable you to check if you are following AWS best practices for cost optimization on your current workloads?

A. AWS Trusted Advisor
B. AWS Pricing Calculator or Simple Monthly Calculator
C. Cost and Usage Reports (CUR)
D. AWS Cost Explorer

Question 26

Your organization is two months into a cloud transition, and a majority of systems have been migrated. Based on your current workload, you want to visualize current spend by AWS service as well as predicting future costs for this workload. What tool should you leverage?

A. TCO Calculator
B. AWS Cost Explorer
C. AWS Pricing Calculator
D. Cost and Usage Reports (CUR)

Question 27

Which of the following is an economic benefit of leveraging the cloud?

A. Elimination of variable operational expenditures (opex)
B. Variable operational expenditures (opex) are tied to usage
C. Increased up front capitalized expenditures (capex)
D. Variable operational expenditures (opex) costs are unrelated to usage

Question 28

Which managed AWS service enables you to leverage your own encryption keys for your data with AWS services?

A. AWS GuardDuty
B. AWS Identity and Access Management (IAM)
C. AWS Key Management Service (KMS)
D. Amazon Macie

Question 29

Where can organizations find pre-configured software from independent software vendors to run in their AWS environments?

A. AWS Marketplace
B. AWS CloudFormation
C. Amazon CloudFront
D. AWS SaaS Factory

Question 30

Which of the following services is considered global (and not region-specific)?

A. AWS Direct Connect
B. Amazon Route 53
C. AWS CloudFormation
D. Amazon S3

Question 61

Your organization has refactored an application that was migrated from your data center to the cloud. The application can now automatically allocate new resources to meet user demand. What benefit of the cloud is illustrated in this scenario?

A. Fault Tolerance
B. Elasticity
C. Agility
D. High Availability

Question 62

Which AWS service enables you to create a logically isolated virtual network that you can define and configure?

A. Amazon Virtual Private Cloud (VPC)
B. AWS Elastic Beanstalk
C. Amazon CloudWatch
D. Amazon Elastic Network

Question 63

Recently your organization launched a new database using Amazon RDS. You chose to deploy the database across multiple availability zones to ensure the database could still function even if an availability zone went down. Which architectural principle does this illustrate?

A. Loose coupling
B. Tight coupling
C. Cost optimization
D. High availability

Question 65

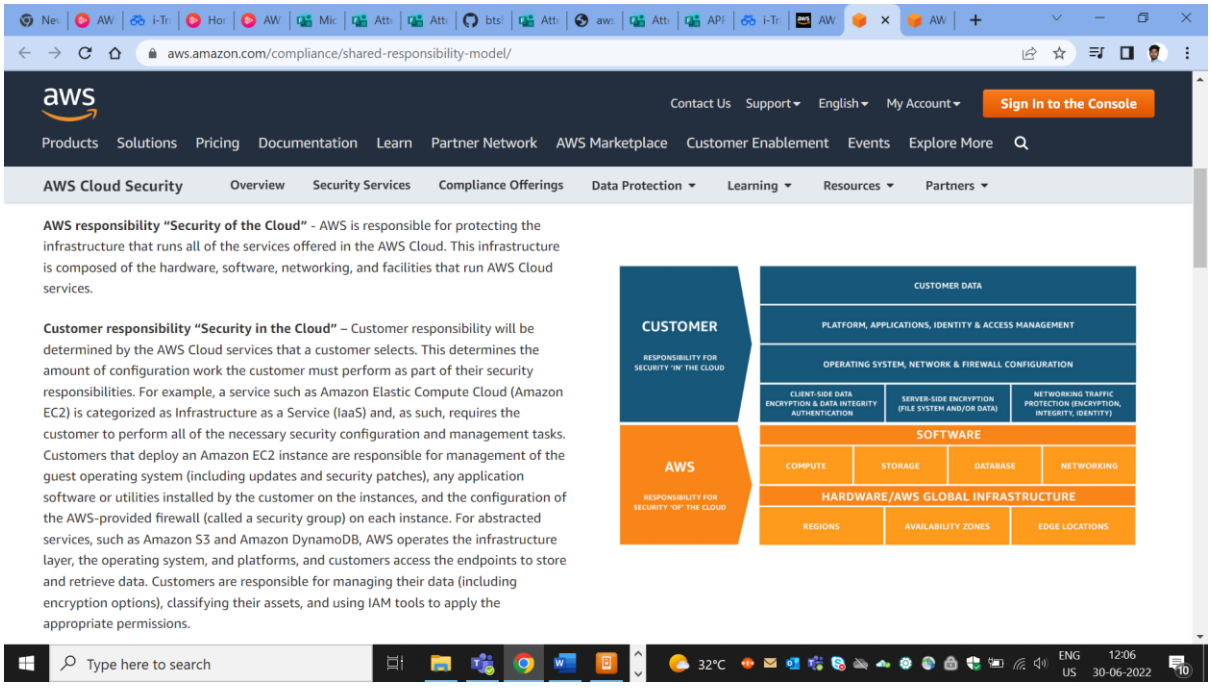
Your company wants to ensure that they have phone, chat, and email access to AWS support with a response within 1 hour when a production system is down. What is the minimum level of support that would meet this criteria?

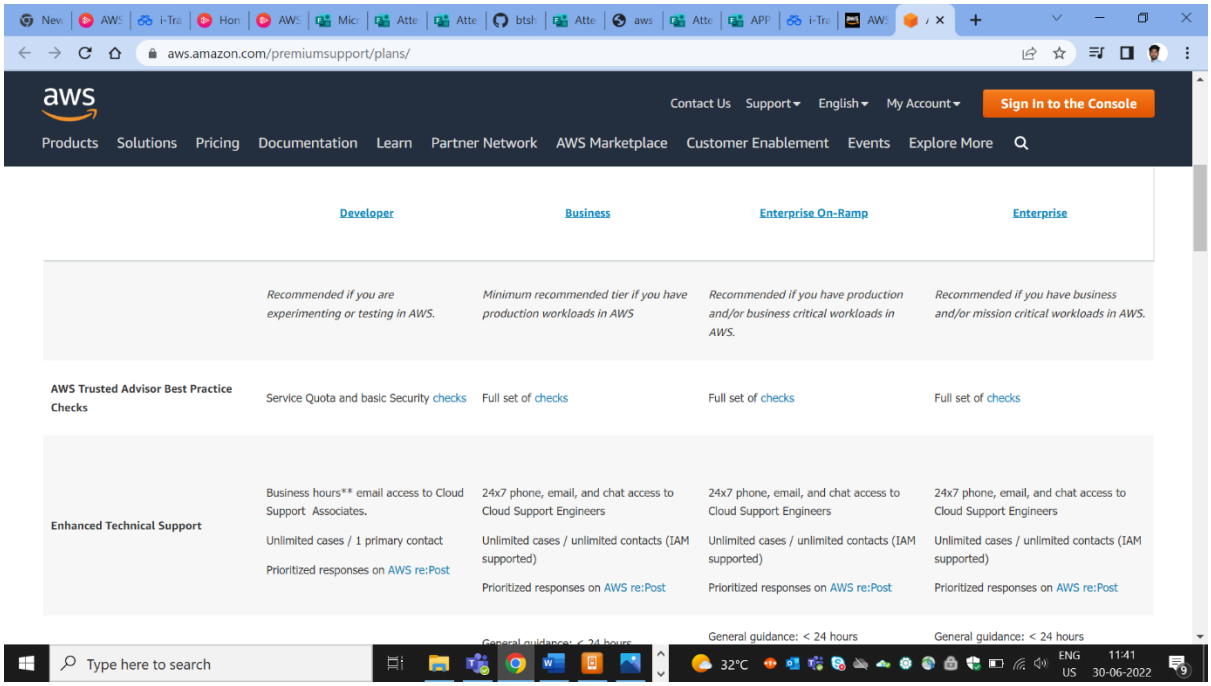
A. Business
B. Enterprise
C. Basic
D. Developer

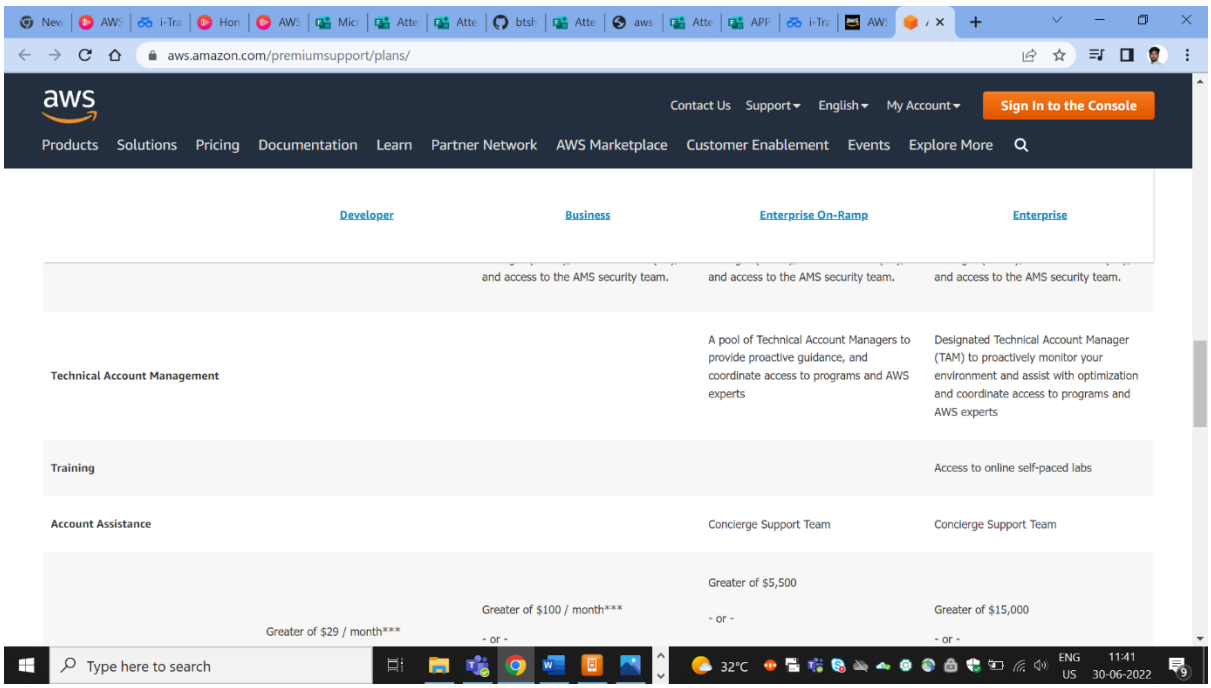
Question 1

Your organization has decided to adopt "infrastructure as code" with AWS CloudFormation for new infrastructure launched into your AWS accounts. Which pillar of the Well-Architected Framework is this recommendation included in?

A. Operational Excellence
B. Security
C. Fault Tolerance
D. Cost Optimization




aws.amazon.com/premiumsupport/plans/
aws
Contact Us
Support
English
My Account
Sign In to the Console
Products
Solutions
Pricing
Documentation
Learn
Partner Network
AWS Marketplace
Customer Enablement
Events
Explore More
Developer
Business
Enterprise On-Ramp
Enterprise
Recommended if you are experimenting or testing in AWS.
Minimum recommended tier if you have production workloads in AWS
Recommended if you have production and/or business critical workloads in AWS.
Recommended if you have business and/or mission critical workloads in AWS.
AWS Trusted Advisor Best Practice Checks
Service Quota and basic Security checks
Full set of checks
Full set of checks
Full set of checks
Enhanced Technical Support
Business hours** email access to Cloud Support Associates.
Unlimited cases / 1 primary contact
Prioritized responses on AWS re:Post
24x7 phone, email, and chat access to Cloud Support Engineers
Unlimited cases / unlimited contacts (IAM supported)
Prioritized responses on AWS re:Post
24x7 phone, email, and chat access to Cloud Support Engineers
Unlimited cases / unlimited contacts (IAM supported)
Prioritized responses on AWS re:Post
24x7 phone, email, and chat access to Cloud Support Engineers
Unlimited cases / unlimited contacts (IAM supported)
Prioritized responses on AWS re:Post
General guidance: < 24 hours
General guidance: < 24 hours
Type here to search
32°C
ENG
US
11:41
30-06-2022


aws.amazon.com/premiumsupport/plans/
aws
Contact Us
Support
English
My Account
Sign In to the Console
Products
Solutions
Pricing
Documentation
Learn
Partner Network
AWS Marketplace
Customer Enablement
Events
Explore More
Developer
Business
Enterprise On-Ramp
Enterprise
and access to the AMS security team.
and access to the AMS security team.
and access to the AMS security team.
Technical Account Management
A pool of Technical Account Managers to provide proactive guidance, and coordinate access to programs and AWS experts
Designated Technical Account Manager (TAM) to proactively monitor your environment and assist with optimization and coordinate access to programs and AWS experts
Training
Access to online self-paced labs
Account Assistance
Concierge Support Team
Concierge Support Team
Greater of $29 / month***
Greater of $100 / month***
- or -
Greater of $5,500
- or -
Greater of $15,000
- or -
Type here to search
32°C
ENG
US
11:41
30-06-2022

aws.amazon.com/compliance/shared-responsibility-model/

Contact Us | Support | English | My Account | Sign In to the Console

Products | Solutions | Pricing | Documentation | Learn | Partner Network | AWS Marketplace | Customer Enablement | Events | Explore More

AWS Cloud Security | Overview | Security Services | Compliance Offerings | Data Protection | Learning | Resources | Partners

Inherited Controls – Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

Customer Specific – Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

Applying the AWS Shared Responsibility Model in Practice

Once a customer understands the AWS Shared Responsibility Model and how it generally applies to operating in the cloud, they must determine how it applies to their use case. Customer responsibility varies based on many factors, including the AWS services and Regions they choose, the integration of those services into their IT environment, and the laws and regulations applicable to their organization and workload.

Type here to search

32°C ENG US 12:06 30-06-2022

aws.amazon.com/compliance/shared-responsibility-model/

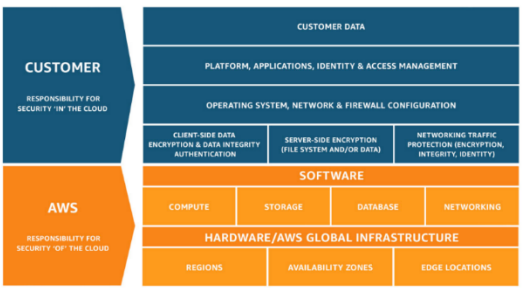
Contact Us | Support | English | My Account | Sign In to the Console

Products | Solutions | Pricing | Documentation | Learn | Partner Network | AWS Marketplace | Customer Enablement | Events | Explore More

AWS Cloud Security | Overview | Security Services | Compliance Offerings | Data Protection | Learning | Resources | Partners

AWS responsibility "Security of the Cloud" - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.



Type here to search

32°C ENG US 12:06 30-06-2022