aws certified Cloud Practitioner

review

review questions

Virtual Private Cloud (VPC)
V2.01

Course title

BackSpace Academy
AWS Certified Associate

BackSpace

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which service or component below allows inbound traffic from the internet to access a VPC?

Answers

A. Internet gateway
B. NAT gateway
C. AWS WAF
D. VPC peering

A

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

An Enterprise company wants to securely access an Amazon S3 bucket from an Amazon EC2 instance without accessing the internet. What should be the best method to accomplish this goal?

Answers

A. VPN connection
B. Internet gateway
C. VPC endpoint
D. NAT gateway

C

A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses. Traffic between your VPC and the other service does not leave the Amazon network. A VPC endpoint does not require an internet gateway, virtual private gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service.

https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which component must be attached to a VPC to enable inbound Internet access?

Answers

A. NAT gateway
B. VPC endpoint
C. VPN connection
D. Internet gateway

D

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

A user is fully responsible for which action when running workloads on AWS?

Answers

A. Patching the infrastructure components
B. Implementing controls to route application traffic
C. Maintaining physical and environmental controls
D. Maintaining the underlying infrastructure components

B

Your VPC has an implicit router (AWS manages this), and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table).

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which AWS benefit below refers to a customer’s ability to deploy applications that scale up and down the meet variable demand?

Answers

A. Elasticity
B. Agility
C. Security
D. Scalability

A

The ability to acquire resources as you need them and release resources when you no longer need them. In the cloud, you want to do this automatically.

https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which components below are required to build a successful site-to-site VPN connection on AWS? (Choose two.)

Answers

A. Internet gateway
B. NAT gateway
C. Customer gateway
D. Transit gateway
E. Virtual private gateway

C E

The following are REQUIIRED:
Customer gateway: An AWS resource which provides information to AWS about your customer gateway device.
Virtual private gateway: The VPN concentrator on the Amazon side of the Site-to-Site VPN connection.

https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

A developer is concerned that a DDoS attack could target an application.
Which services or features below can help protect against such an attack? (Choose two.)

Answers

A. AWS Shield
B. AWS CloudTrail
C. Amazon CloudFront
D. AWS Support Center
E. AWS Service Health Dashboard

A C

When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

https://aws.amazon.com/shield/

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which service or feature below can be used to prevent SQL injection attacks?

Answers

A. Security groups
B. Network ACLs
C. AWS WAF
D. IAM policy

C

Attackers sometimes insert malicious SQL code into web requests in an effort to extract data from your database. To allow or block web requests that appear to contain malicious SQL code, create one or more SQL injection match conditions. A SQL injection match condition identifies the part of web requests, such as the URI path or the query string, that you want AWS WAF Classic to inspect. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious SQL code.

https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-sql-conditions.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

An Enterprise company has an AWS-hosted website located behind an Application Load Balancer. The company wants to safeguard the website from SQL injection or cross-site scripting. Which service below should the company use?

Answers

A. Amazon GuardDuty
B. AWS WAF
C. AWS Trusted Advisor
D. Amazon Inspector

B

AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting.

https://aws.amazon.com/waf/faq/

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which of the services below can be used to extend an on-premises data center to the AWS network? (Choose two.)

Answers

A. AWS VPN
B. NAT gateway
C. AWS Direct Connect
D. Amazon Connect
E. Amazon Route 53

A C

AWS Direct Connect links your network directly to any AWS Region or Local Zone, bypassing the public internet entirely for more consistent, lower-latency performance.

AWS Site-to-Site VPN creates redundant encrypted connections to AWS in minutes, over AWS Direct Connect or the public internet.

https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-onprem.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which service or feature below requires an internet service provider (ISP) and a colocation facility to be implemented?

Answers

A. AWS VPN
B. Amazon Connect
C. AWS Direct Connect
D. Internet gateway

C

With AWS Direct Connect, you can connect to all of your AWS resources in an AWS Region, transfer your business critical data directly from your datacenter, office, or colocation environment into and from AWS, bypassing your internet service provider and removing network congestion and unpredictability.

https://aws.amazon.com/directconnect/features/

Copyright 2018 all rights reserved - BackSpace.Academy

Question

An Enterprise company operates its infrastructure in a single AWS Region. The company has thousands of VPCs in a various AWS account that it wants to interconnect. Which service or feature should the company use to help simplify management and reduce operational costs?

Answers

A. VPC endpoint
B. AWS Direct Connect
C. AWS Transit Gateway
D. VPC peering

D

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Copyright 2018 all rights reserved - BackSpace.Academy

Question

A security officer wants to enable IPsec communications to securely connect users from on-premises networks to AWS. Which service or feature below should the officer use?

Answers

A. Amazon VPC
B. AWS VPN
C. AWS Direct Connect
D. Amazon Connect

B

A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.

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

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which of the following technologies provides a secure network connection from on-premises to AWS?

Answers

A. Virtual Private Network
B. AWS Snowball
C. Amazon Virtual Private Cloud (Amazon VPC)
D. AWS Mobile Hub

A

AWS Virtual Private Network solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. Together, they deliver a highly available, managed, and elastic cloud VPN solution to protect your network traffic.

https://aws.amazon.com/vpn/

Copyright 2018 all rights reserved - BackSpace.Academy

Question

Which services below can be used to block network traffic to an instance? (Choose two.)

Answers

A. Security groups
B. Amazon Virtual Private Cloud (Amazon VPC) flow logs
C. Network ACLs
D. Amazon CloudWatch
E. AWS CloudTrail

A C

To allow or block specific IP addresses for your EC2 instances, use a network Access Control List (ACL) or security group rules in your VPC. Network ACLs and security group rules act as firewalls allowing or blocking IP addresses from accessing your resources. Network ACLs control inbound and outbound traffic at the subnet level. Security group rules act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-block-or-allow-ips/

Copyright 2018 all rights reserved - BackSpace.Academy