⌂ (https://www.whizlabs.com/learn) › My Courses (https://www.whizlabs.com/learn/my-courses)
› AWS Certified Solutions Architect Professional (https://www.whizlabs.com/learn/course/aws-csap-practice-tests#section-1)
› Practice Test III (https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13606) › Report

PRACTICE TEST III

Attempt	1
Marks Obtained	0 / 80
Your score is	0.0%

Completed on	Tuesday , 29 January 2019 , 01:40 PM
Time Taken	00 H 00 M 49 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Security	18	0	1	17
2	Network Design	10	0	0	10
3	High Availability and Business Continuity	19	0	0	19
4	Deployment Management	16	0	0	16
5	Cloud Migration & Hybrid Architecture	3	0	0	3
6	Data Storage	5	0	0	5
7	Costing	2	0	0	2
8	Scalability & Elasticity	7	0	0	7

80	**0**	**1**	**79**
Questions	Correct	Incorrect	Unattempted

Show Answers

All ▾

QUESTION 1 INCORRECT SECURITY

You have an application running on an EC2 instance which allows users to download files from a private S3 bucket using a pre-signed URL. Before generating the URL, the application should verify the existence of the file in S3. How should the application use AWS credentials to access the S3 bucket securely?

○ **A.** Use the AWS account access Keys. The application retrieves the credentials from the source code of the application.

○ **B.** Create an IAM user for the application with permissions that allow list access to the S3 bucket launch the instance as the IAM user and retrieve the IAM user’s credentials from the EC2 instance user data. ✖

○ **C.** Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role’s credentials from the EC2 Instance metadata. ✔

○ **D.** Create an IAM user for the application with permissions that allow list access to the S3 bucket. The application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the application user.

Explanation :

Answer - C

An IAM role is similar to a user. In that, it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources.

Whenever the question presents you with a scenario where an application, user, or service wants to access another service, always prefer creating IAM Role over IAM User. The reason being that when an IAM User is created for the application, it has to use the security credentials such as access key and secret key to use the AWS resource/service. This has security concerns. Whereas, when an IAM Role is created, it has all the necessary policies attached to it. So, the use of access key and secret key is not needed. This is the preferred approach.

Option A is incorrect because you should not use the account access keys , instead you should use the IAM Role.

Option B is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above.

Option C is CORRECT because, (a) it creates the IAM Role with appropriate permissions, and (b) the application accesses the AWS Resource using that role.

Option D is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above.

For more information on IAM roles, please visit the below URL:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

Ask our Experts

👍 👎

QUESTION 2 **UNATTEMPTED** **NETWORK DESIGN**

You’ve been brought in as solutions architect to assist an enterprise customer with their migration of an e-commerce platform to Amazon Virtual Private Cloud (VPC). The previous architect has already deployed a 3- tier VPC. The configuration is as follows:

VPC : vpc-2f8bc447

IGW : ig-2d8bc445

NACL : acl-208bc448

Subnets and Route Tables:

Web server's subnet-258bc44d

Application server's subnet-248bc44c

Database server's subnet-9189c6f9

Route Tables:

rtb-218bc449

rtb-238bc44b

Associations:

Subnet-258bc44d: rtb-218bc449

Subnet-248bc44c: rtb-238bc44b

Subnet-9189c6f9: rtb-238bc44b

You are now ready to begin deploying EC2 instances into the VPC. Web servers must have direct access to the internet Application and database servers cannot have direct access to the internet. Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?

○ **A.** Create a bastion and NAT Instance in subnet-258bc44d and add a route from rtb-238bc44b to subnet-258bc44d.

○ **B.** Add a route from rtb-238bc44b to igw-2d8bc445 and add a bastion and NAT instance within Subnet-248bc44c.

○ **C.** Create a Bastion and NAT Instance in subnet-258bc44d. Add a route from rtb-238bc44b to igw-2d8bc445, and a new NACL that allows access between subnet-258bc44d and subnet-248bc44c.

○ **D.** Create a Bastion and NAT instance in subnet-258bc44d and add a route from rtb-238bc44b to the NAT instance. ✓

Explanation :

Answer - D

Option A is incorrect because the route should be pointing to NAT.

Option B is incorrect because adding IGW to route rtb-238bc44b would expose the application and database server to internet. Bastion and NAT should be in public subnet.

Option C is incorrect because the route should point to NAT and not Internet Gateway else it would be internet accessible.

Option D is CORRECT because Bastion and NAT should be in the public subnet. As Web Server has direct access to Internet, the subnet subnet-258bc44d should be public and Route rtb-2i8bc449 pointing to IGW. Route rtb-238bc44b for private subnets should point to NAT for outgoing internet access.

Ask our Experts

👍 👎

QUESTION 3 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

Which of the following are the best techniques to avoid DDoS attacks for your infrastructure hosted on AWS?

Choose 3 options from the below:

□ **A.** Add multiple Elastic Network Interfaces (ENIs) to each EC2 instance to increase the network bandwidth.

□ **B.** Use dedicated instances to ensure that each instance has the maximum performance possible.

□ **C.** Use an Amazon CloudFront distribution for both static and dynamic content. ✓

□ **D.** Use an Elastic Load Balancer with auto scaling groups for Web servers and Application servers. ✓

□ **E.** Add alert Amazon CloudWatch to look for high Network in and CPU utilization. ✓

□ **F.** Create processes and capabilities to quickly add and remove rules to the instance OS firewall.

Explanation :

Answer – C, D, and E

This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques.

What is a DDoS Attack?

A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users.

DDoS Mitigation Techniques

Some of the recommended techniques for mitigating the DDoS attacks are

(i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc.

(ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems.

(iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic.

(iv) minimizing the surface area of attack

(v) obfuscating the AWS resources

Option A is incorrect because ENIs do not help in increasing the network bandwidth.

Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients.

Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked.

Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack.

Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities.

Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack.

It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency.
https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
(https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf)

Ask our Experts

👍 👎

QUESTION 4 UNATTEMPTED SECURITY

If you want to deliver private content to users from an S3 bucket, which of the below options is the most feasible to fulfill this requirement?

Choose an option from the below:

○ **A.** Use pre-signed URL ✓

○ **B.** Use EC2 to deliver content from the S3 bucket

○ **C.** Use SQS to deliver content from the S3 bucket

○ **D.** None of the above

Explanation :

Answer – A

Option A is CORRECT because a pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permissions to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.
Option B, C, and D are all incorrect.

For more information on pre-signed URLs, please refer to the below URL
http://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html)

Ask our Experts

👍 👎

QUESTION 5 UNATTEMPTED SECURITY

Which is the best option to avoid SQL Injection attacks against your infrastructure in AWS?

○ **A.** Create a DirectConnect connection so that your have a dedicated connection line.

○ **B.** Create NACL rules for the subnet hosting the application

○ **C.** Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group ✔

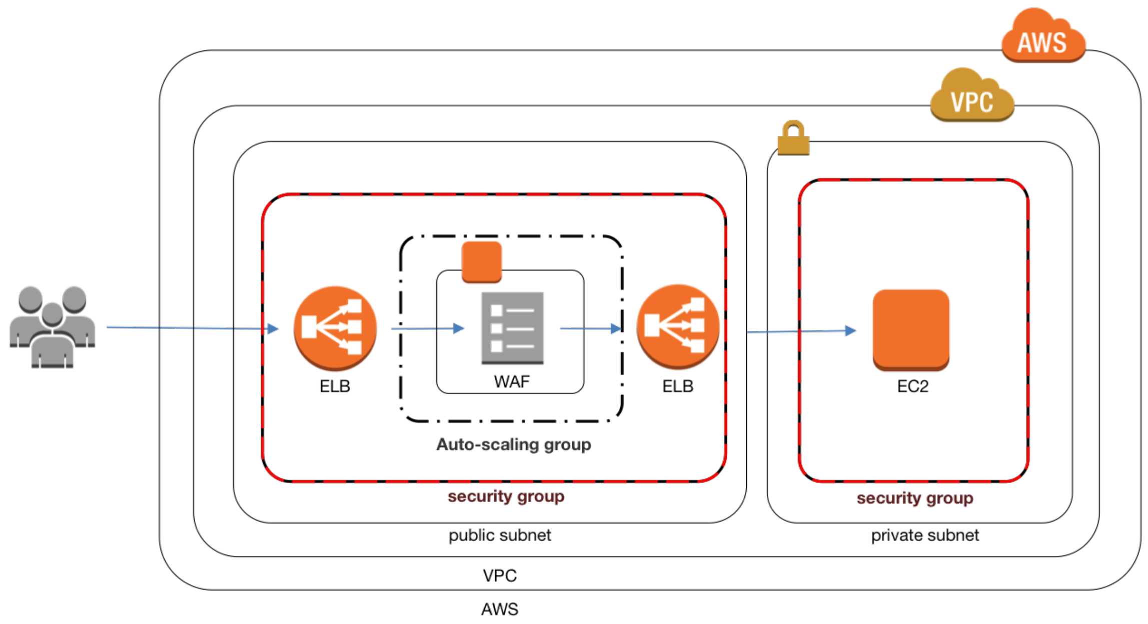
○ **D.** Remove all but TLS 1 & 2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Explanation :

Answer – C

In such scenarios where you are designing a solution to prevent the DDoS attack, always think of using Web Access Firewall (WAF).
AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns.

Option A is incorrect because, although this option could work, the setup is very complex and it not a cost effective solution.
Option B is incorrect because, (a) even though blocking certain IPs will mitigate the risk, the attacker could maneuver the IP address and circumvent the IP check by NACL, and (b) it does not prevent the attack from the new source of threat.
Option C is CORRECT because (a) WAF Tiers acts as the first line of defense, it filters out the known sources of attack and blocks common attack patterns, such as SQL injection or cross-site scripting, (b) the ELB of the application is not exposed to the attack, and most importantly (c) this pattern - known as "WAF Sandwich" pattern - has WAF layer with EC2 instances are placed between two ELBs - one that faces the web, receives all the traffic, and sends them to WAF layer to filter out the malicious requests, and sends the filtered non-malicious requests, another ELB - which receives the non-malicious requests and send them to the EC2 instances for processing. See the image below:



Option D is incorrect because there is no such thing as Advanced Protocol Filtering feature for ELB.

For more information on WAF, please visit the below URL:
https://aws.amazon.com/waf/ (https://aws.amazon.com/waf/)

Ask our Experts

QUESTION 6 UNATTEMPTED DEPLOYMENT MANAGEMENT

Which of the following is a reliable and durable logging solution to track changes made to your AWS resources?

○ **A.** Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs. ✓

○ **B.** Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs

○ **C.** Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.

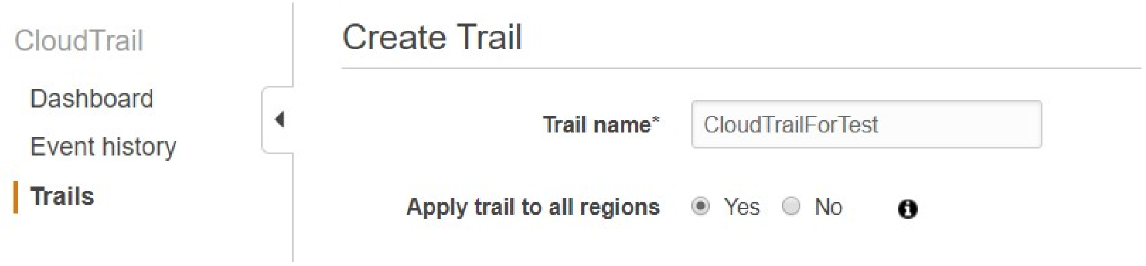
○ **D.** Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

Explanation :

Answer – A

For the scenarios where the application is tracking (or needs to track) the changes made by any AWS service, resource, or API, always think about AWS CloudTrail service.
AWS Identity and Access Management (IAM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets.
The most important points in this question are (a) S3 bucket with global services option enabled, (b) Data integrity, and (c) Confidentiality.

Option A is CORRECT because (a) it uses AWS CloudTrail with Global Option enabled, (b) a single new S3 bucket and IAM Roles so that it has the confidentiality, (c) MFA on Delete on S3 bucket so that it maintains the data integrity. See the AWS CloudTrail setting below which sets the Global Option.



Create Trail

Trail name* CloudTrailForTest

Apply trail to all regions ● Yes ○ No

Options B is incorrect because (a) although it uses AWS CloudTrail, the Global Option is not enabled, and (b) SNS notifications can be a overhead in this situation.
Option C is incorrect because (a) as an existing S3 bucket is used, it may already be accessed to the user, hence not maintaining the confidentiality, and (b) it is not using IAM roles.
Option D is incorrect because (a) although it uses AWS CloudTrail, the Global Option is not enabled, and (b) three S3 buckets are not needed.

For more information on Cloudtrail, please visit the below URL:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events
(https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events)
http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html)

Ask our Experts

👍 👎

QUESTION 7 UNATTEMPTED SECURITY

Your company has recently started using a third party custom SaaS based solution that is hosted on AWS. There is a requirement for the SaaS solution to access your company's AWS resources. Which of the following would meet the requirement for enabling the SaaS solution to work with AWS resources in the most secured manner?

○ **A.** From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.

○ **B.** Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application. Create a new access and secret key for the user and provide these credentials to the SaaS provider.

○ **C.** Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application. ✓

○ **D.** Create an IAM role for EC2 instances, assign it a policy that allows only the actions required tor the Saas application to work, provide the role ARM to the SaaS provider to use when launching their application instances.

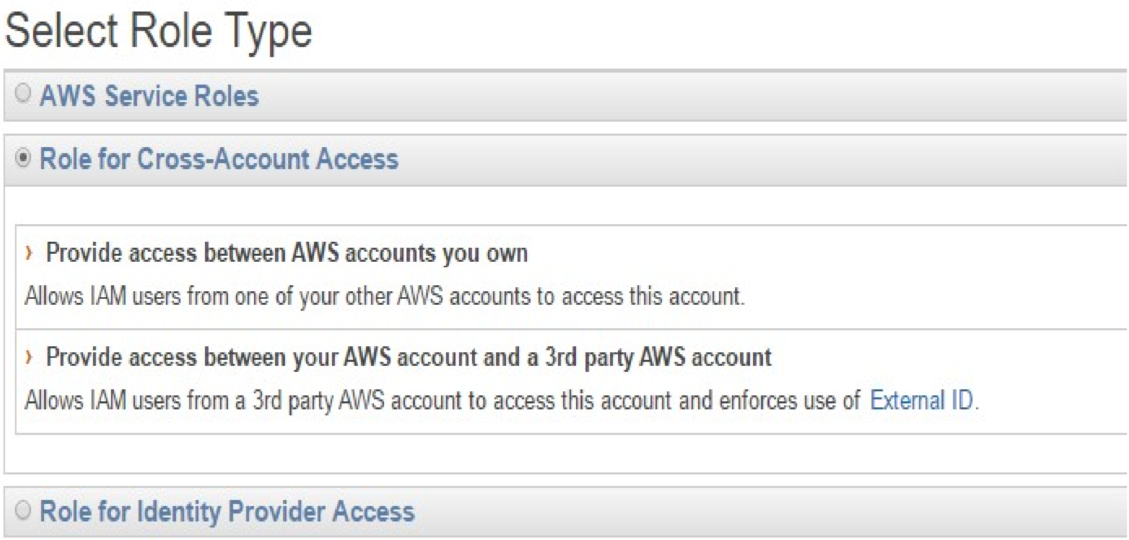
Explanation :

Answer – C

When a user, a resource, an application, or any service needs to access any AWS service or resource, always prefer creating appropriate role that has least privileged access or only required access, rather than using any other credentials such as keys.

- Option A is incorrect because you should never share your access and secret keys.
- Option B is incorrect because (a) when a user is created, even though it may have the appropriate policy attached to it, its security credentials are stored in the EC2 which can be compromised, and (b) creation of the appropriate role is always the better solution rather than creating a user.
- Option C is CORRECT because AWS role creation allows cross-account access to the application to access the necessary resources. See the image and explanation below:

Many SaaS platforms can access AWS resources via a Cross-account access created in AWS. If you go to Roles in your identity management, you will see the ability to add a cross-account role.



Select Role Type

○ AWS Service Roles

● Role for Cross-Account Access

› Provide access between AWS accounts you own

Allows IAM users from one of your other AWS accounts to access this account.

› Provide access between your AWS account and a 3rd party AWS account

Allows IAM users from a 3rd party AWS account to access this account and enforces use of External ID.

○ Role for Identity Provider Access

- Option D is incorrect because the role is to be assigned to the application and it's resources, not the EC2 instances.

For more information on the cross-account role, please visit the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

Ask our Experts

QUESTION 8 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

Your company has recently extended its data center into a VPC on AWS to add burst computing capacity as needed. Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary. You don’t want to create new IAM users for each member and make those users sign in again to the AWS Management Console. Which option below will meet the needs of your NOC members?

○ **A.** Use OAuth 2.0 to retrieve temporary AWS security credentials to enable your members to sign in to the AWS Management Console.

○ **B.** Use web Identity Federation to retrieve AWS temporary security credentials to enable your members to sign in to the AWS Management Console

○ **C.** Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint. ✔

○ **D.** Use your on-premises SAML 2.0-compliant identity provider (IDP) to retrieve temporary security credentials to enable members to sign in to the AWS Management Console.

Explanation :

Answer – C

This scenario has two requirements: (a) temporary access to AWS resources be given to certain users or application (NOC members in this case), and (b) you are not supposed to create new IAM users for the NOC members to log into AWS console.
This scenario is handled by a concept named "Federated Access". Read this for more information on federated access: https://aws.amazon.com/identity/federation/ (https://aws.amazon.com/identity/federation/) .
Read this article for more information on how to establish the federated access to the AWS resources:
https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-active-directory-user-attributes/
(https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-active-directory-user-attributes/)

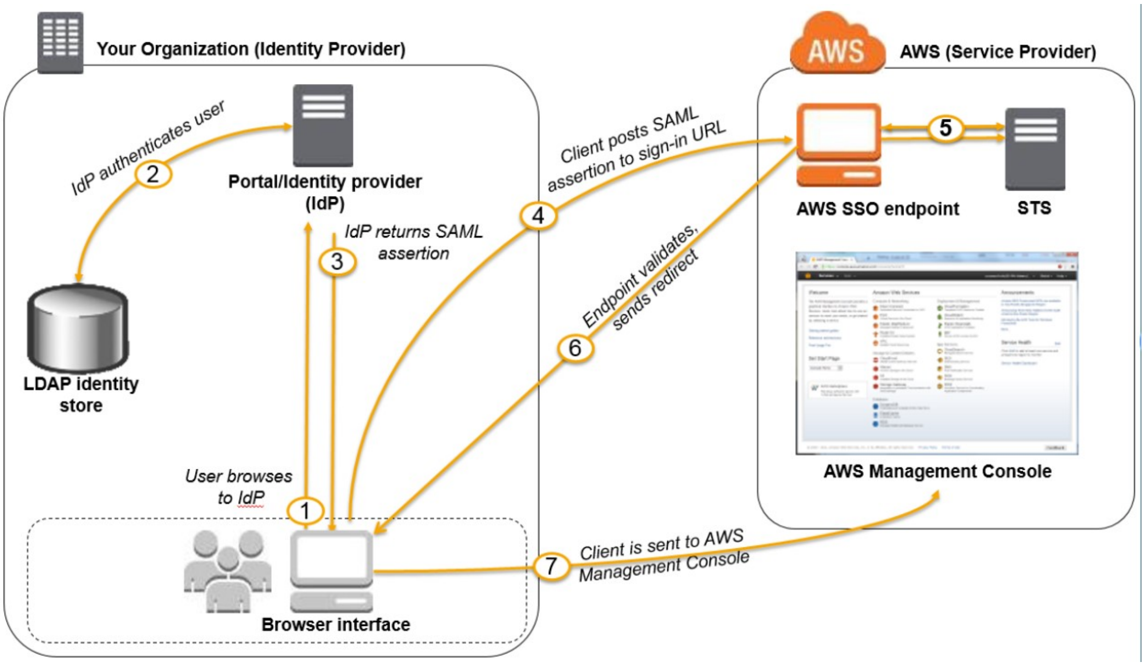
Option A is incorrect because OAuth 2.0 is not applicable in this scenario as we are not using Web Identity Federation as it is used with public identity providers such as Facebook, Google etc.

Option B is incorrect because we are not using Web Identity Federation as it is used with public identity providers such as Facebook, Google etc.

Option C is CORRECT because (a) it gives a federated access to the NOC members to AWS resources by using SAML 2.0 identity provider, and (b) it uses on-premise single sign on (SSO) endpoint to authenticate users and gives them access tokens prior to providing the federated access.

Option D is incorrect because, even though it uses SAML 2.0 identity provider, one of the requirements is not to let users sign in to AWS console using any security credentials.

See this diagram that explains the Federated Access using SAML 2.0.


Your Organization (Identity Provider)
AWS
AWS (Service Provider)
IdP authenticates user
2
Portal/Identity provider (IdP)
LDAP identity store
3
IdP returns SAML assertion
Client posts SAML assertion to sign-in URL
4
5
AWS SSO endpoint
STS
Endpoint validates, sends redirect
6
AWS Management Console
User browses to IdP
1
Browser interface
7
Client is sent to AWS Management Console

Ask our Experts

QUESTION 9 UNATTEMPTED SECURITY

You have an application running on an EC2 Instance that accesses an SQS queue. How should the application use AWS credentials to access the SQS queue securely?

○ **A.** Use the AWS account access Keys the application retrieves the credentials from the source code of the application.

○ **B.** Create an IAM user for the application with permissions that allow access to the SQS queue launch the instance as the IAM user and retrieve the IAM user's credentials from the EC2 instance user data

○ **C.** Create an IAM role for EC2 that allows access to the SQS queue. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata ✓

○ **D.** Create an IAM user for the application with permissions that allows access to the SQS queue. The application retrieves the IAM user credentials from a temporary directory with permissions that allow access only to the application user.

Explanation :

Answer - C

An IAM *role* is similar to a user. In that, it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.
You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources.
Whenever the question presents you with a scenario where an application, user, or service wants to access another service, always prefer creating IAM Role over IAM User. The reason being that when an IAM User is created for the application, it has to use the security credentials such as access key and secret key to use the AWS resource/service. This has security concerns. Whereas, when an IAM Role is created, it has all the necessary policies attached to it. So, the use of access key and secret key is not needed. This is the preferred approach.

Option A is incorrect because you should not use the account access keys, instead you should use the IAM Role.
Option B is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above.
Option C is CORRECT because, (a) it creates the IAM Role with appropriate permissions, and (b) the application accesses the AWS Resource using that role.
Option D is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above.

For more information on IAM roles, please visit the below URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

Ask our Experts

👍 👎

QUESTION 10 UNATTEMPTED SECURITY

Which of the below-mentioned methods is the best to stop a series of attacks coming from a set of determined IP ranges?

○ **A.** Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)

○ **B.** Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP

○ **C.** Create 15 Security Group rules to block the attacking IP addresses over port 80

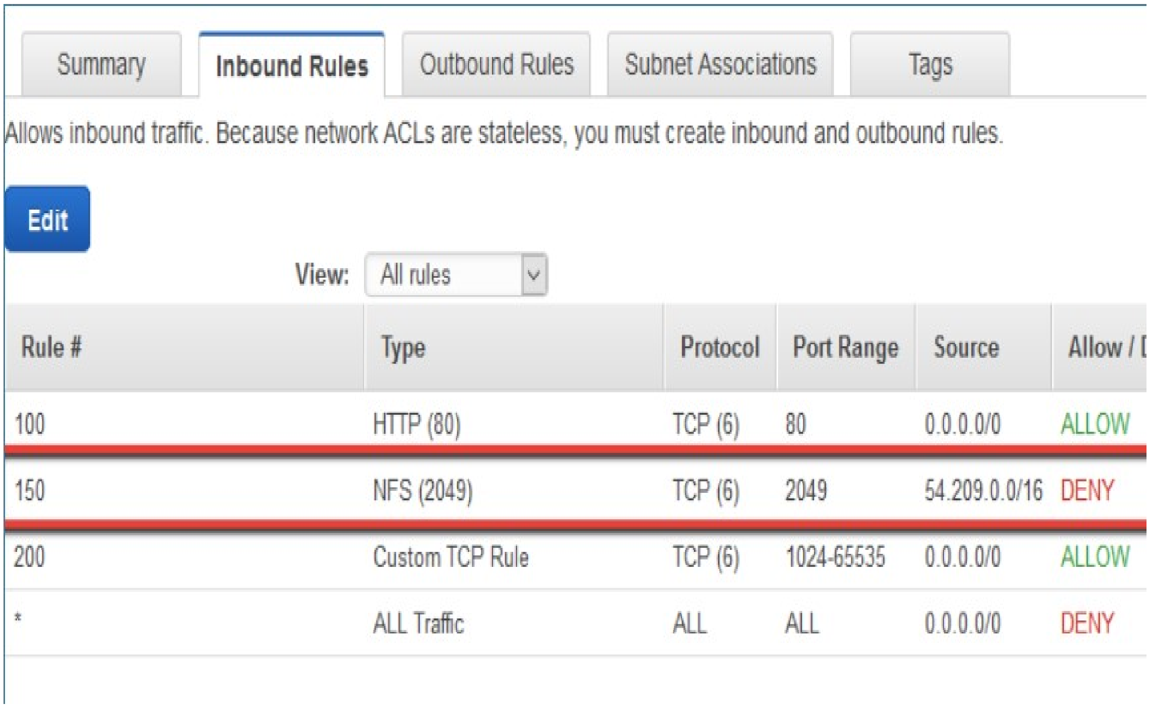
○ **D.** Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses ✔

Explanation :

Answer – D

In this scenario, the attack is coming from a set of certain IP addresses over specific port from a specific country. You are supposed to defend against this attack.
In such questions, always think about two options: Security groups and Network Access Control List (NACL). Security Groups operate at the individual instance level, whereas NACL operates at subnet level. You should always fortify the NACL first, as it is encounter first during the communication with the instances in the VPC.

Option A is incorrect because IP addresses cannot be blocked using route table or IGW.
Option B is incorrect because changing the EIP of NAT instance cannot block the incoming traffic from a particular IP address.
Option C is incorrect because (a) you cannot deny port access using security groups, and (b) by default all requests are denied; you open access for particular IP address or range. You cannot deny access for particular IP addresses using security groups.
Option D is CORRECT because (a) you can add deny rules in NACL and block access to certain IP addresses. See an example below:



Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Rule #	Type	Protocol	Port Range	Source	Allow /
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
150	NFS (2049)	TCP (6)	2049	54.209.0.0/16	DENY
200	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Ask our Experts

QUESTION 11 UNATTEMPTED DATA STORAGE

A company has the requirement to analyze the clickstreams from a web application in real time? Which of the below AWS services will fulfill this requirement?

○ **A.** Amazon Kinesis ✓

○ **B.** Amazon SQS

○ **C.** Amazon Redshift

○ **D.** AWS IoT

Explanation :

Answer – A

Kinesis Data Streams are extremely useful for rapid and continuous data intake and aggregation. The type of data used includes IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data. Because the response time for the data intake and processing is in real time, the processing is typically lightweight.

Option A is CORRECT because Amazon Kinesis Data Streams are very useful in processing website clickstreams in real time, and then analyzing using multiple different Kinesis Data Streams applications running in parallel.
Option B is incorrect because SQS is used for storing messages/work items for asynchronous processing in the application, not the real time processing of clickstream data.
Option C is incorrect because Redshift is a data warehouse solution that is used for Online Analytical Processing of data, and where complex analytic queries against petabytes of structured data. It is not used in real time processing of clickstream data.
Option D is incorrect because AWS IoT is a platform that enables you to connect devices to AWS Services and other devices, secure data and interactions, process and act upon device data. It does not do the real time processing of the clickstream data. However, it can leverage Amazon Kinesis Analytics to do it.

For more information on Kinesis , please visit the below link
http://docs.aws.amazon.com/streams/latest/dev/introduction.html
(http://docs.aws.amazon.com/streams/latest/dev/introduction.html)

Ask our Experts

👍 👎

QUESTION 12 UNATTEMPTED SECURITY

A customer is deploying an SSL enabled Web application on AWS and would like to implement a separation of roles between the EC2 service administrators that are entitled to login to Instances as well making API calls and the security officers who will maintain and have exclusive access to the application's X.509 certificate that contains the private key. Which configuration option would satisfy the above requirements?

○ **A.** Configure IAM policies authorizing access to the certificate store only to the security officer's and terminate SSL on the ELB. ✔

○ **B.** Configure system permissions on the web servers to restrict access to the certificate only to the authorized security officers.

○ **C.** Upload the certificate on an S3 bucket owned by the security officers and accessible only by the EC2 role of the web servers

○ **D.** Configure the web servers to retrieve the certificate upon boot from an CloudHSM that is managed by the security officers.

Explanation :

Answer – A

Option A is CORRECT because (a) only the security officers have access to the certificate store, and (b) the certificate is not stored on an EC2 instances, hence avoiding giving access to it to the EC2 service administrators.
Option B is incorrect because it will still involve storing the certificate on the EC2 instances and additional configuration overhead to give access to the security officers which is unnecessary.
Option C and D both are incorrect because giving EC2 instances the access to the certificate should be avoided. It is better to let ELB manage the SSL certificate, instead of the EC2 web servers.

For more information please refer to the links given below:
http://docs.aws.amazon.com/IAM/latest/APIReference/API_UploadServerCertificate.html
(http://docs.aws.amazon.com/IAM/latest/APIReference/API_UploadServerCertificate.html)
https://aws.amazon.com/blogs/aws/elastic-load-balancer-support-for-ssl-termination/
(https://aws.amazon.com/blogs/aws/elastic-load-balancer-support-for-ssl-termination/)

Ask our Experts

QUESTION 13 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company runs a customer facing event registration site which is built with a 3-tier architecture with web and application tier servers, and a MySQL database. The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs) which architecture provides high availability?

○ **A.** A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), an application tier deployed across 2 AZs with 3 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB, and one RDS (Relational Database Service) instance deployed with read replicas in the other AZ.

○ **B.** A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB, and one RDS (Relational Database Service) instance deployed with read replicas in the two other AZs.

○ **C.** A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), an application tier deployed across 2 AZs with 3 EC2 instances m each AZ inside an Auto Scaling Group behind an ELB, and a Multi-AZ RDS (Relational Database Service) deployment.

○ **D.** A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB, and a Multi-AZ RDS (Relational Database services) deployment. ✓

Explanation :

Answer - D

In this scenario, the application can run on minimum 65% of the overall capacity of servers. I.e. it can run on minimum 4 web and 4 application servers.

Since there are 3 AZs, there are many ways the instances can be put across them. The most important point to consider is that even of an entire AZ becomes unavailable, there should be minimum 4 servers running. So, placing 3 servers in 2 AZs is not a good architecture. Based on this, option A and C are incorrect. The best solution would be to have 2 servers in each AZ. So, in case of an entire AZ being unavailable, the application still has 4 servers available.

Now, regarding RDS instance, the high availability is provided by the Multi-AZ deployment, not by read replicas (although they improve the performance in case of read-heavy workload). So, option B is incorrect.

Hence, option D is CORRECT because (a) it places 2 EC2 instances in each of the 3 AZs, and (b) it uses the Multi-AZ deployment of RDS.

Ask our Experts

👍 👎

QUESTION 14 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company's on-premises content management system has the following architecture. It has an Application Tier hosted on IIS. The database Tier is MySQL database. This is regularly backed up to Amazon Simple Storage Service (S3) using the a custom backup utility. The static Content is stored on a 512GB gateway stored Storage Gateway volume attached to the application server via the iSCSI interface

Which AWS based disaster recovery strategy will give you the best RTO?

○ **A.** Deploy the MySQL database and the IIS app server on EC2. Restore the backups from Amazon S3. Generate an EBS volume of static content from the Storage Gateway and attach it to the IIS EC2 server. ✔

○ **B.** Deploy the MySQL database on RDS. Deploy the IIS app server on EC2. Restore the backups from Amazon Glacier. Generate an EBS volume of static content from the Storage Gateway and attach it to the IIS EC2 server.

○ **C.** Deploy the MySQL database and the IIS app server on EC2. Restore the MySQL backups from Amazon S3. Restore the static content by attaching an AWS Storage Gateway running on Amazon EC2 as an iSCSI volume to the IIS EC2 server.

○ **D.** Deploy the MySQL database and the IIS app server on EC2. Restore the backups from Amazon S3. Restore the static content from an AWS Storage Gateway-VTL running on Amazon EC2. Deploy the MySQL database and the IIS app server on EC2. Restore the backups from Amazon S3.

Explanation :

Answer - A

- Option A is CORRECT because (i) it deploys the MySQL database on EC2 instance by restoring the backups from S3 which is quick, and (ii) it generates the EBS volume of static content from Storage Gateway. Due to these points, option A meet the best RTO compared to all the remaining options.

- Option B is incorrect because restoring the backups from the Amazon Glacier will be slow and will not meet the RTO.

- Option C is incorrect because there is no need to attach the Storage Gateway as an iSCSI volume; you can just easily and quickly create an EBS volume from the Storage Gateway. Then you can generate snapshots from the EBS volumes for better recovery time.

- Option D is incorrect as restoring the content from Virtual Tape Library will not fit into the RTO.

Ask our Experts

👍 👎

QUESTION 15 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

An application is deployed in multiple Availability Zones in a single region. In the event of failure, the RTO must be less than 3 hours, and the RPO is 15 minutes. Which DR strategy can be used to achieve this RTO and RPO in the event of this kind of failure?

○ **A.** Take 15-minute DB backups stored in Amazon Glacier, with transaction logs stored in Amazon S3 every 5 minutes

○ **B.** Use synchronous database master-slave replication between two Availability Zones

○ **C.** Take hourly DB backups to Amazon S3, with transaction logs stored in S3 every 5 minutes ✓

○ **D.** Take hourly DB backups to an Amazon EC2 instance store volume, with transaction logs stored in Amazon S3 every 5 minutes.

Explanation :

Answer - C

Option A is incorrect because restoring the backups from Amazon Glacier would be slow and will definitely not meet the RTO and RPO.
Option B is incorrect because with the synchronous replication you cannot go back to point in time recovery. You will always have the latest data.
Option C is CORRECT because it takes hourly backups to Amazon S3 - which makes restoring the backups quick, and since the transaction logs are stored in S3 every 5 minutes, it will help to restore the application to a state that is within the RPO of 15 minutes.
Option D is incorrect because instant store volume is ephemeral. i.e. the data can get lost when the instance is terminated.

NOTE:
Although Glacier supports expedited retrieval (On-Demand and Provisioned), it is an expensive option and is recommended only for occasional urgent request for a small number of archives. Having said this (and even if we go with glacier as solution), the option also mentions taking database snapshots every 15 minutes. Now if you keep taking backups every 15 mins, the database users are going to face lot of outages during the backup (due to I/O suspension especially in non-AZ deployment). Also, within 15 minutes the backup process may not even finish!

As an architect you need to use the database change (transaction) logs along with the backups to restore your database to a point in time. Since option (c) stores the transaction details up to last 5 minutes, you can easily restore your database and meet the RPO of 15 minutes. Hence, C is the best choice.

Ask our Experts

👍 👎

QUESTION 16 UNATTEMPTED COSTING

The Marketing Director in your company asked you to create a mobile app that lets users post sightings of good deeds known as random acts of kindness in 80-character summaries. You decided to write the application in JavaScript so that it would run on the broadest range of phones, browsers, and tablets. Your application should provide access to Amazon DynamoDB to store the good deed summaries. Initial testing of a prototype shows that there aren’t large spikes in usage. Which option provides the most cost-effective and scalable architecture for this application?

○ **A.** Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) on an EC2 instance to provide signed credentials mapped to an Amazon Identity and Access Management (IAM) user allowing DynamoDB puts and S3 gets. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB

○ **B.** Register the application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow S3 gets and DynamoDB puts. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB. ✓

○ **C.** Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) to provide signed credentials mapped to an IAM user allowing DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB.

○ **D.** Register the JavaScript application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB.

Explanation :

Answer – B

This scenario asks to design a cost-effective and scalable solution where a multi-platform application needs to communicate with DynamoDB. For such scenarios, federated access to the application is the most likely solution.

Option A is incorrect because the Token Vending Machine (STS Service) is implemented on a single EC2 instance which is a single point of failure. This is not a scalable solution either as the instance can become the performance bottleneck.

Option B is CORRECT because, (i) it authenticates the application via federated identity provider such as Amazon, Google, Facebook etc, (ii) it sets up the proper permisssion for DynamoDB access, and (iii) S3 website which supports Javascript - is a highly scalable and cost effective solution.

Option C is incorrect because deploying EC2 instances in auto-scaled environment is not as cost-effective solution as the S3 website, even though it is scalable.

Option D is incorrect because (i) it does not mention any security token service that generates temporary credentials, and (ii) deploying EC2 instances in auto-scaled environment is not as cost-effective solution as the S3 website, even though it is scalable.

Ask our Experts

👍 👎

QUESTION 17 UNATTEMPTED SECURITY

You have an ELB on AWS which has a set of web servers behind them. There is a requirement that the SSL key used to encrypt data is always kept secure. Secondly, the logs of ELB should only be decrypted by a subset of users. Which of these architectures meets all of the requirements?

○ **A.** Use Elastic Load Balancing to distribute traffic to a set of web servers. To protect the SSL private key, upload the key to the load balancer and configure the load balancer to offload the SSL traffic. Write your web server logs to an ephemeral volume that has been encrypted using a randomly generated AES key.

○ **B.** Use Elastic Load Balancing to distribute traffic to a set of web servers. Use TCP load balancing on the load balancer and configure your web servers to retrieve the private key from a private Amazon S3 bucket on boot. Write your web server logs to a private Amazon S3 bucket using Amazon S3 server-side encryption.

○ **C.** Use Elastic Load Balancing to distribute traffic to a set of web servers, configure the load balancer to perform TCP load balancing, use an AWS CloudHSM to perform the SSL transactions, and write your web server logs to a private Amazon S3 bucket using Amazon S3 server-side encryption. ✔

○ **D.** Use Elastic Load Balancing to distribute traffic to a set of web servers. Configure the load balancer to perform TCP load balancing, use an AWS CloudHSM to perform the SSL transactions, and write your web server logs to an ephemeral volume that has been encrypted using a randomly generated AES key.

Explanation :

Answer – C

Option A and D both are incorrect because the logs - which contain the sensitive information - are written to ephemeral volume. So there are chances that the data can get lost upon termination of the EC2 instance.
Option B is incorrect because it does not use a secure way of managing the SSL private key for SSL transaction.
Option C is CORRECT because it uses CloudHSM for performing the SSL transaction without requiring any additional way of storing or managing the SSL private key. This is the most secure way of ensuring that the key will not be moved outside of the AWS environment. Also, it uses the highly available and durable S3 service for storing the logs.

More information on AWS CloudHSM:
The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM.

Ask our Experts

👍 👎

QUESTION 18 UNATTEMPTED NETWORK DESIGN

A company host a web application. The application is designed for business travelers who must be able to connect to it from their hotel rooms, cafes, public Wi-Fi hotspots, and elsewhere on the Internet, but the application server itself should not be exposed to the internet. Which of the below options can help to fulfill these requirements?

○ **A.** Implement AWS Direct Connect, and create a private interface to your VPC. Create a public subnet and place your application servers in it.

○ **B.** Implement Elastic Load Balancing with an SSL listener that terminates the back-end connection to the application.

○ **C.** Configure an IPsec VPN connection, and provide the users with the configuration details. Create a public subnet in your VPC, and place your application servers in it.

○ **D.** Configure an SSL VPN solution in a public subnet of your VPC, then install and configure SSL VPN client software on all user computers. Create a private subnet in your VPC and place your application servers in it. ✓

Explanation :

Answer – D
Option A is incorrect because AWS Direct Connect is not a cost effective solution compared to using VPN solution.
Option B is incorrect because it does not mention how the application would be accessible only to the business travelers and not to the public.
Option C is incorrect because if the application servers are put in the public subnet, they would be publicly accessible via the internet.

Option D is CORRECT because configuring the SSL VPN solution is cost-effective and allows access only to the business travelers and since the application servers are in private subnet, the application is not accessible via the internet.
Please refer to the below attached AWS Docs for further info:
https://aws.amazon.com/marketplace/pp/B00MI40CAE/ref=mkt_wir_openvpn_byol
(https://aws.amazon.com/marketplace/pp/B00MI40CAE/ref=mkt_wir_openvpn_byol)

Ask our Experts

QUESTION 19 UNATTEMPTED NETWORK DESIGN

An application is composed of multiple components. Currently, all the components are hosted on a single EC2 instance. Due to security reasons, the organization wants to implement 2 separate SSL for the separate modules. How can the organization achieve this with a single instance?

Choose an answer from the below options:

○ **A.** Create an EC2 instance which has multiple network interfaces with multiple elastic IP addresses. ✓

○ **B.** Create an EC2 instance which has both an ACL and the security group attached to it and have separate rules for each IP address.

○ **C.** Create an EC2 instance which has multiple subnets attached to it and each will have a separate IP address.

○ **D.** Create an EC2 instance with a NAT address.

Explanation :

Answer - A

It can be useful to assign multiple IP addresses to an instance in your VPC to do the following:

(1) Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address.
(2) Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface.
(3) Redirect internal traffic to a standby instance in case your instance fails, by reassigning the secondary IP address to the standby instance.

Option A is CORRECT because, as mentioned above, if you have multiple elastic network interfaces (ENIs) attached to the EC2 instance, each network IP can have a component running with a separate SSL certificate.
Option B is incorrect because having separate rules in security group as well as NACL does not mean that the instance supports multiple SSLs.
Option C is incorrect because an EC2 instance cannot belong to multiple subnets.
Option D is incorrect because NAT address is not related to supporting multiple SSLs.

For more information on Multiple IP Addresses, please refer to the link below:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html)

Ask our Experts

👍 👎

QUESTION 20 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company hosts an on-premises legacy engineering application with 900GB of data shared via a central file server. The engineering data consists of thousands of individual files ranging in size from megabytes to multiple gigabytes. Engineers typically modify 5-10 percent of the files a day. Your CTO would like to migrate this application to AWS, but only if the application can be migrated over the weekend to minimize user downtime. You calculate that it will take a minimum of 48 hours to transfer 900GB of data using your company's existing 45-Mbps Internet connection.

After replicating the application's environment in AWS, which option will allow you to move the application's data to AWS without losing any data and within the given timeframe?

○ **A.** Copy the data to Amazon S3 using multiple threads and multi-part upload for large files over the weekend, and work in parallel with your developers to reconfigure the replicated application environment to leverage Amazon S3 to serve the engineering files.

○ **B.** Sync the application data to Amazon S3 starting a week before the migration, on Friday morning perform a final sync, and copy the entire data set to your AWS file server after the sync completes. ✓

○ **C.** Copy the application data to a 1-TB USB drive on Friday and immediately send overnight, with Saturday delivery, the USB drive to AWS Import/Export to be imported as an EBS volume, mount the resulting EBS volume to your AWS file server on Sunday

○ **D.** Leverage the AWS Storage Gateway to create a Gateway-Stored volume. On Friday copy the application data to the Storage Gateway volume. After the data has been copied, perform a snapshot of the volume and restore the volume as an EBS volume to be attached to your AWS file server on Sunday.

Explanation :

Answer – B

In this scenario, following important points need to be considered - (i) only fraction of the data (5-10%) is modified every day, (ii) there are only 48 hrs for the migration, (iii) downtime should be minimized, and (iv) there should be no data loss.

Option A is incorrect because even though it is theoretically possible to transfer 972GB of data in 48 hours with 45Mbps speed, this option will only work if you consistently utilize the bandwidth to the max. This option will have less time in hand if there are any problems with the multipart upload. Hence, not a practical solution.

Option B is a proactive approach, which is CORRECT, because the data changes are limited and can be propagated over the week. Also, the bandwidth would be used efficiently, and you would have sufficient time and bandwidth in hand, should there be any unexpected issues while migrating.
Option C is incorrect because physically shipping the disk to Amazon would involve many external factors such as shipping delays, loss of shipping, damage to the disk, and also the time would not be sufficient to import the data in a day (Sunday). This is a very risky option and should not be exercised.
Option D is incorrect because AWS Storage Gateway involves creating S3 snapshots and synchronizing. This option is slow and may not meet the limitation of 48 hrs downtime.

Please view the below video for best practices for cloud migration to AWS:

https://www.youtube.com/watch?v=UpeV4OqB6Us&list=PL_RVC-cMNyYTz8zlxq117O1bfji-knooI&index=23 (https://www.youtube.com/watch?v=UpeV4OqB6Us&list=PL_RVC-cMNyYTz8zlxq117O1bfji-knooI&index=23)

Ask our Experts

👍 👎

QUESTION 21 UNATTEMPTED DATA STORAGE

Which of the following are some of the best examples where Amazon Kinesis can be used?

○ **A.** Accelerated log and data feed intake

○ **B.** Real-time metrics and reporting

○ **C.** Real-time data analytics

○ **D.** All of the above ✓

Explanation :

Answer - D

The following are typical scenarios for using Kinesis Data Streams:

Accelerated log and data feed intake and processing
You can have producers push data directly into a stream. For example, push system and application logs and they are available for processing in seconds. This prevents the log data from being lost if the front end or application server fails. Kinesis Data Streams provides accelerated data feed intake because you don't batch the data on the servers before you submit it for intake.

Real-time metrics and reporting
You can use data collected into Kinesis Data Streams for simple data analysis and reporting in real time. For example, your data-processing application can work on metrics and reporting for system and application logs as the data is streaming in, rather than wait to receive batches of data.

Real-time data analytics
This combines the power of parallel processing with the value of real-time data. For example, process website clickstreams in real time, and then analyze site usability engagement using multiple different Kinesis Data Streams applications running in parallel.

Complex stream processing
You can create Directed Acyclic Graphs (DAGs) of Amazon Kinesis Data Streams applications and data streams. This typically involves putting data from multiple Amazon Kinesis Data Streams applications into another stream for downstream processing by a different Amazon Kinesis Data Streams application.

For more information on Kinesis, please refer to the below URL:
https://docs.aws.amazon.com/streams/latest/dev/introduction.html
(https://docs.aws.amazon.com/streams/latest/dev/introduction.html)

Ask our Experts

QUESTION 22 UNATTEMPTED DEPLOYMENT MANAGEMENT

Which of the following are Lifecycle events available in OpsWorks?

Choose 3 options from the below:

□ **A.** Setup ✓

□ **B.** Decommision

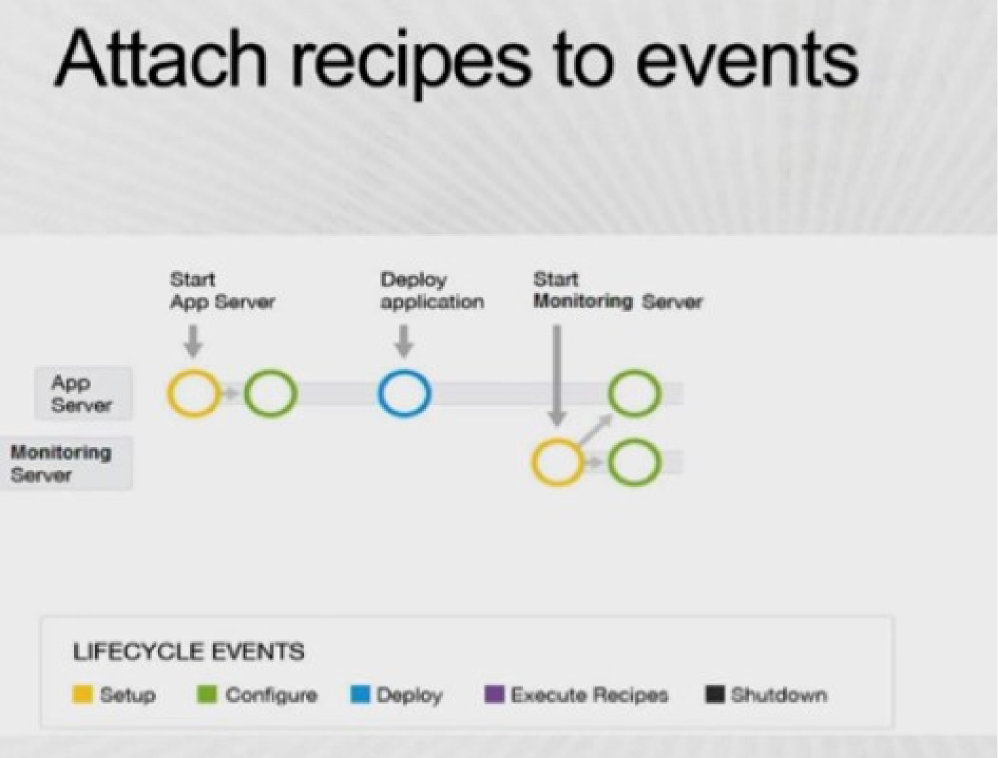
□ **C.** Deploy ✓

□ **D.** Shutdown ✓

Explanation :

Answer – A, C, and D

Below is a snapshot of the Lifecycle events in OpsWorks.



Attach recipes to events

For more information on Lifecycle events, please refer to the below URL:
http://docs.aws.amazon.com/opsworks/latest/userguide/workingcookbook-events.html
(http://docs.aws.amazon.com/opsworks/latest/userguide/workingcookbook-events.html)

Ask our Experts

QUESTION 23 UNATTEMPTED DEPLOYMENT MANAGEMENT

You tried to integrate 2 systems (front end and back end) with an HTTP interface to one large system. These subsystems don't store any state inside. All of the state information is stored in a DynamoDB table. You have launched each of the subsystems with separate AMIs.

After testing, these servers stopped running and are issuing malformed requests that do not meet the HTTP specifications of the client. Your developers fix the issue and deploy the fix to the subsystems as soon as possible without service disruption.

What are the 3 most effective options from the below to deploy these fixes and ensure that healthy instances are redeployed?

□ **A.** Use VPC.

□ **B.** Use AWS Opsworks autohealing for both the front end and back end instance pair. ✓

□ **C.** Use Elastic Load balancing in front of the front-end system and Auto scaling to keep the specified number of instances. ✓

□ **D.** Use Elastic Load balancing in front of the back-end system and Auto scaling to keep the specified number of instances. ✓

□ **E.** Use Amazon Cloudfront with access the front end server with origin fetch.

□ **F.** Use Amazon SQS between the front end and back end subsystems.

Explanation :

Answer – B, C, and D

Option A is incorrect because the instances should already be there in a VPC, and even if not, this option is not going to help fix the issue.
Option B is CORRECT because Autohealing would try to bring the instances back up with the healthy configuration with which it was launched. Please see the "More information.." section.
Option C and D are CORRECT because you can pause instances in AutoScaling, apply the patches and then add the instances back to AutoScaling and it will be registered with ELB.
Option E is incorrect because deploying CloudFront is not needed in this situation.
Option F is incorrect because if you deploy SQS, even the malformed requests will also get queued and later processed. You should be avoiding that.

More information on Auto Healing in OpsWork:
Auto healing is an excellent feature of OpsWorks and is something that provides disaster recovery within a stack. All OpsWorks instances have an agent installed which not only works to install and configure each instance using Chef, but to also update OpsWorks with resource

utilization information. If auto healing is enabled at the layer, and one or more instances experiences a health-related issue where the polling stops, OpsWorks will heal the instance. When OpsWorks heals an instance, it first terminates the problem instance, and then starts a new one as per the layer configuration. Being that the configuration is pulled from the layer; the new instance will be set up exactly as the old instance which has just been terminated.

For more information on Auto-healing, please refer to the below link
http://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-autohealing.html (http://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-autohealing.html)
For more information on the suspension process in AutoScaling, please refer to the below link
http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html (http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html)

Ask our Experts

👍 👎

QUESTION 24 UNATTEMPTED COSTING

You are the new IT architect in a company that operates a mobile sleep tracking application. When activated at night, the mobile app is sending collected data points of 1 kilobyte every 5 minutes to your backend. The backend takes care of authenticating the user and writing the data points into an Amazon DynamoDB table. Every morning, you scan the table to extract and aggregate last night's data on a per user basis, and store the results in Amazon S3. Users are notified via Amazon SNS mobile push notifications that new data is available, which is parsed and visualized by the mobile app. Currently you have around 100k users who are mostly based out of North America. You have been tasked to optimize the architecture of the backend system to lower cost.

What would you recommend? Choose 2 answers:

□ **A.** Have the mobile app access Amazon DynamoDB directly instead of JSON files stored on Amazon S3.

□ **B.** Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.

□ **C.** Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput. ✓

□ **D.** Introduce Amazon Elasticache to cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.

□ **E.** Create a new Amazon DynamoDB table each day and drop the one for the previous day after its data is on Amazon S3. ✓

Explanation :

Answers - C & E

Option A is incorrect because, accessing the DynamoDB table for read and write by 100k users will exhaust the read and write capacity, which will increase the cost drastically.

Option B is incorrect because, creating clusters of EC2 instances will be a very expensive solution in this scenario.

Option C is CORRECT because, (a) with SQS, the huge number of writes overnight will be buffered/queued which will avoid exhausting the write capacity (hence, cutting down on cost), and (b) SQS can handle a sudden high load, if any.

Option D is incorrect because, the data is not directly accessed from the DynamoDB table by the users, it is accessed from S3. So, there is no need for caching. Since the results are stored in S3, introducing ElastiCache is unnecessary.

Option E is CORRECT because once the aggregated data is stored on S3, there is no point in keeping the DynamoDB tables pertaining to the previous days. Keeping the tables for the latest data only will certainly cut the unnecessary costs, keeping the overall cost of the solution down.

Ask our Experts

👍 👎

QUESTION 25 UNATTEMPTED NETWORK DESIGN

A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?

○ **A.** It will throw a CIDR overlap error ✓

○ **B.** It is not possible to create a subnet with the same CIDR as the VPC

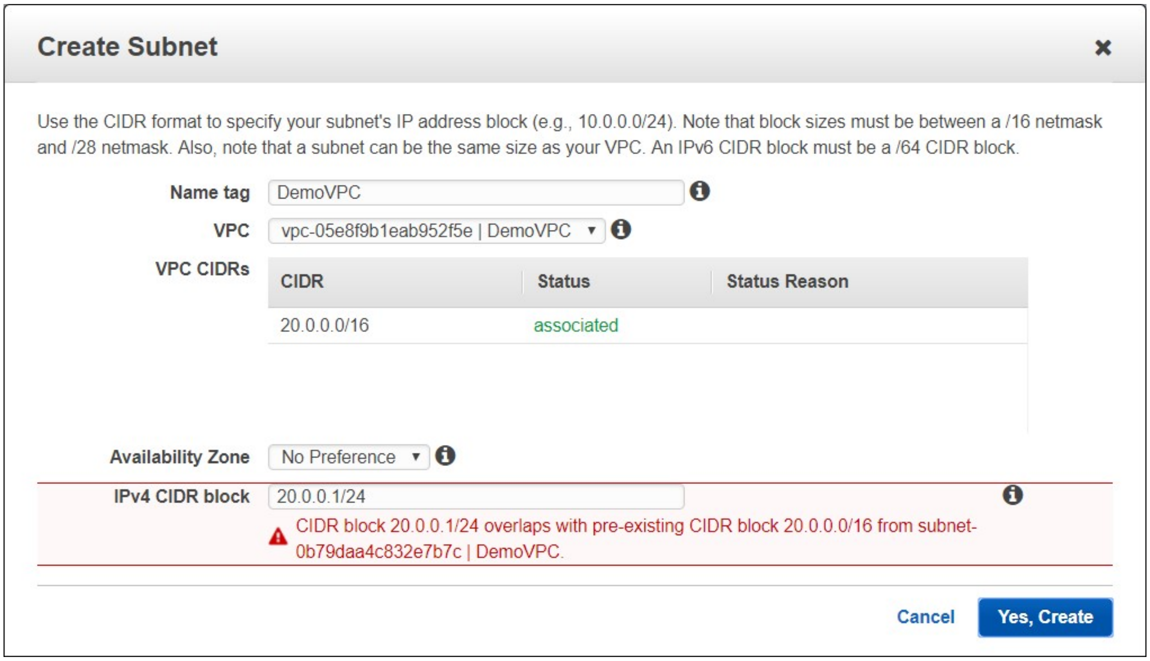
○ **C.** The second subnet will be created

○ **D.** The VPC will modify the first subnet to allow this IP range

Explanation :

Answer - A

Since the CIDR of the new subnet overlaps with that of the first subnet, an overlap error will be displayed. See the snapshot below:



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag DemoVPC

VPC vpc-05e8f9b1eab952f5e | DemoVPC

VPC CIDRs

CIDR	Status	Status Reason
20.0.0.0/16	associated	

Availability Zone No Preference

IPv4 CIDR block 20.0.0.1/24

CIDR block 20.0.0.1/24 overlaps with pre-existing CIDR block 20.0.0.0/16 from subnet-0b79daa4c832e7b7c | DemoVPC.

For more information on VPC subnets, please refer to the below link http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Ask our Experts

👍 👎

QUESTION 26 UNATTEMPTED DATA STORAGE

Currently, a company uses Redshift to store its analyzed data. They have started with the base configuration. What would they get when they initially start using Redshift?

○ **A.** Two nodes with 320GB each

○ **B.** One node of 320GB

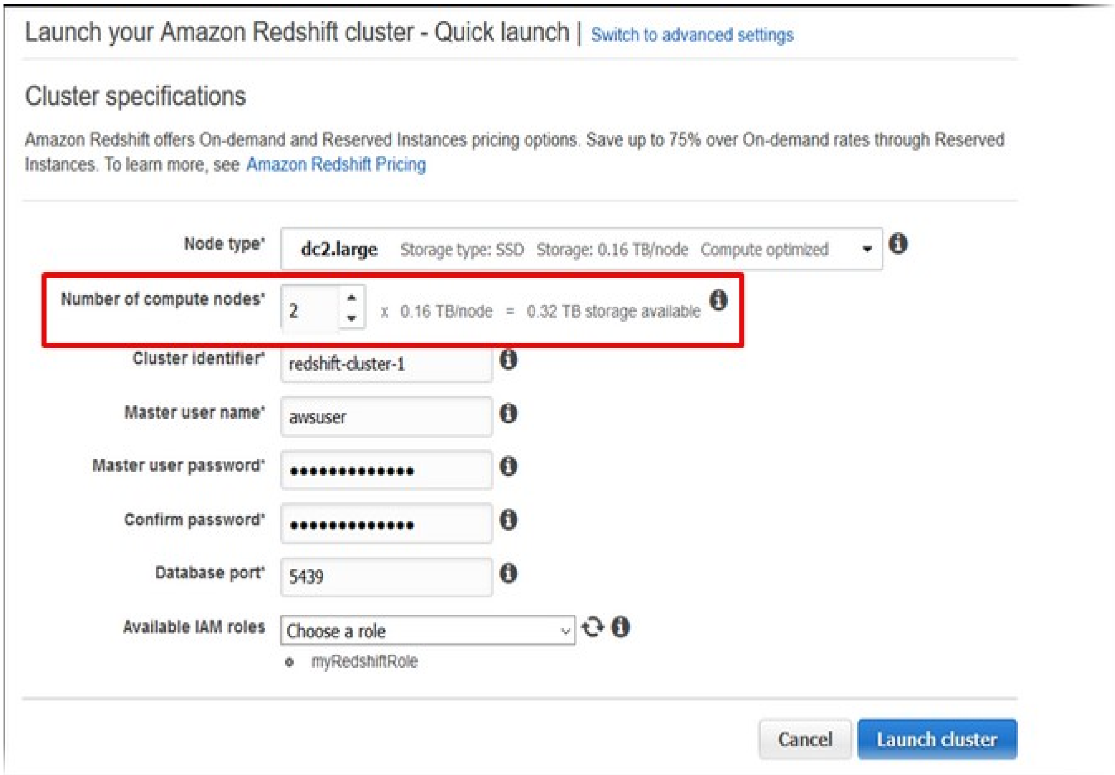
○ **C.** Two nodes with 160GB each ✓

○ **D.** One node of 160GB

Explanation :

Answer – C
As per the AWS documentation,
########
On the Cluster specifications page, enter the following values and then choose **Launch cluster**:

- **Node type**: Choose **dc2.large**.
- **Number of compute nodes**: Keep the default value of **2**.
- **Master user name**: Keep the default value of **awsuser**.
- **Master user password** and **Confirm password**: Enter a password for the master user account.
- **Database port**: Accept the default value of **5439**.
- **Available IAM roles**: Choose **myRedshiftRole**.



Launch your Amazon Redshift cluster - Quick launch | Switch to advanced settings

Cluster specifications

Amazon Redshift offers On-demand and Reserved Instances pricing options. Save up to 75% over On-demand rates through Reserved Instances. To learn more, see Amazon Redshift Pricing

Node type* dc2.large Storage type: SSD Storage: 0.16 TB/node Compute optimized

Number of compute nodes* 2 x 0.16 TB/node = 0.32 TB storage available

Cluster identifier* redshift-cluster-1

Master user name* awsuser

Master user password* ••••••••••••••

Confirm password* ••••••••••••••

Database port* 5439

Available IAM roles Choose a role

- myRedshiftRole

########

For more information on Redshift please refer to the below URL:

- https://docs.aws.amazon.com/redshift/latest/gsg/rs-gsg-launch-sample-cluster.html (https://docs.aws.amazon.com/redshift/latest/gsg/rs-gsg-launch-sample-cluster.html)

Ask our Experts

👍 👎

QUESTION 27 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

If an on-premise application is dependent on multicast and is required to be moved on to AWS, which of the below steps need to be carried out on the Operating system hosting that app so that it can be moved to AWS?

○ **A.** Provide Elastic Network Interfaces between the subnets.

○ **B.** Create a virtual overlay network that runs on the OS level of the instance.

○ **C.** All of the answers listed will help in deploying applications that require multicast on AWS.

○ **D.** Create all the subnets on a different VPC and use VPC peering between them.

Explanation :

Answer – B

Option A is incorrect because just providing ENIs between the subnets would not resolve the dependency on multicast.
Option B is CORRECT because overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC).
Option C is incorrect because the only option that will work in this scenario is creating a virtual overlay network.
Option D is incorrect because VPC peering and multicast are not the same.

For more information on Overlay Multicast in Amazon VPC, please visit the URL below:
https://aws.amazon.com/articles/6234671078671125
(https://aws.amazon.com/articles/6234671078671125)

Ask our Experts

👍 👎

QUESTION 28 UNATTEMPTED SECURITY

An auditor needs read-only access to the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. What is the best way for giving them this sort of access?

○ **A.** Create a role that has the full permissions to access the resources for the auditor.

○ **B.** Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.

○ **C.** The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.

○ **D.** Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. ✓

Explanation :

Answer – D

Option A is incorrect because (i) full permission to all the resources is not required, read only permissions should be given, and (ii) just creating access role in not sufficient, CloudTrail logging needs to be enabled as well.
Option B is incorrect because sending the logs via email is not a good architecture.
Option C is incorrect because granting the auditor access to AWS resources is not AWS's responsibility. It is the AWS user or account owner's responsibility.
Option D is CORRECT because you need to enable the CloudTrail logging in order to generate the logs with information about all the activities related to the AWS account and resources. It also creates an IAM user that has permissions to read the logs that are stored in the S3 bucket.

More information on AWS CloudTrail
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.
For more information on CloudTrail, please visit the below URL:
https://aws.amazon.com/cloudtrail/ (https://aws.amazon.com/cloudtrail/)

Ask our Experts

👍 👎

QUESTION 29 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

Which of the following is the most recommended approach to replicate an RDS instance from an on-premise location to AWS in the most secure manner?

○ **A.** Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.

○ **B.** RDS cannot replicate to an on-premise database server. Instead, first configure the RDS instance to replicate to an EC2 instance with core MySQL, and then configure replication over a secure VPN/VPG connection.

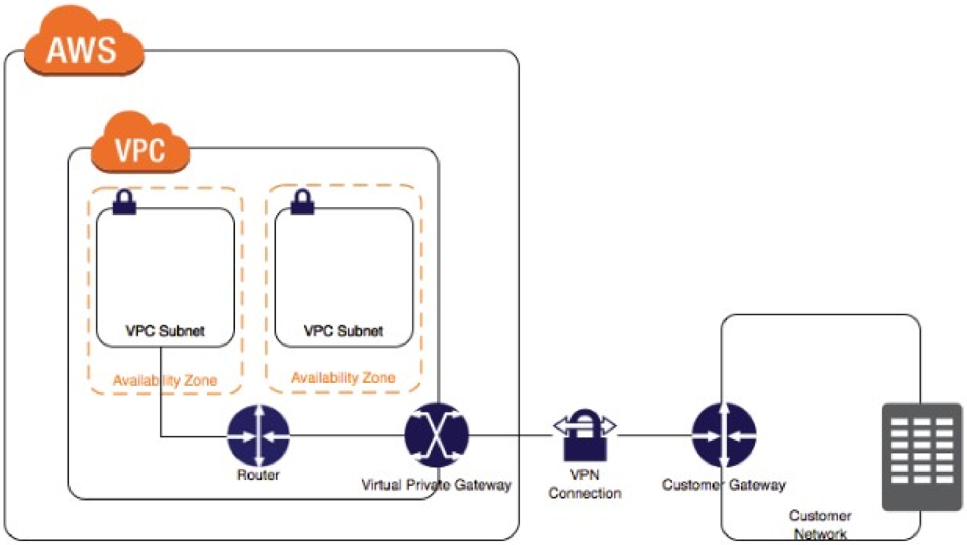
○ **C.** Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint.

○ **D.** Create an IPSec VPN connection using either VPN/VGW through the Virtual Private Cloud service. ✔

Explanation :

Answer – D

Option A is incorrect because SSL endpoint cannot be used here as it is used for securely accessing the database.
Option B is incorrect because replicating via EC2 instances is very time consuming and very expensive cost-wise.
Option C is incorrect because Data Pipeline is for batch jobs and not suitable for this scenario.
Option D is CORRECT because it is feasible to setup the secure IPSec VPN connection between the on premise server and AWS VPC using the VPN/Gateways.
See the image below:



For more information on VPN connections, please visit the below URL:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts

QUESTION 30 UNATTEMPTED SCALABILITY & ELASTICITY

A mobile application has been developed which stores data in DynamoDB. The application needs to scale to handle millions of views. The customer also needs access to the data in the DynamoDB table as part of the application. Which of the below methods would help to fulfill this requirement?

○ **A.** Configure an on-premise AD server utilizing SAML 2.0 to manage the application users inside of the on-premise AD server and write code that authenticates against the LD serves. Grant a role assigned to the STS token to allow the end-user to access the required data in the DynamoDB table.

○ **B.** Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWith API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket.

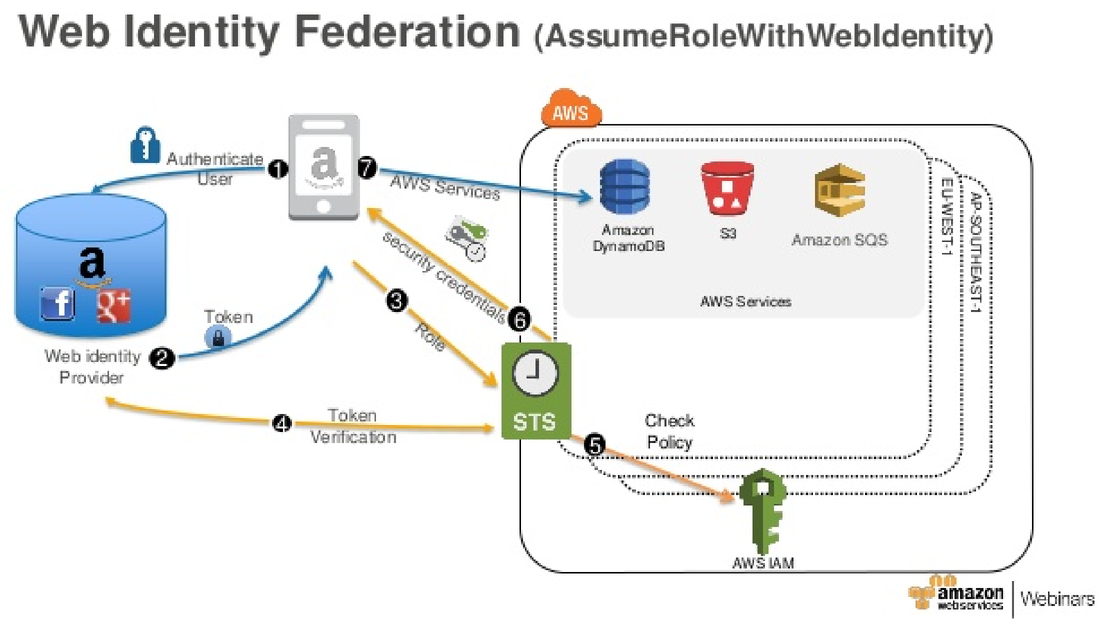
○ **C.** Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in a server-side language using the AWS SDK and host the application in an S3 bucket for scalability.

○ **D.** Let the users sign in to the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket. ✓

Explanation :

Answer – D

The AssumeRolewithWebIdentity returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider.
Out of option C and D, Option C is invalid because S3 is used to host static websites and not server side language websites.



For more information on AssumeRolewithWebIdentity, please visit the below URL:
http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html
(http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html)

Ask our Experts

QUESTION 31 UNATTEMPTED DEPLOYMENT MANAGEMENT

You've created a temporary application that accepts image uploads, stores them in S3, and records information about the image in RDS. After building this architecture and accepting images for the duration required, it's time to delete the CloudFormation template. However, your manager has informed you that for archival reasons the RDS data needs to be stored and the S3 bucket with the images needs to remain. Your manager has also instructed you to ensure that the application can be restored by a CloudFormation template and run next year during the same period.

Knowing that when a CloudFormation template is deleted, it will remove the resources it created. What is the best method for achieving the desired goals?

Choose the correct option from the below:

○ **A.** Enable S3 bucket replication on the source bucket to a destination bucket to maintain a copy of all the S3 objects, set the deletion policy for the RDS instance to snapshot.

○ **B.** For both the RDS and S3 resource types on the CloudFormation template, set the DeletionPolicy to retain.

○ **C.** Set the DeletionPolicy on the S3 resource to snapshot and the DeletionPolicy on the RDS resource to snapshot.

○ **D.** Set the DeletionPolicy on the S3 resource declaration in the CloudFormation template to retain, set the RDS resource declaration DeletionPolicy to snapshot. ✓

Explanation :

Answer - D

The main points in this questions are: (i) need for an ability by which the RDS data that is stored and can be restored of needed and (ii) the S3 bucket with the images needs to retain.

Option A is incorrect because this option replicates the images into another bucket, but does not ensure that the bucket itself would retain.
Option B is incorrect because RDS data does not need to be retained, you just need an ability to be able to restore the RDS data - for which you need to use snapshot policy.
Option C is incorrect because S3 bucket itself needs to be retained, hence you need to use retain policy for S3 bucket.
Option D is CORRECT because it uses retain policy for S3 bucket and snapshot policy for RDS such that the data can be restored when needed.

More information on DeletionPolicy Options:
Delete
AWS CloudFormation deletes the resource and all its content if applicable during stack deletion.

Retain
AWS CloudFormation keeps the resource without deleting the resource or its contents when its stack is deleted.

Snapshot
For resources that support snapshots (AWS::EC2::Volume, AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup, AWS::RDS::DBInstance, AWS::RDS::DBCluster, and AWS::Redshift::Cluster), AWS CloudFormation creates a snapshot for the resource before deleting it.

For more information on CloudFormation deletion policy, please visit the below URL:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html
(http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html)

Ask our Experts

👍 👎

QUESTION 32 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

What can be done if a company wants to establish a low latency dedicated connection to an S3 public endpoint over the Direct Connect?

○ **A.** Configure a public virtual interface to connect to a public S3 endpoint resource. ✓

○ **B.** Establish a VPN connection from the VPC to the public S3 endpoint.

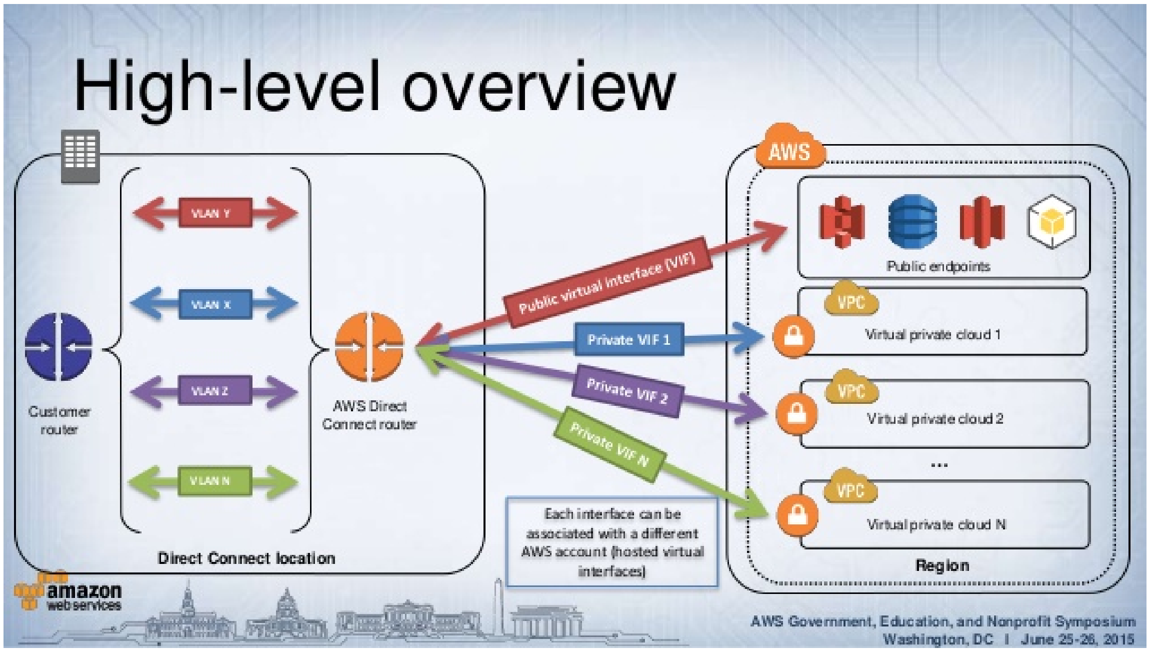
○ **C.** Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.

○ **D.** Add a BGP route as part of the on-premise router; this will route S3 related traffic to the public S3 endpoint to dedicated AWS region.

Explanation :

Answer – A

You can create a public virtual interface to connect to public resources or a private virtual interface to connect to your VPC. You can configure multiple virtual interfaces on a single AWS Direct Connect connection, and you'll need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key. See the image below:



High-level overview

Each interface can be associated with a different AWS account (hosted virtual interfaces)

AWS Government, Education, and Nonprofit Symposium
Washington, DC | June 25-26, 2015

Option A is CORRECT because, as mentioned above, it creates a public virtual interface to connect to S3 endpoint.
Option B is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not VPN.
Option C is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not private.
Option D is incorrect because this setup will not help connecting to the S3 endpoint.

For more information on virtual interfaces, please visit the below URL
http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html
(http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html)

Ask our Experts

QUESTION 33 UNATTEMPTED DATA STORAGE

How can you configure the backups of an Oracle RAC configuration which is hosted on the AWS public cloud?

○ **A.** Create manual snapshots of the RDS backup and write a script that runs the manual snapshot.

○ **B.** Enable Multi-AZ failover on the RDS RAC cluster to reduce the RPO and RTO in the event of disaster or failure.

○ **C.** Create a script that runs snapshots against the EBS volumes to create backups and durability. ✓

○ **D.** Enable automated backups on the RDS RAC cluster; enable auto snapshot copy to a backup region to reduce RPO and RTO.

Explanation :

Answer – C

Currently, Oracle Real Application Cluster (RAC) is not supported as per the AWS documentation. However, you can deploy scalable RAC on Amazon EC2 using the recently-published tutorial (https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/)and Amazon Machine Images (AMI). So, in order to take the backups, you need to take the backup in the form of EBS volume snapshots of the EC2 that is deployed for RAC.

Option A, B, and D are all incorrect because RDS does not support Oracle RAC.
Option C is CORRECT because Oracle RAC is supported via the deployment using Amazon EC2. Hence, for the data backup, you can create a script that takes the snapshots of the EBS volumes.

For more information on Oracle RAC on AWS, please visit the below URL:
https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/
(https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/)
https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/
(https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/)
https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/
(https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/)

Ask our Experts

QUESTION 34 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You are moving an existing traditional system to AWS. During migration, you discover that the master server is the single point of failure. Having examined the implementation of the master server you realize that there is not enough time during migration to re-engineer it to be highly available. You also discover that it stores its state in local MySQL database.

In order to minimize downtime, you select RDS to replace the local database and configure the master to use it. What steps would best allow you to create a self-healing architecture?

○ **A.** Migrate the local database into Multi-AZ database. Place the master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks. ✓

○ **B.** Migrate the local database into Multi-AZ database. Place the master node into a Cross Zone ELB with a minimum of one and maximum of one with health checks

○ **C.** Replicate the local database into a RDS Read Replica. Place the master node into a Cross Zone ELB with a minimum of one and maximum of one with health checks

○ **D.** Replicate the local database into a RDS Read Replica.Place the master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks.

Explanation :

Answer - A

Option A is CORRECT because (i) for database, Multi-AZ architecture provides high availability and can meet shortest of RTO and RPO requirements in case of failures, since it uses synchronous replication and maintains standby instance which gets promoted to primary, and (ii) for master server, it uses auto scaling which ensures that at least one server is always running.
Option B is incorrect because ELB cannot ensure the minimum or maximum number of instances running.
Option C is incorrect because (i) read replicas do not provide high availability, and (ii) ELB cannot ensure the minimum or maximum number of instances running.
Option D is incorrect because read replicas do not provide high availability.

More information on Multi-AZ RDS architecture:
Multi-AZ is used for highly available architecture. If a failover happens, the secondary DB which is a synchronous replica will have the data, and it's just the CNAME which changes. For Read replica, it's primarily used for distributing workloads.

For more information on Multi-AZ RDS, please refer to the below link
https://aws.amazon.com/rds/details/multi-az/ (https://aws.amazon.com/rds/details/multi-az/)

Ask our Experts

👍 👎

QUESTION 35 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You're migrating an existing application to the AWS cloud. The application will be primarily using EC2 instances. This application needs to be built with the highest availability architecture available. The application currently relies on hardcoded hostnames for intercommunication between the three tiers. You've migrated the application and configured the multi-tiers using the internal Elastic Load Balancer for serving the traffic. The load balancer hostname is demo-app.us-east-1.elb.amazonaws.com. The current hard-coded hostname in your application used to communicate between your multi-tier application is demolayer.example.com. What is the best method for architecting this setup to have as much high availability as possible?

Choose the correct answer from the below options:

○ **A.** Create an environment variable passed to the EC2 instances using user-data with the ELB hostname, demo-app.us-east-1.elb.amazonaws.com.

○ **B.** Create a private resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com. ✔

○ **C.** Create a public resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.

○ **D.** Add a cname record to the existing on-premise DNS server with a value of demo-app.us-east-1.elb.amazonaws.com. Create a public resource record set using Route 53 with a hostname of applayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.

Explanation :

Answer – B

Since demolayer.example.com is an internal DNS record, the best way is Route 53 to create an internal resource record. One can then point the resource record to the create ELB.
While ordinary Amazon Route 53 resource record sets are standard DNS resource record sets, *alias resource record sets* provide an Amazon Route 53–specific extension to DNS functionality. Instead of an IP address or a domain name, an alias resource record set contains a pointer to a CloudFront distribution, an Elastic Beanstalk environment, an ELB Classic or Application Load Balancer, an Amazon S3 bucket that is configured as a static website, or another Amazon Route 53 resource record set in the same hosted zone.

Option A is incorrect because it does not mention how the mapping between the existing hard-coded host name and the ELB host name.
Option B is CORRECT because it creates an internal ALIAS record set where it defines the mapping between the hard-coded host name and the ELB host name that is to be used.
Option C and D are incorrect because it should create a private record set, not public, since the mapping between the hard-coded host name and ELB host name should be done internally.

For more information on alias and non-alias records please refer to the below link
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html
(http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html)

Ask our Experts

QUESTION 36 UNATTEMPTED DEPLOYMENT MANAGEMENT

A company has an application that is hosted on an EC2 instance. The code is written in .NET and connects to a MySQL RDS database. If you're executing .NET code against AWS on an EC2 instance that is assigned an IAM role, which of the following is a true statement?

Choose the correct option from the below:

○ **A.** The code will assume the same permissions as the EC2 role ✔

○ **B.** The code must have AWS access keys in order to execute

○ **C.** Only .NET code can assume IAM roles

○ **D.** None of the above

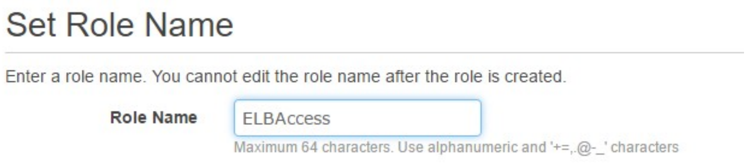
Explanation :

Answer – A

The best practice for IAM is to create roles which have specific access to an AWS service and then give the user permission to the AWS service via the role.

To get the role in place, follow the below steps

Step 1) Create a role which has the required ELB access



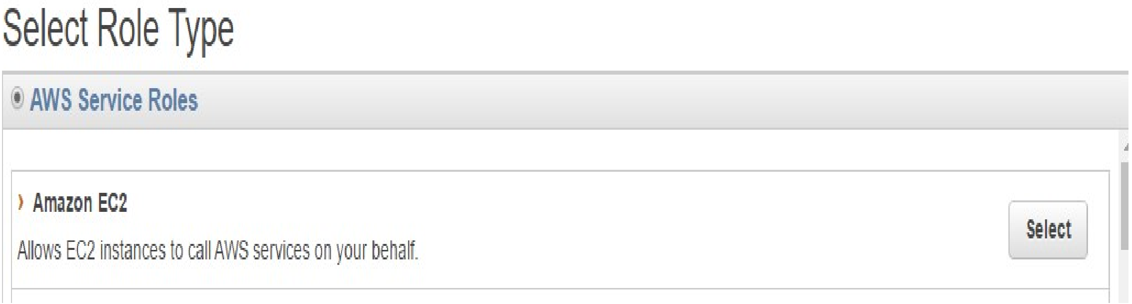
Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name: ELBAccess

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters

Step 2) You need to provide permissions to the underlying EC2 instances in the Elastic Load Balancer

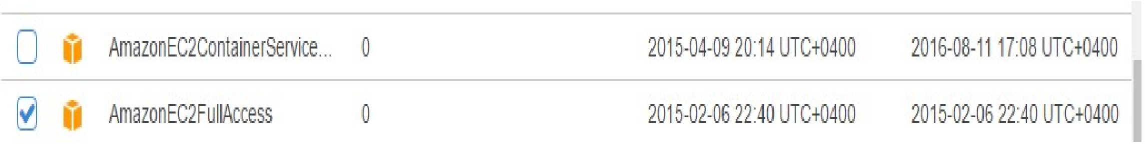


Select Role Type

● AWS Service Roles

› Amazon EC2

Allows EC2 instances to call AWS services on your behalf.



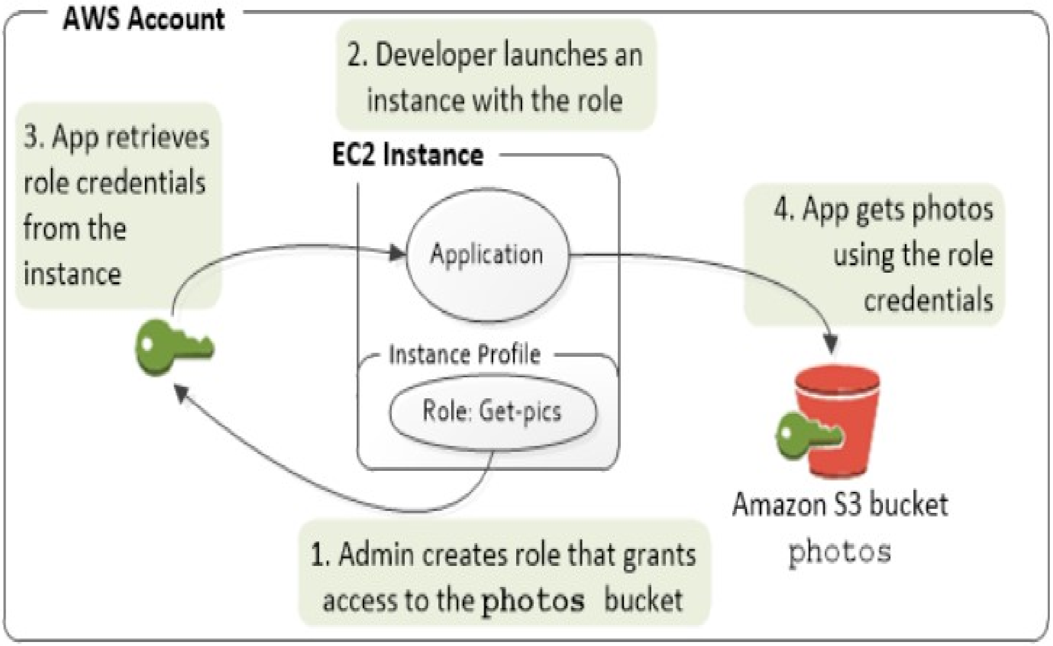
□	AmazonEC2ContainerService...	0	2015-04-09 20:14 UTC+0400	2016-08-11 17:08 UTC+0400
☑	AmazonEC2FullAccess	0	2015-02-06 22:40 UTC+0400	2015-02-06 22:40 UTC+0400

For the best practices on IAM policies, please visit the link

- http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)

Note:
As per AWS,
When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.
Using roles to grant permissions to applications that run on EC2 instances requires a bit of extra configuration. An application running on an EC2 instance is abstracted from AWS by the virtualized operating system. Because of this extra separation, an additional step is needed to assign an AWS role and its associated permissions to an EC2 instance and make them available to its applications. This extra step is the creation of an *instance profile (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html)* that is attached to the instance. The instance profile contains the role and can provide the role's temporary credentials to an application that runs on the instance. Those temporary credentials can then be used in the application's API calls to access resources and to limit access to only those resources that the role specifies. Note that only one role can be assigned to an EC2 instance at a time, and all applications on the instance share the same role and permissions.

The example given here shows how the application retrieves role permissions from the instance for accessing the bucket.


AWS Account
2. Developer launches an instance with the role
3. App retrieves role credentials from the instance
EC2 Instance
Application
4. App gets photos using the role credentials
Instance Profile
Role: Get-pics
Amazon S3 bucket
photos
1. Admin creates role that grants access to the photos bucket

Ask our Experts

QUESTION 37 UNATTEMPTED DEPLOYMENT MANAGEMENT

A company is making extensive use of S3. They have a strict security policy and require that all artifacts are stored securely in S3. Which of the following request headers, when specified in an API call, will cause an object to be SSE?

Choose the correct option from the below:

○ **A.** AES256

○ **B.** amz-server-side-encryption

○ **C.** x-amz-server-side-encryption ✔

○ **D.** server-side-encryption

Explanation :

Answer – C

Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
The object creation REST APIs (see Specifying Server-Side Encryption Using the REST API) provides a request header, x-amz-server-side-encryption that you can use to request server-side encryption.
To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3.

```
PUT /example-object HTTP/1.1
Host: myBucket.s3.amazonaws.com
Date: Wed, 8 Jun 2016 17:50:00 GMT
Authorization: authorization string
Content-Type: text/plain
Content-Length: 11434
x-amz-meta-author: Janet
Expect: 100-continue
x-amz-server-side-encryption: AES256
[11434 bytes of object data]
```

In order to enforce object encryption, create an S3 bucket policy that denies any S3 Put request that does not include the x-amz-server-side-encryption header. There are two possible values for the x-amz-server-side-encryption header: AES256, which tells S3 to use S3-managed keys, and aws:kms, which tells S3 to use AWS KMS–managed keys.

For more information on S3 encryption, please visit the link
http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html)
https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/ (https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/)

Ask our Experts

👍 👎

QUESTION 38 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You decide to create a bucket on AWS S3 called 'mybucket' and then perform the following actions in the order that they are listed here.

- You upload a file to the bucket called 'file1'

- You enable versioning on the bucket

- You upload a file called 'file2'

- You upload a file called 'file3'

- You upload another file called 'file2'

Which of the following is true for 'mybucket'? Choose the correct option from the below:

○ **A.** There will be 1 version ID for file1, there will be 2 version IDs for file2 and 1 version ID for file3

○ **B.** The version ID for file1 will be null, there will be 2 version IDs for file2 and 1 version ID for file3 ✓

○ **C.** There will be 1 version ID for file1, the version ID for file2 will be null and there will be 1 version ID for file3

○ **D.** All file version ID's will be null because versioning must be enabled before uploading objects to 'mybucket'

Explanation :

Answer – B

Objects stored in your bucket before you set the versioning state have a version ID of null. When you enable versioning, existing objects in your bucket do not change. What changes is how Amazon S3 handles the objects in future requests.

Option A is incorrect because the version ID for file1 would be null.
Option B is CORRECT because the file1 was put in the bucket before the versioning was enabled; hence, it will have null version ID. The file2 will have two version IDs, and file3 will have a single version ID.
Option C is incorrect because file2 cannot have a null version ID as the versioning was enabled

before putting it in the bucket.
Option D is incorrect because once the versioning is enabled, all the files put *after* that will not have null version ID. But file1 was put *before* versioning was enabled, so it will have null as its version ID.

For more information on S3 versioning, please visit the below link
http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html)

Ask our Experts

👍 👎

QUESTION 39 UNATTEMPTED SECURITY

One of your requirements is to setup an S3 bucket to store your files like documents and images. However, those objects should not be directly accessible via the S3 URL, they should only be accessible from pages on your website so that only your paying customers can see them. How could you implement this?

Choose the correct option from the below:

○ **A.** Use HTTPS endpoints to encrypt your data.

○ **B.** You can use a bucket policy and check for the AWS: Referer key in a condition, where that key matches your domain ✓

○ **C.** You can't. The S3 URL must be public in order to use it on your website.

○ **D.** You can use server-side and client-side encryption, where only your application can decrypt the objects

Explanation :

Answer – B

Suppose you have a website with the domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket, examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them.

To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using theaws:referer key, that the get request must originate from specific web pages.

Option A is incorrect because HTTPS endpoint will not ensure that only authenticated users can get access to the content.
Option B is CORRECT because it defines appropriate bucket policy to give the access to the S3 content to the authenticated users.
Option C is incorrect because you can control the access to the S3 content via bucket policy.
Option D is incorrect because the question is not about encrypting/decrypting the data. To give access to the S3 content to certain users, proper bucket policy needs to be defined.

For more information on S3 bucket policy examples, please visit the link
http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html)

Ask our Experts

👍 👎

QUESTION 40 UNATTEMPTED DEPLOYMENT MANAGEMENT

While hosting a static website with Amazon S3, your static JavaScript code attempts to include resources from another S3 bucket but permission is denied. How might you solve the problem?

Choose the correct option from the below:

○ **A.** Enable CORS Configuration ✔

○ **B.** Disable Public Object Permissions

○ **C.** Move the object to the main bucket

○ **D.** None of the above

Explanation :

Answer – A

Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support in Amazon S3, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.

For more information on S3 CORS configuration, please visit the link
http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html)

Ask our Experts

👍 👎

QUESTION 41 UNATTEMPTED SCALABILITY & ELASTICITY

You are having trouble maintaining session states on some of your applications that are using an Elastic Load Balancer(ELB). There does not seem to be an even distribution of sessions across your ELB. Which of the following is the recommended method by AWS to try and rectify the issues to overcome this problem that you are having?

Choose the correct option from the below:

○ **A.** Use ElastiCache, which is a web service that makes it easy to set up, manage, and scale a distributed in-memory cache environment in the cloud. ✓

○ **B.** Use a special cookie to track the instance for each request to each listener. When the load balancer receives a request, it will then check to see if this cookie is present in the request.

○ **C.** Use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.

○ **D.** If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration.

Explanation :

Answer – A

Option A is CORRECT because ElastiCache can be utilized to store the session state in cache rather than in any database. It also improves the performance by allowing you to quickly retrieve the session state information.
Option B and D are incorrect because the cookies will only help identifying the instance which would be tied to the request. It will not store any session state.
Option C is incorrect because sticky session allows the ELB to bind the user session to a particular instance, but it will not store any session state.

More information on Amazon ElastiCache
Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring, and operation of in-memory environments, enabling your engineering resources to focus on developing applications. Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries but also reduce the cost associated with scaling web applications.
As an example for application session stickiness using Elastic cache, please refer to the below link
https://aws.amazon.com/blogs/developer/elasticache-as-an-asp-net-session-store/
(https://aws.amazon.com/blogs/developer/elasticache-as-an-asp-net-session-store/)

Ask our Experts

👍 👎

QUESTION 42 UNATTEMPTED NETWORK DESIGN

You are deploying your first EC2 instance in AWS and are using the AWS console to do this. You have chosen your AMI and your instance type and have now come to the screen where you configure your instance details. One of the things that you need to decide is whether you want to auto-assign a public IP address or not. You assume that if you do not choose this option you will be able to assign an Elastic IP address later, which happens to be a correct assumption. Which of the below options best describes why an Elastic IP address would be preferable to a public IP address?

Choose the correct option from the below:

○ **A.** An Elastic IP address is free, whilst you must pay for a public IP address.

○ **B.** With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. ✓

○ **C.** You can have an unlimited amount of Elastic IP addresses, however public IP addresses are limited in number.

○ **D.** An Elastic IP address cannot be accessed from the internet like a public IP address and hence is safer from a security standpoint.

Explanation :

Answer – B

Option A is incorrect because public IP addresses are free.
Option B is CORRECT because in case of an instance failure, you can reassign the EIP to a new instance, thus you do not need to change any reference to the IP address in your application.
Option C is incorrect because the number of EIPs per account per region is limited (5).
Option D is incorrect because EIPs are accessible from the internet.

More information on EIPs
An *Elastic IP address* is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet; for example, to connect to your instance from your local computer.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html)

Ask our Experts

👍 👎

QUESTION 43 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have an EBS root device on /dev/sda1 on one of your EC2 instances. You are having trouble with this particular instance and you want to either Stop/Start, Reboot or Terminate the instance but you do not want to lose any data that you have stored on /dev/sda1. Which of the below statements best describes the effect each change of instance state would have on the data you have stored on /dev/sda1?

Choose the correct option from the below:

○ **A.** Whether you stop/start, reboot or terminate the instance it does not matter because data on an EBS volume is not ephemeral and the data will not be lost regardless of what method is used

○ **B.** Whether you stop/start, reboot or terminate the instance it does not matter because data on an EBS volume is ephemeral and it will be lost no matter what method is used.

○ **C.** If you stop/start the instance the data will not be lost. However, if you either terminate or reboot the instance the data will be lost.

○ **D.** The data in root EBS volume is not permanent with default setting - it only persists during the lifetime of the instance. The data will be lost if you terminate the instance. However, the data will remain on /dev/sda1 if you reboot or stop/start the instance because data on an EBS volume is not ephemeral. ✓

Explanation :

Answer – D

Since this is an EBS backed instance, it can be stopped and later restarted without affecting data stored in the attached volumes. By default, the root device volume for this instance will be deleted when the instance terminates.

Option A is incorrect because upon termination, the volume would get deleted and the data would get lost (DeleteOnTermination setting is not mentioned, so this is a default case).

Option B is incorrect because the data on EBS volume would not get lost upon stop/start or reboot.
Option C is incorrect because the data on EBS volume would not get lost upon reboot.
Option D is CORRECT because the data on EBS volume would not get lost upon stop/start or reboot as it is not ephemeral. Instance store, on the other hand, is an ephemeral storage and the data would get lost upon starting/stopping of the instance.

More information on this topic:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html)
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html)

Ask our Experts

👍 👎

QUESTION 44 UNATTEMPTED NETWORK DESIGN

Someone on your team configured a Virtual Private Cloud with two public subnets in two separate AZs and two private subnets in two separate AZs. Each public subnet AZ has a matching private subnet AZ. The VPC and its subnets are properly configured. You also notice that there are multiple webserver instances in the private subnet, and you've been charged with setting up a public-facing Elastic Load Balancer which will accept requests from clients and distribute those requests to the webserver instances. How can you set this up without making any significant architectural changes?

Choose the correct option from the below:

○ **A.** Select both of the private subnets which contain the webserver instances when configuring the ELB.

○ **B.** Put the webserver instances in the public subnets and then configure the ELB with those subnets.

○ **C.** Select both of the public subnets when configuring the ELB. ✓

○ **D.** You can't. Webserver instances must be in public subnets in order for this to work.

Explanation :

Answer – C

Option A is incorrect because you need to setup the internet facing load balancer, to which the public subnets need to be associated.
Option B is incorrect because webservers need to remain in the private subnets. Shifting them to the public subnet would be a significant architectural change.
Option C is CORRECT because you need to associate the public subnets with the internet facing load balancer. You would also need to ensure that the security group that is assigned to the load balancer has the listener ports open and the security groups of the private instances allow traffic on the listener ports and the health check ports.
Option D is incorrect because you can configure the internet facing load balancer with the public subnet.

For more information on the AWS ELB, please refer to the below link:
https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/ (https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/)
https://aws.amazon.com/elasticloadbalancing/classicloadbalancer/
(https://aws.amazon.com/elasticloadbalancing/classicloadbalancer/)

Ask our Experts

👍 👎

QUESTION 45 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A company has hired you to assist with the migration of an interactive website that allows registered users to rate local restaurants. Updates to the ratings are displayed on the home page and ratings are updated in real time. Although the website is not very popular today, the company anticipates that it will grow over the next few weeks. They also want to ensure that the website to remain highly available. The current architecture consists of a single Windows server 2008R2 web server and a MySQL database on Linux. Both reside inside on an on-premise hypervisor. What would be the most efficient way to transfer the application to AWS, ensuring high performance and availability?

○ **A.** Launch one Windows Server 2008 R2 instance in us-west-1b and one in us-west-1a and configure auto-scaling. Copy the web files from on premises web server to each Amazon EC2 web server, using Amazon S3 as the repository. Launch a multi AZ MySQL Amazon RDS Instance in us-west-1a and us-west-1b. Import the data into Amazon RDS from the latest MySQL backup. Create an elastic load balancer (ELB) to front your web servers. Use Route 53 and create an alias record pointing to the ELB. ✓

○ **B.** Export web files to an Amazon S3 bucket in us-west-1. Run the website directly out of Amazon S3. Launch a multi-AZ MySQL Amazon RDS instance in us-west-1a. Import the data into Amazon RDS from the latest MySQL backup. Use Route 53 and create an alias record pointing to the elastic load balancer.

○ **C.** Use AWS VM Import/Export to create an Amazon EC2 AMI of the web server. Configure auto-scaling to launch one web server in us-west-1a and one in us-west-1b. Launch a multi-AZ MySQL Amazon RDS instance in us-west-1. Import the data Into Amazon RDS from the latest MySQL backup. Create an elastic load balancer (ELB) in front of your web servers. Use Amazon Route 53 and create an A record pointing to the ELB.

○ **D.** Use AWS VM Import/Export to create an Amazon EC2 AMI of the web server. Configure auto-scaling to launch one web server in us-west-1a and one in us-west-1b. Launch a Multi-AZ MySQL Amazon RDS instance in us-west-1. Import the data into Amazon RDS from the latest MySQL backup. Use Amazon Route 53 to create a hosted zone and point an A record to the elastic load balancer.

Explanation :

Answer – A

The main consideration in the question is that the architecture should be highly available with high performance.

Option A is CORRECT because (a) EC2 servers can communicate with S3 for the web files, and (b) auto-scaling of web servers and the setup of Multi-AZ RDS instance as well as the Route 53 alias record with ELB provides high availability.
Option B is incorrect because this is an interactive website and S3 is suitable for static website.
Option C is incorrect because Route 53 should create an Alias Record, not A record.
Option D is incorrect because, even though it tries to set up the ELB with Route 53 record set, it actually does not create an ELB.
For more information, please refer to the below URL
http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html)

Ask our Experts

👍 👎

QUESTION 46 UNATTEMPTED DATA STORAGE

You have been asked to design the storage layer for an application. The application requires disk performance of at least 100,000 IOPS. In addition, the storage layer must be able to survive the loss of an individual disk, EC2 instance, or Availability Zone without any data loss. The volume you provide must have a capacity of at least 3 TB. Which of the following designs will meet these objectives?

○ **A.** Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Provision 3×1 TB EBS volumes attach them to the instance and configure them as a second RAID 0 volume. Configure synchronous, block-level replication from the ephemeral backed volume to the EBS-backed volume.

○ **B.** Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the Instance Configure synchronous block-level replication to an identically configured instance in us-east-1b. ✔

○ **C.** Instantiate a c3.8xlarge instance in us-east-1. Provision an AWS Storage Gateway and configure it for 3 TB of storage and 100,000 IOPS. Attach the volume to the instance.

○ **D.** Instantiate a c3.8xlarge instance in us-east-1 provision 4x1TB EBS volumes, attach them to the instance, and configure them as a single RAID 5 volume Ensure that EBS snapshots are performed every 15 minutes.

○ **E.** Instantiate a c3 8xlarge Instance in us-east-1 Provision 3x1TB EBS volumes attach them to the instance, and configure them as a single RAID 0 volume. Ensure that EBS snapshots are performed every 15 minutes.

Explanation :

Answer - B

Option A is incorrect because this configuration is done entirely in a single AZ. There will be a data loss if the entire AZ goes down.

Option B is CORRECT because (a) it uses RAID 0 configuration that utilizes all the volumes and gives the aggregated IOPS performance, and (b) the replication across another AZ gives higher availability and fault tolerance even in case of an entire AZ becomes unavailable.

Option C is incorrect because it uses asynchronous backup of the data. The problem scenario demands a synchronous replication to prevent any data loss.

Option D is incorrect because, RAID 5 is not recommended for Amazon EBS since the parity write operations consume some of the IOPS available to the volumes. See the link below for more details.

- http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/raid-config.html (http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/raid-config.html)
- https://en.wikipedia.org/wiki/Standard_RAID_levels (https://en.wikipedia.org/wiki/Standard_RAID_levels)

Option E is incorrect because, even if the snapshots are taken every 15 minutes, there are chances that there will be data loss during this time. The requirement is that there should be absolutely no data loss.

Ask our Experts

👍 👎

QUESTION 47 UNATTEMPTED SECURITY

There are currently multiple applications hosted in a VPC. During monitoring, it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Addresses?

○ **A.** Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.

○ **B.** Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block ✔

○ **C.** Add a rule to all of the VPC Security Groups to deny access from the IP Address block

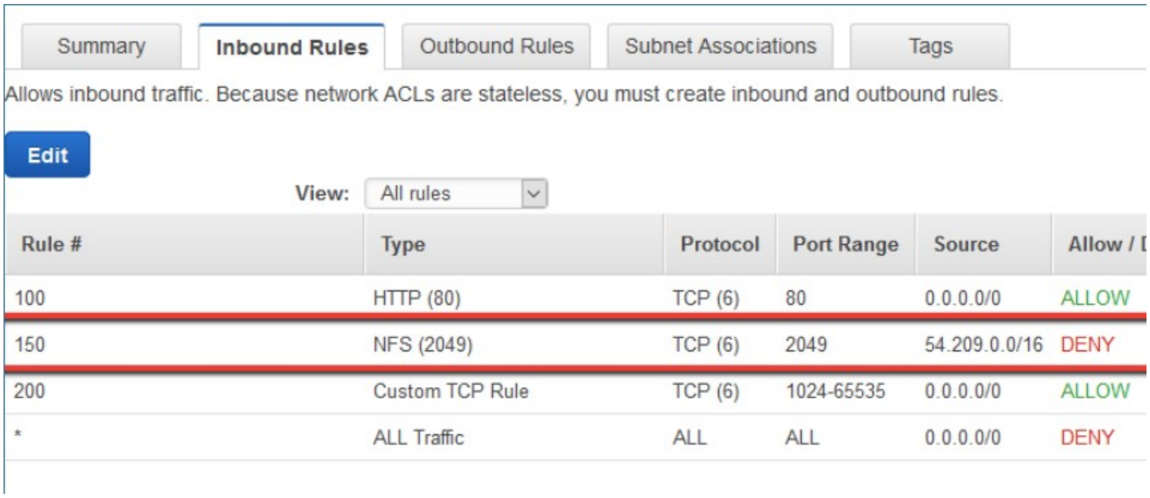
○ **D.** Modify the Windows Firewall settings on all AMI's that your organization uses in that VPC to deny access from the IP address block

Explanation :

Answer – B

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

Option A and D are incorrect because (a) it will only work for windows-based instances, and (b) better approach is to block the traffic at the subnet layer via NACL rather than instance layer (windows firewall).
Option B is CORRECT because the best way to allow or deny IP address-based access to the resources in the VPC is to configure rules in the Network access control list (NACL) which are applied at the subnet level.
Option C is incorrect because (a) you cannot explicitly deny access to particular IP addresses via security group, and (b) better approach is to block the traffic at the subnet layer via NACL rather than instance layer (security group).



Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow /
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
150	NFS (2049)	TCP (6)	2049	54.209.0.0/16	DENY
200	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

For more information on network ACL's please refer to the below link
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

Ask our Experts

QUESTION 48 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have been asked to leverage Amazon VPC EC2 and SQS to implement an application that submits and receives millions of messages per second to a message queue. You want to ensure that your application has sufficient bandwidth between your EC2 instances and SQS. Which option will provide the most scalable solution for communicating between the application and SQS?

○ **A.** Ensure the application instances are properly configured with an Elastic Load Balancer.

○ **B.** Ensure the application instances are launched in private subnets with the EBS-optimized option enabled.

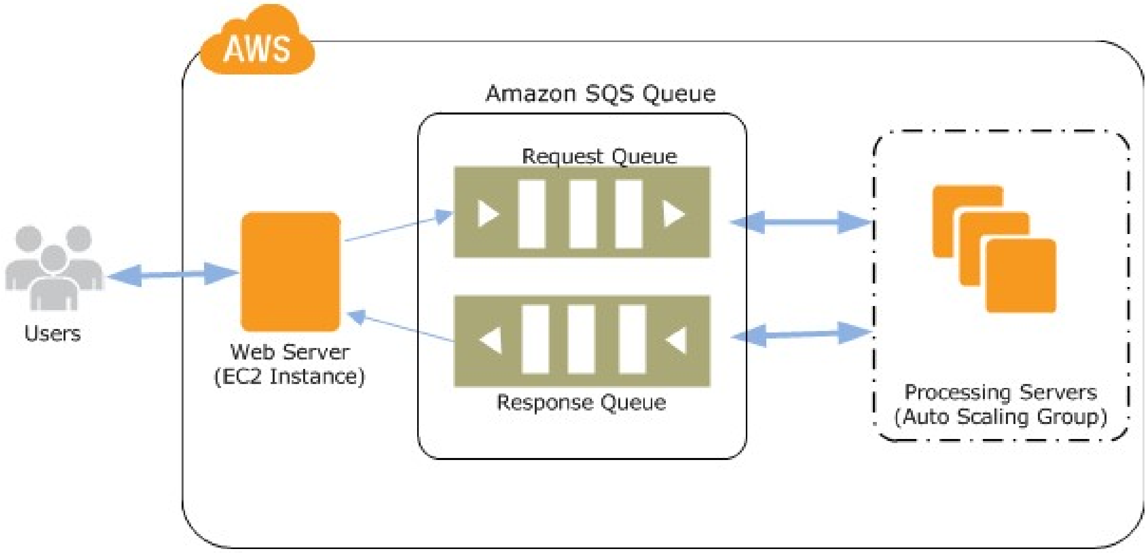
○ **C.** Ensure the application instances are launched in private subnets with the associate-public-IP-address=true option enabled. Remove any NAT instance from the public subnet, if any.

○ **D.** Ensure the application instances are launched in public subnets with an Auto Scaling group and Auto Scaling triggers are configured to watch the SQS queue size. ✓

Explanation :

Answer – D
For the exam, remember that Amazon SQS is an Internet-based service. To connect to the Amazon SQS Endpoint (sqs.us-east-1.amazonaws.com), the Amazon EC2 instance requires access to the Internet. Hence, either it should be in a public subnet or be in a private subnet with a NAT instance/gateway in the public subnet.

Option A is incorrect because ELB does not ensure scalability.
Option B is incorrect because (a) EBS-optimized option will not contribute to scalability, and (b) there should be a NAT instance/gateway in the public subnet of the VPC for accessing SQS.
Option C is incorrect because if you remove the NAT instance, the EC2 instance cannot access SQS service.
Option D is CORRECT because (a) it uses Auto Scaling for ensuring scalability of the application, and (b) it has instances in the public subnet so they can access the SQS service over the internet.



For more information on SQS, please visit the below URL
https://aws.amazon.com/sqs/faqs/ (https://aws.amazon.com/sqs/faqs/)

Ask our Experts

👍 👎

QUESTION 49 UNATTEMPTED NETWORK DESIGN

You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database. You want to confirm that they can talk to each other for your application to work properly. Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC?

Choose 2 options from the below:

□ **A.** A network ACL that allows communication between the two subnets. ✓

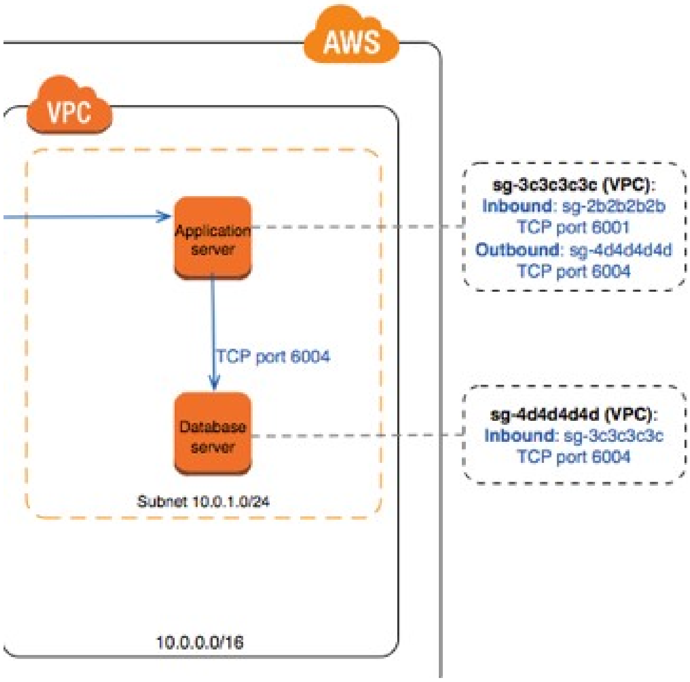
□ **B.** Both instances are the same instance class and using the same Key-pair.

□ **C.** That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.

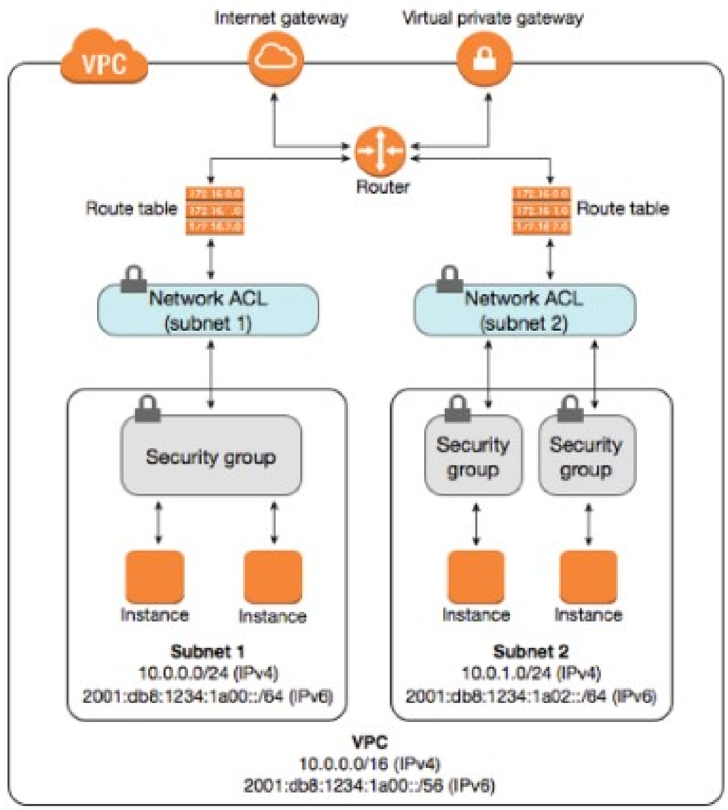
□ **D.** Security groups are set to allow the application host to talk to the database on the right port/protocol. ✓

Explanation :

Answer - A and D
In order to have the instances communicate with each other, you need to properly configure both Security Group and Network access control lists (NACLs). For the exam, remember that Security Group operates at the instance level; where as, the NACL operates at subnet level.
Option A is CORRECT because the security groups must be defined in order to allow web server to communicate with the database server. An example image from the AWS documentation is given below:



Option B is incorrect because it is not necessary to have the two instances of the same type or be using same key-pair.
Option C incorrect is because configuring NAT instance or NAT gateway will not enable the two servers to communicate with each other. NAT instance/NAT gateway are used to enable the communication between instances in the private subnets and internet.
Option D is CORRECT because the two servers are in two separate subnets. In order for them to communicate with each other, you need to have the NACL's configured as shown below:



For more information on VPC and Subnets, please visit the below URL:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Ask our Experts

QUESTION 50 UNATTEMPTED DEPLOYMENT MANAGEMENT

Your team is excited about the use of AWS because now they have access to "programmable Infrastructure". You have been asked to manage your AWS infrastructure In a manner similar to the way you might manage application code. You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development test QA . production). Which approach addresses this requirement?

○ **A.** Use cost allocation reports and AWS Opsworks to deploy and manage your infrastructure.

○ **B.** Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure.

○ **C.** Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure.

○ **D.** Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure. ✓

Explanation :

Answer – D

You can use AWS Cloud Formation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer.

Option A is incorrect because Cost Allocation Reports is not helpful for the purpose of the question.
Option B is incorrect because CloudWatch is used for monitoring the metrics pertaining to different AWS resources.
Option C is incorrect because it does not have the concept of programmable Infrastructure.
Option D is CORRECT because AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

For more information on CloudFormation, please visit the link:
https://aws.amazon.com/cloudformation/ (https://aws.amazon.com/cloudformation/)

Ask our Experts

👍 👎

QUESTION 51 UNATTEMPTED DEPLOYMENT MANAGEMENT

An organization is planning to use AWS for their production roll out. The organization wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3 and setup the ELB.

Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?

○ **A.** AWS Elastic Beanstalk ✓

○ **B.** AWS Cloudfront

○ **C.** AWS Cloudformation

○ **D.** AWS DevOps

Explanation :

Answer – A
The Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services.

We can simply upload code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Meanwhile we can retain full control over the AWS resources used in the application and can access the underlying resources at any time.
Hence, A is the CORRECT answer.
For more information on launching a LAMP stack with Elastic Beanstalk:

- https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/ (https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/)

Note:
Even though i believe AWS Cloudformation can be correct for the a answer for this question, the context for the question points us to AWS Elastic Beanstalk.

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services.

We can simply upload code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Meanwhile we can retain full control over the AWS resources used in the application and can access the underlying resources at any time.

Launch LAMP stack with Elastic Beanstalk:

- https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/ (https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/)

We can do it on AWS CloudFormation as well, but it’s harder and less native:

- http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html (http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html)

Ask our Experts

👍 👎

QUESTION 52 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A user is accessing RDS from an application. The user has enabled the Multi-AZ feature with the MS SQL RDS DB. During a planned outage how will AWS ensure that a switch from DB to a standby replica will not affect access to the application?

○ **A.** RDS will have an internal IP which will redirect all requests to the new DB

○ **B.** RDS uses DNS to switch over to stand by replica for seamless transition ✓

○ **C.** The switch over changes hardware so RDS does not need to worry about access

○ **D.** RDS will have both the DBs running independently and the user has to manually switch over

Explanation :

Answer – B

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure (for example, instance hardware failure, storage failure, or network disruption), Amazon RDS performs an automatic failover to the standby by changing the CNAME for the DB instance to point to the standby, so that you can resume database operations as soon as the failover is complete.

Option A is incorrect because there is no internal IP that is maintained by RDS.
Option B is CORRECT because, as mentioned above, RDS performs automatic failover by flipping the CNAME for the DB instance from primary to standby instance.
Option C is incorrect because there is no changes done by RDS in the hardware.
Option D is incorrect because with Multi-AZ there is no manual intervention needed for the failover.

For more information on RDS Multi-AZ please visit the link –
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html
(http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html)

Ask our Experts

👍 👎

QUESTION 53 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A user has launched a large EBS backed EC2 instance in the US-East-1a region. The user wants to achieve Disaster Recovery (DR) for that instance by creating another small instance in Europe. How can the user achieve DR?

○ **A.** Copy the running instance using the “Instance Copy” command to the EU region.

○ **B.** Create an AMI of the instance and copy the AMI to the EU region. Then launch the instance from the EU AMI. ✓

○ **C.** Copy the instance from the US East region to the EU region.

○ **D.** Use the “Launch more like this” option to copy the instance from one region to another.

Explanation :

Answer – B

Option A and C are incorrect because you cannot directly copy the instance. You need to create AMI of each instance.
Option B is CORRECT because if you need an AMI across multiple regions, then you have to copy the AMI across regions. Note that by default AMI’s that you have created will not be available across all regions.
Option D is incorrect because using "Launch More Like This..." enables you to use a current instance as a base for launching other instances in the same availability zone. It does not clone your selected instance; it only replicates some configuration details. To create a copy of your instance, first create an AMI from it, then launch more instances from the AMI.

For the entire details to copy AMI’s, please visit the link -
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html)

Ask our Experts

👍 👎

QUESTION 54 UNATTEMPTED SECURITY

You are managing the AWS account of a big organization. The organization has more than 1000+ employees and they want to provide access to the various services to most of the employees. Which of the below-mentioned options is the best possible solution in this case?

○ **A.** The user should create a separate IAM user for each employee and provide access to them as per the policy.

○ **B.** The user should create an IAM role and attach STS with the role. The user should attach that role to the EC2 instance and setup AWS authentication on that server.

○ **C.** The user should create IAM groups as per the organization's departments and add each user to the group for better access control.

○ **D.** Attach an IAM role with the organization's authentication service to authorize each user for various AWS services. ✓

Explanation :

Answer – D

The best practice for IAM is to create roles which have specific access to an AWS service and then give the user permission to the AWS service via the role.

Option A is incorrect because creating a separate IAM user is not a feasible solution here. Instead, creating an IAM role would be more appropriate solution.
Option B is incorrect because this is an invalid workflow of using IAM roles for authenticating the users.
Option C is incorrect because you should be creating IAM Role rather than IAM Users which will be added to the IAM group.
Option D is CORRECT because it authenticates the users with the organization's authentication service and creates an appropriate IAM Role for accessing the AWS services.

For the best practices on IAM policies, please visit the link
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)

Ask our Experts

👍 👎

QUESTION 55 UNATTEMPTED DEPLOYMENT MANAGEMENT

A user is using CloudFormation to launch an EC2 instance and then planning to configure an application after the instance is launched. The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly. How can the user configure this?

○ **A.** It is not possible that the stack creation will wait until one service is created and launched.

○ **B.** The user can use the HoldCondition resource to wait for the creation of the other dependentresources.

○ **C.** The user can use the DependentCondition resource to hold the creation of the other dependent resources.

○ **D.** The user can use the WaitCondition resource to hold the creation of the other dependent resources. ✔

Explanation :

Answer – D

You can use a wait condition for situations like the following:

- To coordinate stack resource creation with configuration actions that are external to the stack creation
- To track the status of a configuration process

For more information on Cloudformation Wait condition please visit the link http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html (http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html)

Ask our Experts

👍 👎

QUESTION 56 UNATTEMPTED DEPLOYMENT MANAGEMENT

A marketing research company has developed a tracking system that collects user behavior during web marketing campaigns on behalf of the customers all over the world. The tracking system consists of an auto-scaled group of EC2 instances behind an ELB. And the collected data is stored in DynamoDB. After the campaign is terminated the tracking system is torn down and the data is moved to Amazon Redshift, where it is aggregated and used to generate detailed reports.

The company wants to be able to instantiate new tracking systems in any region without any manual intervention and therefore adopted CloudFormation.

What needs to be done to make sure that the AWS Cloudformation template works for every AWS region?

Choose 2 options from the below:

□ **A.** Avoid using Deletion Policies for the EBS snapshots.

□ **B.** The names of the DynamoDB tables must be different in every target region.

□ **C.** Use the built-in function of Cloudformation to set the AZ attribute of the ELB resource. ✓

□ **D.** IAM users with the right to start Cloudformation stacks must be defined for every target region.

□ **E.** Use the built-in Mappings and FindInMap functions of AWS Cloudformation to refer to the AMI ID set in the ImageID attribute of the Autoscaling::LaunchConfiguration resource. ✓

Explanation :

Answer – C and E

Option A is incorrect because you need to retain or keep the snapshots of the EBS volumes in order to launch similar instances in the new region.
Option B is incorrect because DynamoDB table with the same name can be created in different regions. They have to be unique in a single region.
Option C is CORRECT because you need to get the name of the Availability Zone based on the region in which the template would be used.
Option D is incorrect because you do not need to define IAM users per region as they are global.
Option E is CORRECT because the AMI ID would be needed to launch the similar instances in the new region where the template would be used.

More information on CloudFormation intrinsic functions:
You can use the Fn::GetAZs function of CloudFormation to get the AZ of the region and assign it to the ELB.
An example of the Fn::GetAZs function is given below

```
{ "Fn::GetAZs" : "" }
{ "Fn::GetAZs" : { "Ref" : "AWS::Region" } }
{ "Fn::GetAZs" : "us-east-1" }
```

An example of the FindInMap is shown below. This is useful when you want to get particular values region wise which can be used as parameters. Since the Launch configuration contains the AMI ID information and since the AMI ID is different in different regions, you need to recreate the Launch Configurations based on the AMI ID.

```
{
 ...
 "Mappings" : {
   "RegionMap" : {
     "us-east-1" : { "32" : "ami-6411e20d", "64" : "ami-7a11e213" },
     "us-west-1" : { "32" : "ami-c9c7978c", "64" : "ami-cfc7978a" },
     "eu-west-1" : { "32" : "ami-37c2f643", "64" : "ami-31c2f645" },
      "ap-southeast-1" : { "32" : "ami-66f28c34", "64" : "ami-60f28c32" },
      "ap-northeast-1" : { "32" : "ami-9c03a89d", "64" : "ami-a003a8a1" }
  }
 },

 "Resources" : {
   "myEC2Instance" : {
     "Type" : "AWS::EC2::Instance",
     "Properties" : {
        "ImageId" : { "Fn::FindInMap" : [ "RegionMap", { "Ref" : "AWS::Region" }, "32"]},
        "InstanceType" : "m1.small"
      }
    }
  }
}
```

For more information on the Fn::FindInMap function, please refer to below link
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference.html
(https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference.html)
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-findinmap.html
(http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-findinmap.html)

Ask our Experts

QUESTION 57 UNATTEMPTED NETWORK DESIGN

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below-mentioned entries is required in the private subnet database security group DBSecGrp?

○ **A.** Allow Inbound on port 3306 for the source Web Server Security Group WebSecGrp. ✓

○ **B.** Allow Inbound on port 3306 from source 20.0.0.0/16.

○ **C.** Allow Outbound on port 3306 for destination Web Server Security Group WebSecGrp.

○ **D.** Allow Outbound on port 80 for destination NAT instance IP.

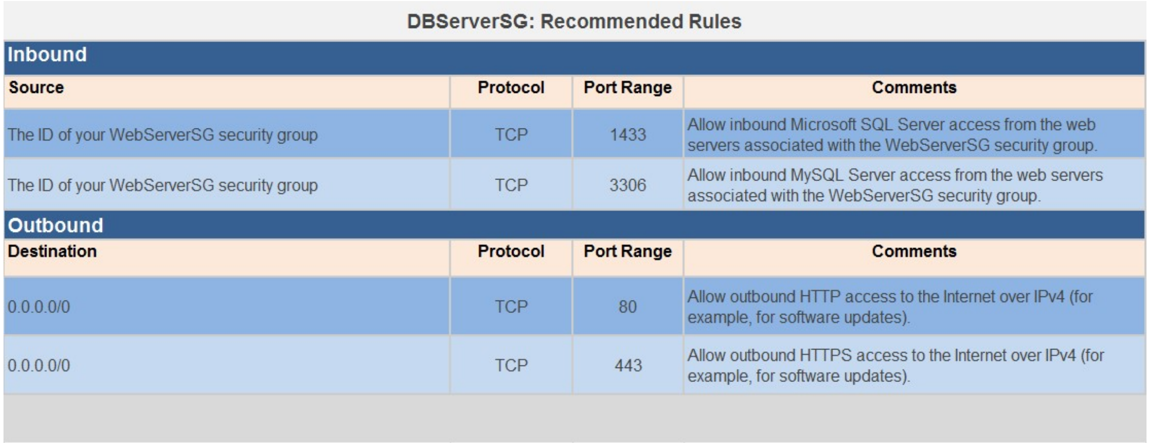
Explanation :

Answer – A

The important point in this question is to allow the incoming traffic to the private subnet on port 3306 only for the instances in the private subnet.

Option A is CORRECT because (a) it allows the inbound traffic only for the required port 3306, and (b) it allows only the traffic from the instances in the public subnet (WebSecGrp).
Option B is incorrect because it is allowing the inbound traffic to all the instances in the VPC which is not the requirement.
Option C is incorrect because defining outbound traffic will not ensure the incoming traffic from the public subnet. Also, since the security groups are stateful, you just need to define the inbound traffic for the public subnet only (WebSecGrp). The outbound traffic would be automatically allowed.
Option D is incorrect because you do not need to open the port 80 in this case.

More information on Web Server and DB Server Security Group settings:
Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the AWS documentation shows how the security groups should be set up.



DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).

For more information on security groups please visit the below link
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts

👍 👎

QUESTION 58 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your customer is implementing a video-on-demand streaming platform on AWS. The requirement is to be able to support multiple devices such as iOS, Android, and Windows as client devices, using a standard client player, using streaming technology and scalable architecture with cost-effectiveness.

Which architecture meets the requirements?

○ **A.** Store the video contents to Amazon Simple Storage Service (S3) as an origin server. Configure the Amazon CloudFront distribution with a streaming option to stream the video contents.

○ **B.** Store the video contents to Amazon S3 as an origin server. Configure the Amazon CloudFront distribution with a download option to stream the video contents ✔

○ **C.** Launch a streaming server on Amazon Elastic Compute Cloud (EC2) (for example, Adobe Media Server), and store the video contents as an origin server. Configure the Amazon CloudFront distribution with a download option to stream the video contents.

○ **D.** Launch a streaming server on Amazon EC2 (for example, Adobe Media Server), and store the video contents as an origin server. Launch and configure the required amount of streaming servers on Amazon EC2 as an edge server to stream the video contents.

Explanation :

Answer – B

Option A is incorrect because it uses CloudFront distribution with streaming option which does not work on all platforms; where as, it should use download option.
Option B is CORRECT because (a) it uses CloudFront distribution with download option for streaming the on demand videos using HLS on any mobile, and (b) it uses S3 as origin, so keeps the cost low.
Option C is incorrect because (a) provisioning streaming EC2 instances is a costly solution, (b) the videos are to be delivered on-demand, not live streaming.
Option D is incorrect because the videos are to be delivered on-demand, not live streaming. So, streaming server is not required.

For more information on live and on-demand streaming using CloudFront, please visit the below URL:

https://aws.amazon.com/blogs/aws/using-amazon-cloudfront-for-video-streaming/ (https://aws.amazon.com/blogs/aws/using-amazon-cloudfront-for-video-streaming/)

Note:

In the on demand streaming case, your video content is stored in Amazon S3. Viewers can choose to watch it at any desired time. A complete on-demand streaming solution typically makes use of Amazon S3 for storage, AWS Elemental MediaConvert for file-based video processing, and Amazon CloudFront for delivery.
Once uploaded, you may need to convert your video into the size, resolution, or format needed by a particular television or connected device. AWS Elemental MediaConvert will take care of this for you. MediaConvert takes content from S3, transcodes it per your request, and stores

the result back in S3. Transcoding processes video files, creating compressed versions of the original content to reduce its size, change its format, or increase playback device compatibility.You can also create assets that vary in resolution and bitrate for adaptive bitrate streaming, which adjusts the viewing quality depending on the viewer's available bandwidth. AWS Elemental MediaConvert outputs the transcoded video to an S3 bucket.
The next step is global delivery with Amazon CloudFront. CloudFront caches content at the edges for low latency and high throughput video delivery. This delivery can be made in two different ways. You can deliver the entire video file to the device before playing it, or you can stream it to the device.

More information is available at:
https://aws.amazon.com/cloudfront/streaming/
(https://aws.amazon.com/cloudfront/streaming/)
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-video.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-video.html)

Ask our Experts

👍 👎

QUESTION 59 UNATTEMPTED SCALABILITY & ELASTICITY

A document storage company is deploying their application to AWS and changing their business model to support both Free Tier and Premium Tier users. The premium Tier users will be allowed to store up to 200GB of data and Free Tier customers will be allowed to store only 5GB. The customer expects that billions of files will be stored. All users need to be alerted when approaching 75 percent quota utilization and again at 90 percent quota use.

To support the Free Tier and Premium Tier users, how should they architect their application?

○ **A.** The company should utilize an Amazon Simple Workflow Service activity worker that updates the user's used data counter in Amazon DynamoDB. The Activity Worker will use Simple Email Service to send an email if the counter increases above the appropriate thresholds. ✓

○ **B.** The company should deploy an Amazon Relational Database Service (RDS) relational database with a stored objects table that has a row for each stored object along with the size of each object. The upload server will query the aggregate consumption of the user in question (by first determining the files stored by the user, and then querying the stored objects table for respective file sizes) and send an email via Amazon Simple Email Service if the thresholds are breached.

○ **C.** The company should write both the content length and the username of the files owner as S3 metadata for the object. They should then create a file watcher to iterate over each object and aggregate the size for each user and send a notification via Amazon Simple Queue Service to an emailing service if the storage threshold is exceeded.

○ **D.** The company should create two separate Amazon Simple Storage Service buckets, one for date storage for Free Tier Users, and another for data storage for Premium Tier users. An Amazon Simple Workflow Service activity worker will query all objects for a given user based on the bucket the data is stored in and aggregate storage. The activity worker will notify the user via Amazon Simple Notification Service when necessary.

Explanation :

Answer – A

Option A is CORRECT because DynamoDB which is highly scalable service is best suitable in this scenario.

Option B is incorrect because RDS would not be a suitable solution for storing billions of files.

Option C and D are both incorrect because it uses object level storage and iterating over billions of objects for each operation is performance-wise not a good option at all.

Ask our Experts

QUESTION 60 UNATTEMPTED SECURITY

You are designing security inside your VPC. You are considering the options for establishing separate security zones, and enforcing network traffic rules across the different zones to limit which instances can communicate. How would you accomplish these requirements?

Choose 2 options from the below:

□ **A.** Configure a security group for every zone. Configure a default allow all rule. Configure explicit deny rules for the zones that shouldn't be able to communicate with one another.

□ **B.** NACLs to explicitly allow or deny communication between the different IP address ranges, as required for inter zone communication. ✓

□ **C.** Configure multiple subnets in your VPC, one for each zone. Configure routing within your VPC in such a way that each subnet only has routes to other subnets with which it needs to communicate, and doesn't have routes to subnets with which it shouldn't be able to communicate.

□ **D.** Configure a security group for every zone. Configure allow rules only between zones that need to be able to communicate with one another. Use the implicit deny all rule to block any other traffic. ✓

Explanation :

Answer - B and D

Option A is incorrect because you cannot set up explicit deny rules in the Security Groups.
Option B is CORRECT because you can explicitly allow or deny traffic based on certain IP address range.
Option C is incorrect because you cannot delete the main route table, but you can replace the main route table with a custom table that you've created (so that this table is the default table each new subnet is associated with).
Option D is CORRECT because Security Group in this case would act like a Firewall that provides security and control at the port/protocol level, and have "implicit deny all" rule and only allow what is needed.

For more information on VPC and subnets, please visit the below URL:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

Note:
If we configure the default routing in a VPC, in such a way that each subnet only has routes to other subnets with which it needs to communicate and doesn't have routes to subnets with which it shouldn't be able to communicate.
By doing this we are restricting the communication of all the instances present in a subnet to communicate with yet another subnet instances; which is not the actual requirement.
Here there is no way to fine control the access to a particular instance where as if we configure the controls at the Security Group level and NACL level it gives us a fine control over the traffic to various instances.
Option D is correct because it will implicitly deny all the traffic and you can then open the port/protocol to only the traffic which is coming from the valid sources..

Ask our Experts

👍 👎

QUESTION 61 UNATTEMPTED SCALABILITY & ELASTICITY

You’ve been tasked with moving an e-commerce web application from a customer’s data center into a VPC. The application must be fault tolerant and well as highly scalable. Moreover, the customer is adamant that service interruptions not affect the user experience. As you near launch, you discover that the application currently uses multicast to share session state between web servers. In order to handle session state within the VPC, you choose to which of the following option:

○ **A.** Enable session stickiness via Elastic Load Balancing.

○ **B.** Store session state in Amazon ElastiCache for Redis. ✓

○ **C.** Create a mesh VPN between instances and allow multicast on it.

○ **D.** Store session state in Amazon Relational Database Service.

Explanation :

Answer – B

Option A is incorrect because ELB does not help in storing the state; it only routes the traffic by session cookie. If the EC2 instance fails, the session will be lost.
Option B is CORRECT because Redis is a fast, open source, in-memory data store and caching service. It is highly available, reliable, and with high performance suitable for the most demanding applications such as this one.
Option C is incorrect because Mesh VPN is just not fault tolerant or highly scalable - the client's real priorities. It's failure would impact users. The supernode that handles the registration is a single point of failure and in case of failure, new VPN nodes would not be able to register. Also, the nodes would't register across multiple AZs. Even if it is possible it is very cumbersome.
Option D is incorrect because RDS is not highly scalable.

For more information on Elastic Cache, please visit the below URL:
https://aws.amazon.com/elasticache/ (https://aws.amazon.com/elasticache/)

Note:
Our main requirement is to provide fault tolerance and high scalability.

Redis data resides in-memory, in contrast to databases that store data on disk or SSDs. By eliminating the need to access disks, in-memory data stores such as Redis avoid seek time delays and can access data in microseconds. Redis is a popular choice for caching, session management, real-time analytics, geospatial, chat/messaging, media streaming, and gaming leaderboards.

ElastiCache Redis can provide high scalability and is fault tolerant.

Ask our Experts

👍 👎

QUESTION 62 UNATTEMPTED SECURITY

Your company is migrating infrastructure to AWS. A large number of developers and administrators will need to control this infrastructure using the AWS Management Console. The Identity Management team is objecting to creating an entirely new directory of IAM users for all employees, and the employees are reluctant to commit yet another password to memory.

Which of the following will satisfy both these stakeholders?

○ **A.** Users sign in using an OpenID Connect (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the AWS Management Console.

○ **B.** Users log in directly to the AWS Management Console using the credentials from your on-premises Kerberos compliant Identity provider.

○ **C.** Users log in to the AWS Management Console using the AWS Command Line Interface.

○ **D.** Users request a SAML assertion from your on-premises SAML 2.0-compliant identity provider (IdP) and use that assertion to obtain federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint. ✓

Explanation :

Answer – D

Option A is incorrect because, although it is a workable solution, the users need not use the OpenID IdP (such as Facebook, Google, SalesForce etc.)in this scenario as they can use the on-premises 2.0 SAML compliant IdP and get the federated access to the AWS. Access via OpenID IdP is most suitable for the mobile apps.
Option B is incorrect because you cannot login to AWS using the IdP provided credentials. You need temporary credentials provided by Security Token Service (STS) for that.
Option C is incorrect because you should avoid using Access Key and Secret Key for the login. This is the least secure way to login.
Option D is CORRECT because it uses the on-premises 2.0 SAML compliant IdP and get the federated access to the AWS, thus avoiding creating any IAM User for the employees in the organization.

For more information on SAML Authentication in AWS, please visit the below URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html)

Ask our Experts

👍 👎

QUESTION 63 UNATTEMPTED DEPLOYMENT MANAGEMENT

A gaming company adopted AWS Cloud Formation to automate load-testing of their games. They have created an AWS Cloud Formation template for each gaming environment including one for the load-testing stack. The load-testing stack creates an Amazon Relational Database Service (RDS) Postgres database and two web servers running on Amazon Elastic Compute Cloud (EC2) that send HTTP requests, measure response times, and write the results into the database. A test run usually takes between 15 and 30 minutes. Once the tests are done, the AWS Cloud Formation stacks are torn down immediately. The test results written to the Amazon RDS database must remain accessible for visualization and analysis. Select possible solutions that allow access to the test results after the AWS Cloud Formation load -testing stack is deleted.

Choose 2 options from the below:.

□ **A.** Define an Amazon RDS Read-Replica in the load-testing AWS CloudFormation stack and define a dependency relation between master and replica via the DependsOn attribute.

□ **B.** Define an update policy to prevent deletion of the Amazon RDS database after the AWS CloudFormation stack is deleted.

□ **C.** Define a deletion policy of type Retain for the Amazon RDS resource to assure that the RDS database is not deleted with the AWS CloudFormation stack. ✓

□ **D.** Define a deletion policy of type Snapshot for the Amazon RDS resource to assure that the RDS database can be restored after the AWS CloudFormation stack is deleted. ✓

□ **E.** Define automated backups with a backup retention period of 30 days for the Amazon RDS database and perform point-in-time recovery of the database after the AWS CloudFormation stack is deleted.

Explanation :

Answer – C and D

Option A is incorrect because (a) creation of read replicas is not needed in this scenario, and (b) they would anyways be deleted after the stacks get deleted, so there is no need to define any dependency in the template.
Option B is incorrect because UpdatePolicy attribute is only applicable to certain resources like AutoScalingGroup, AWS Lambda Alias. It is not applicable to RDS.
Option C is CORRECT because, with Retain deletion policy, the RDS resources would be preserved for the visualization and analysis after the stack gets deleted.
Option D is CORRECT because, with the Snapshot deletion policy, a snapshot of the RDS instance would get created for visualization and analysis later after the stack gets deleted.
Option E is incorrect because automated snapshots are not needed in this case. All that is needed is a single snapshot of the RDS instance after the test gets finished - which can be taken via Snapshot deletion policy.

NOTE: This question is asking for two possible answers. It does not say that both need to be used at the same time. Hence both C and D are valid options.

For more information on deletion policy, please visit the below URL:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html
(http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html)

Ask our Experts

👍 👎

QUESTION 64 UNATTEMPTED SECURITY

A large enterprise wants to adopt Cloud Formation to automate administrative tasks and implement the security principles of least privilege and separation of duties. They have identified the following roles with the corresponding tasks in the company:

Network administrators: create, modify and delete VPCs, subnets, NACLs, routing tables and security groups.
Application operators: deploy complete application stacks (ELB, Auto-Scaling groups, RDS) whereas all resources must be deployed in the VPCs managed by the network administrators.
Both groups must maintain their own Cloud Formation templates and should

be able to create, update and delete only their own Cloud Formation stacks.

The company has followed your advice to create two IAM groups, one for applications and one for networks. Both IAM groups are attached to IAM policies that grant rights to perform the necessary task of each group as well as the creation, update, and deletion of Cloud Formation stacks.

Given setup and requirements, which statements represent valid design considerations?

Choose 2 options from the below:

□ **A.** Network stack updates will fail upon attempts to delete a subnet with EC2 instances. ✓

□ **B.** Restricting the launch of EC2 instances into VPCs requires resource level permissions in the IAM policy of the application group. ✓

□ **C.** Nesting network stacks within application stacks simplifies management and debugging, but requires resource level permissions in the IAM policy of the network group.

□ **D.** The application stack cannot be deleted before all network stacks are deleted.

□ **E.** Unless resource level permissions are used on the cloud formation: Delete Stack action, network administrators could tear down application stacks.

Explanation :

Answer – A and B

Option A is CORRECT because subnets cannot be deleted with instances in them.
Option B is CORRECT because to explicitly launch instances, we need IAM permissions.
Option C is incorrect because even though stacks can be nested, Network group needs all the application group permissions.
Option D is incorrect because application stack can be deleted before network stack.
Option E is incorrect because network administrators have no rights to delete application stack.

For more information, please visit the below URL:
https://aws.amazon.com/blogs/devops/aws-cloudformation-security-best-practices/
(https://aws.amazon.com/blogs/devops/aws-cloudformation-security-best-practices/)

Ask our Experts

👍 👎

QUESTION 65 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

An Enterprise customer is starting their migration to the cloud, their main reason for migrating is agility, and they want to make their internal Microsoft Active Directory available to any applications running on AWS; this is so internal users only have to remember one set of credentials and as a central point of user control for leavers and joiners. How could they make their Active Directory secure, and highly available, with minimal on-premises infrastructure changes, in the most cost and time-efficient way?

Choose the most appropriate option from the below:

○ **A.** Using Amazon Elastic Compute Cloud (EC2), they could create a DMZ using a security group; within the security group they could provision two smaller Amazon EC2 instances that are running Openswan for resilient IPSec tunnels, and two larger instances that are domain controllers; they would use multiple Availability Zones.

○ **B.** Using VPC, they could create an extension to their data center and make use of resilient hardware IPSec tunnels; they could then have two domain controller instances that are joined to their existing domain and reside within different subnets, in different Availability Zones. ✓

○ **C.** Within the customer's existing infrastructure, they could provision new hardware to run Active Directory Federation Services; this would present Active Directory as a SAML2 endpoint on the internet; any new application on AWS could be written to authenticate using SAML2

○ **D.** The customer could create a stand-alone VPC with its own Active Directory Domain Controllers; two domain controller instances could be configured, one in each Availability Zone; new applications would authenticate with those domain controllers.

Explanation :

Answer – B

Option A incorrect because it is just a complicated environment to setup and does not meet the purpose of the requirement.
Option B is CORRECT because using an IPSec tunnel can help decrypt all the traffic from the on-premise to AWS. The domain controllers in separate AZ’s can address high availability.
Option C is incorrect because the question mentions that they want minimal changes to the on-premise environment.
Option D is incorrect because it does not address the secure communication part from on-premise to AWS.

For more information on creating VPN tunnels using Hardware VPN and Virtual private gateways, please refer to the below link
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts

👍 👎

QUESTION 66 UNATTEMPTED SECURITY

An AWS customer is deploying a web application that is composed of a front end running on Amazon EC2 and confidential data that is stored on Amazon S3.

The customer's Security policy requires that the all-access operations to this sensitive data must be authenticated and authorized by a centralized access management system that is operated by a separate security team.

In addition, the web application team that owns and administers the EC2 web front-end instances is prohibited from having any ability to access the data that circumvents this centralized access management system.

Which of the following configurations will support these requirements:

^

○ **A.** Configure the web application to authenticate end users against the centralized access management system. Have the web application provision trusted users STS tokens entitling the download of approved data directly from Amazon S3. ✔

○ **B.** Encrypt the data on Amazon S3 using a CloudHSM that is operated by the separate security team. Configure the web application to integrate with the CloudHSM for decrypting approved data access operations for trusted end users.

○ **C.** Configure the web application to authenticate end users against the centralized access management system using SAML. Have the end users authenticate to IAM using their SAML token and download the approved data directly from Amazon S3.

○ **D.** Have the separate security team create an IAM Role that is entitled to access the data on Amazon S3. Have the web application team provision their instances with this Role while denying their IAM users access to the data on Amazon S3.

Explanation :

Answer – A

Option A is CORRECT because the access to the sensitive data on Amazon S3 is only given to the authenticated users.
Option B is incorrect because S3 doesn't integrate directly with CloudHSM, also there is no centralized access management system control.
Option C is incorrect because this is an incorrect workflow of use of SAML and it does not mention if the centralized access management system is SAML complaint.
Option D is incorrect because with this configuration the web team would have access to the sensitive data on S3.

For more information on STS, please refer to the URL:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

Ask our Experts

QUESTION 67 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A customer is running an application in the US-West region and wants to set up disaster recovery failover to Singapore region. The customer is interested in achieving a low RPO for an RDS multi-AZ DB instance. Which approach is best suited to this need?

○ **A.** Synchronous replication

○ **B.** Asynchronous replication ✓

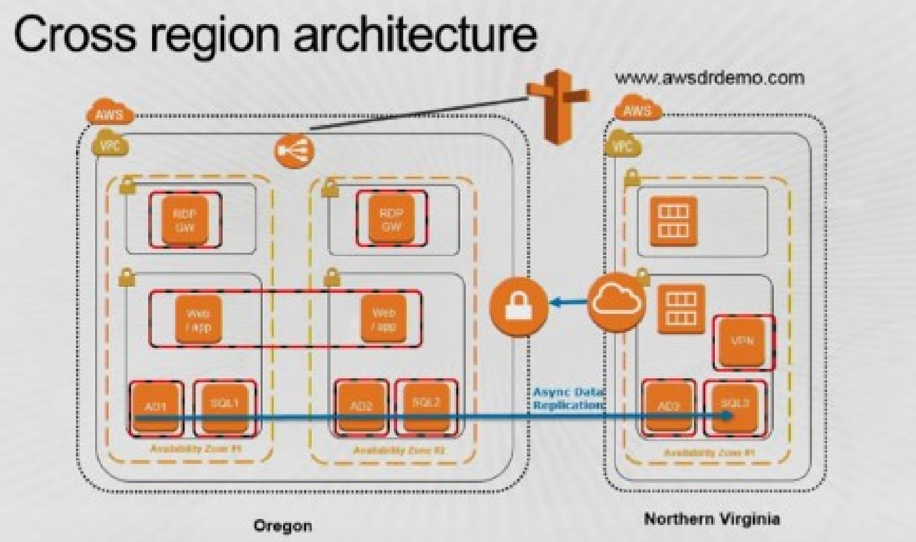
○ **C.** Route53 health checks

○ **D.** Copying of RDS incremental snapshots

Explanation :

Answer – B

When you have cross-region replication for RDS, this is done Asynchronously. Having Synchronous replication would be too much of an overhead for a cross-region replication.



Please refer to a blog article for cross-region replication for MySQL
https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/
(https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/)

Ask our Experts

👍 👎

QUESTION 68 UNATTEMPTED SCALABILITY & ELASTICITY

A public archives organization is about to move a pilot application they are running on AWS into production. You have been hired to analyze their application architecture and give cost-saving recommendations. The application displays scanned historical documents.

Each document is split into individual image tiles at multiple zoom levels to improve responsiveness and ease of use for the end users. At maximum zoom level the average document will be 8000 X 6000 pixels in size, split into multiple 40px X 40px image tiles. The tiles are batch processed by Amazon Elastic Compute Cloud (EC2) instances and put into an Amazon Simple Storage Service (S3) bucket. A browser-based JavaScript viewer fetches tiles from the Amazon (S3) bucket and displays them to users as they zoom and pan around each document. The average storage size of all zoom levels for a document is approximately 30MB of JPEG tiles. Originals of each document are archived in Amazon Glacier. The company expects to process and host over 500,000 scanned documents in the first year. What are your recommendations?

Choose 3 options from the below:

- □ **A.** Deploy an Amazon CloudFront distribution in front of the Amazon S3 tiles bucket. ✓
- □ **B.** Increase the size (width/height) of the individual tiles at the maximum zoom level. ✓
- □ **C.** Use Amazon S3 Reduced Redundancy Storage for each zoom level. ✓
- □ **D.** Decrease the size (width/height) of the individual tiles at the maximum zoom level.
- □ **E.** Store the maximum zoom level in the low cost Amazon S3 Glacier option and only retrieve the most frequently access tiles as they are requested by users.

^

Explanation :

Answer – A, B, and C

Option A is CORRECT because the caching is done by CloudFront via the edge locations which reduces the load on the origin.
Option B is CORRECT because increasing the size of the images would help reduce the cost of number of GET/PUT requests on the origin server.
Option C is CORRECT because RRS is a low cost storage option and will help keeping the overall cost low.
Option D is incorrect because decreasing the size would require more requests and will increase the overall cost.
Option E is incorrect because Glacier is an archival solution and will not be suitable for frequent access of the tiles.

Ask our Experts

QUESTION 69 UNATTEMPTED NETWORK DESIGN

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user's data center. The user's data center has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-12345) to allow traffic to the internet from the VPN subnet. Which of the below-mentioned options is not a valid entry for the main route table in this scenario?

○ **A.** Destination: 20.0.1.0/24 and Target: i-12345 ✓

○ **B.** Destination: 0.0.0.0/0 and Target: i-12345

○ **C.** Destination: 172.28.0.0/12 and Target: vgw-12345

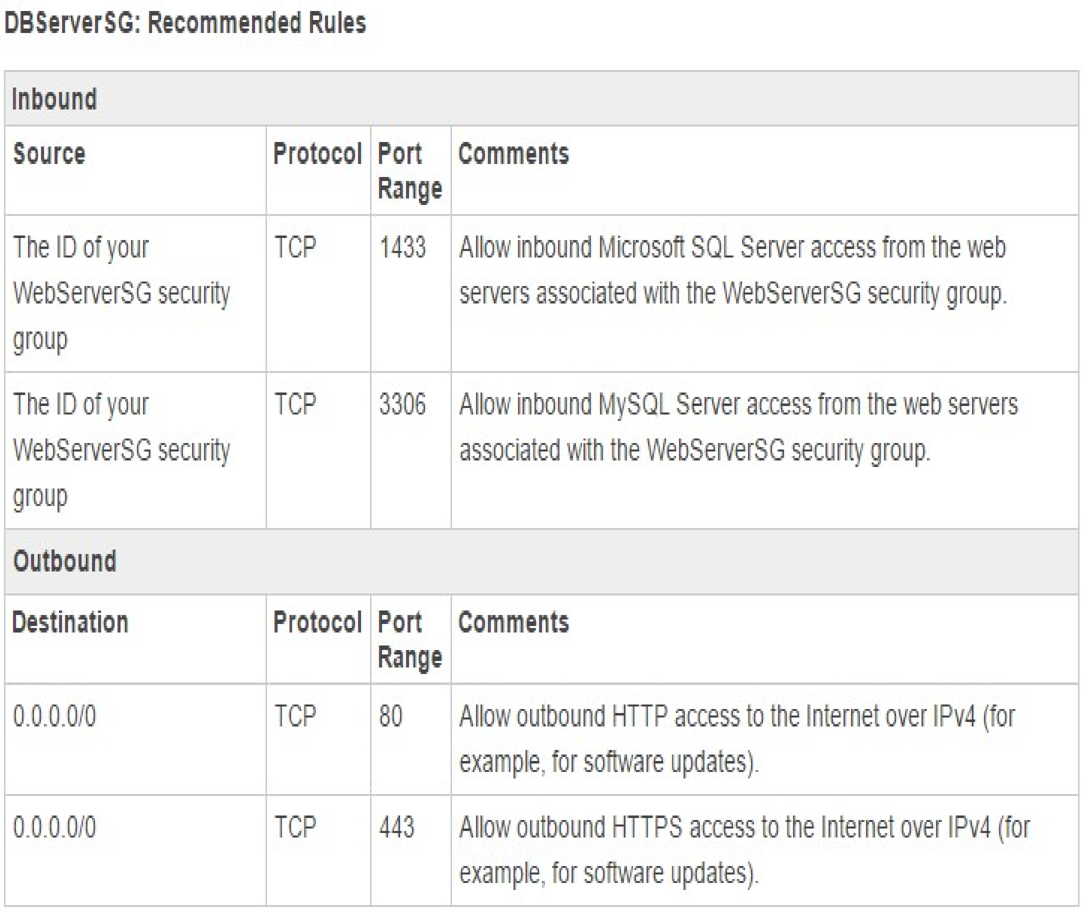
○ **D.** Destination: 20.0.0.0/16 and Target: local

Explanation :

Answer – A

- Option A is CORRECT because the destination of private subnet with NAT instance as target is not needed in the route table. This is an invalid entry.
- Option B is incorrect because you would need this entry to be able to communicate with the internet via NAT instance (e.g. for patch updates).
- Option C is incorrect because you need this entry for communicating with customer network via the virtual private gateway.
- Option D is incorrect because this entry is present by default to allow the resources in the VPC to communicate with each other.

The below diagram shows how a typical setup for a VPC with VPN and Internet gateway would look like. The only routing option which should have access to the internet gateway should be the 0.0.0.0/0 address. So Option A is the right answer.



DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).

For more information on VPC with the option of VPN, please visit the link

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html)

Ask our Experts

👍 👎

QUESTION 70 UNATTEMPTED SECURITY

A user has created a mobile application which makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below-mentioned statements is true with respect to the best practice for security in this scenario?

○ **A.** The user should create a separate IAM user for each mobile application and provide DynamoDB access with it.

○ **B.** The user should create an IAM role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2.

○ **C.** The application should use an IAM role with web identity federation which validates calls toDynamoDB with identity providers, such as Google, Amazon, and Facebook. ✔

○ **D.** Create an IAM Role with DynamoDB access and attach it with the mobile application.

Explanation :

Answer – C

Option A is incorrect because creating a separate user for each application user is not a feasible, secure, and recommended solution.
Option B is incorrect because the mobile users may not all be AWS users. You need to give access to the mobile application via federated identity provider.

Option C is CORRECT because it creates a role for Federated Users which enables the users to sign in to the app using their Amazon, Facebook, or Google identity and authorize them to seamlessly access DynamoDB.
Option D is incorrect because creating IAM Role is not sufficient. You need to authenticate the users of the application via web identity provider, then get the temporary credentials via a Security Token Service (STS) and then access DynamoDB.

More information on Web Identity Federation:
With Web Identity Federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC) (http://openid.net/connect/)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account.

For more information on Web Identity Federation, please visit the link
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

Ask our Experts

👍 👎

QUESTION 71 UNATTEMPTED NETWORK DESIGN

You work as a Solution Architect for a firm and your client has a multi-AZ infrastructure running on a VPC on AWS cloud. They are planning to implement a centralized custom dashboard on the client's data center. The dashboard will need to interact with the multi AZ infrastructure. Data from the multi AZ will be pulled from the data center. The solution should ensure less latency and good performance. Which of the following provides a best solution?

○ **A.** Use direct connect connection to the VPC as this will provide access to all AZs ✓

○ **B.** Use VPN connections to 2 VGW routers in the region as this should give you access to the infrastructure in all AZs

○ **C.** You cannot connect to multiple AZ's from a single location.

○ **D.** Use one direct connect connection from the data centre to each AZ in the region

Explanation :

Answer – A

Explanation

Direct connect connection will satisfy both the requirements of the scenario since it provides good bandwidth and low latency.

Option B is incorrect – Since VPN uses internet it does not ensure high bandwidth

Option C is incorrect – It is not true

Option D is incorrect – You don’t need a Direct connect connection to each AZ.

https://aws.amazon.com/directconnect/faqs/ (https://aws.amazon.com/directconnect/faqs/)

Ask our Experts

👍 👎

QUESTION 72 UNATTEMPTED DEPLOYMENT MANAGEMENT

A user has launched an EC2 instance store-backed instance in the us-east-1a zone. The user created AMI #1 and copied it to the eu-west-1 region. After that, the user made a few updates to the application running in the us-east-1a zone. The user makes an AMI #2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below-mentioned statements is true?

○ **A.** The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copying. Thus, the copied AMI will have all the updated data.

○ **B.** The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI.

○ **C.** It is not possible to copy the instance store backed AMI from one region to another.

○ **D.** The new instance in the eu-west-1 region will not have the changes made after the AMI copy. ✓

Explanation :

Answer – D

Option A is incorrect because (a) the changes made to the instance will not automatically get updated in the AMI in US-East-1, and (b) the already copied AMI will not have any reference to the AMI in the US-East-1 region.
Option B is incorrect because AWS does not automatically update the AMIs. It needs to be done manually.
Option C is incorrect because you can copy the instance store AMI between different regions.
Option D is CORRECT because the instance in the EU region will not have any changes made after copying the AMI. You will need to copy the AMI#2 to eu-west-1 and then launch the instance again to have all the changes.

For the entire details to copy AMI's, please visit the link –
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html)

Ask our Experts

👍 👎

QUESTION 73 UNATTEMPTED DEPLOYMENT MANAGEMENT

Company B has created an e-commerce site using DynamoDB and is designing a table named Products that includes items purchased and the users who purchased them. When creating a primary key on this table which of the following can be selected as the best attribute for a Partition key?

Select the best possible answer:

○ **A.** user_id where there are many users to few products ✓

○ **B.** product_id where there are few products to many users

○ **C.** category_id where there are few categories to many products

○ **D.** None of the above

Explanation :

Answer – A

When defining primary keys, you should always use the "many to few principle". Hence, option A is the best answer.

For more information on DynamoDB, please visit the link
https://aws.amazon.com/dynamodb/faqs/ (https://aws.amazon.com/dynamodb/faqs/)

Ask our Experts

👍 👎

QUESTION 74 UNATTEMPTED DEPLOYMENT MANAGEMENT

You are writing an AWS CloudFormation template and you want to assign values to properties that will not be available until runtime. You know that you can use intrinsic functions to do this but are unsure as to which part of the template they can be used in. Which of the following is correct in describing how you can currently use intrinsic functions in an AWS CloudFormation template?

Choose an option from the below:

○ **A.** You can use intrinsic functions in any part of a template.

○ **B.** You can only use intrinsic functions in specific parts of a template. You can use intrinsic functions in resource properties, metadata attributes, and update policy attributes. ✓

○ **C.** You can use intrinsic functions only in the resource properties part of a template.

○ **D.** You can use intrinsic functions in any part of a template, except AWSTemplateFormatVersion and Description.

Explanation :

Answer – B

As per AWS documentation:
You can use intrinsic functions only in specific parts of a template. Currently, you can use intrinsic functions in resource properties, outputs, metadata attributes, and update policy attributes. You can also use intrinsic functions to conditionally create stack resources.

Hence, B is the correct answer.

For more information on intrinsic function please refer to the below link
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference.html
(http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference.html)

Ask our Experts

👍 👎

QUESTION 75 UNATTEMPTED SECURITY

A corporate web application is deployed within an Amazon VPC and is connected to the corporate data center via IPSec VPN. The application must authenticate against the on-premise LDAP server. Once authenticated, logged-in users can only access an S3 keyspace specific to the user.

Choose 2 options from the below:

□ **A.** Develop an identity broker that authenticates against IAM Security Token Service (STS) to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.

□ **B.** The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service (STS) to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket. ✓

□ **C.** Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service (STS) to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket. ✓

□ **D.** The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket.

Explanation :

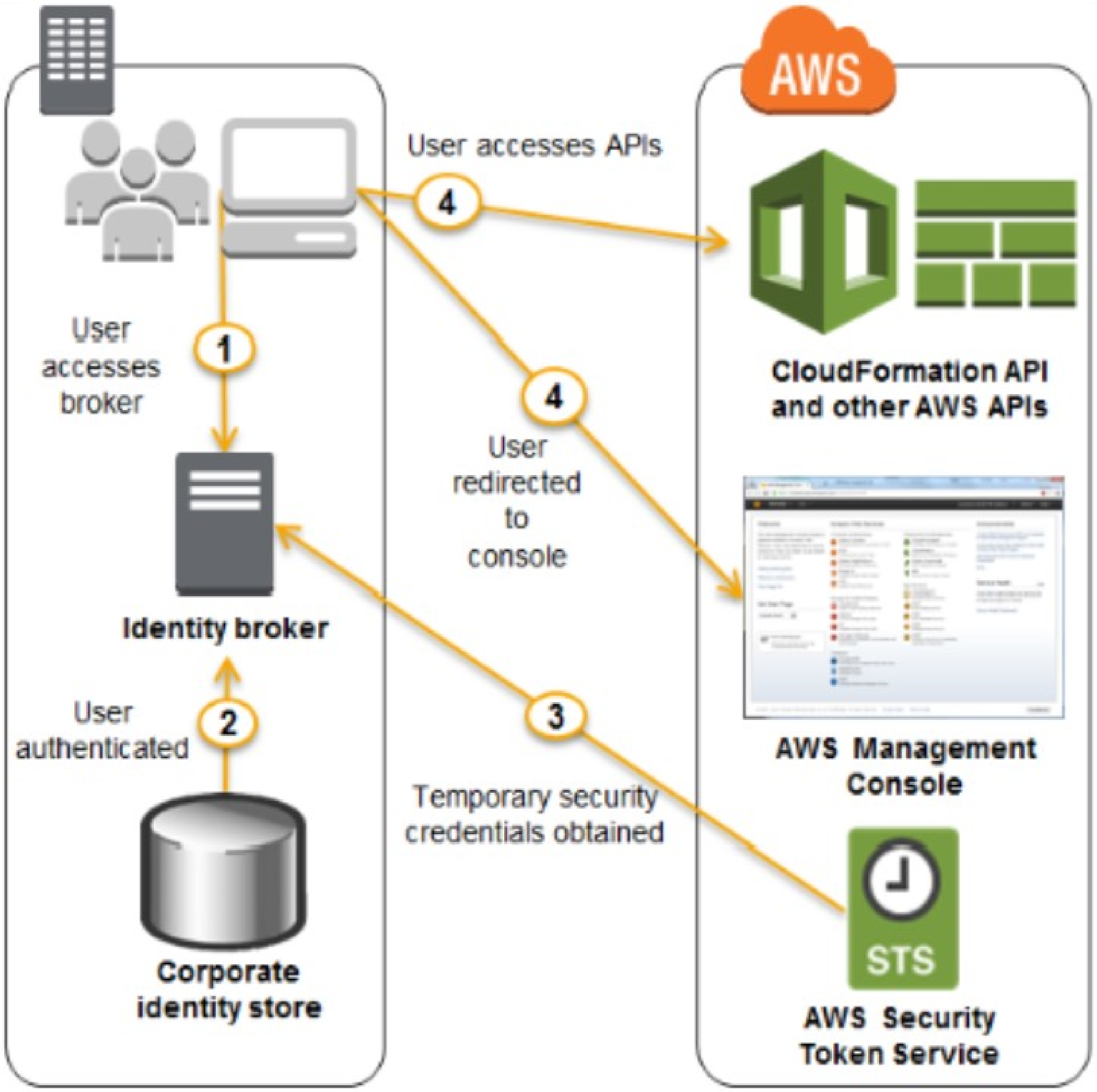
Answer – B and C

There are two architectural considerations here: (1) The users must be authenticated via the on-premise LDAP server, and (2) each user should have access to S3 only.

With this information, it is important to first authenticate the users using LDAP, get the IAM Role name, then get the temporary credentials from STS, and finally access the S3 bucket using those credentials. And second, create an IAM Role that provides access to S3.

Option A is incorrect because the users need to be authenticated using LDAP first, not STS. Also, the temporary credentials to log into AWS are provided by STS, not identity broker.
Option B is CORRECT because it follows the correct sequence. It authenticates users using LDAP, gets the security token from STS, and then accesses the S3 bucket using the temporary credentials.
Option C is CORRECT because it follows the correct sequence. It develops an identity broker that authenticates users against LDAP, gets the security token from STS, and then accesses the S3 bucket using the IAM federated user credentials.
Option D is incorrect because you cannot use the LDAP credentials to log into IAM.

An example diagram of how this works from the AWS documentation is given below.


AWS
User accesses APIs
4
CloudFormation API and other AWS APIs
User accesses broker
1
4
User redirected to console
Identity broker
AWS Management Console
User authenticated
2
3
Temporary security credentials obtained
STS
Corporate identity store
AWS Security Token Service

For more information on federated access, please visit the below link: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html)

Ask our Experts

QUESTION 76 UNATTEMPTED DEPLOYMENT MANAGEMENT

You have created an Elastic Load Balancer with Duration-Based sticky sessions enabled in front of your six EC2 web application instances in US-West-2. For High Availability, there are three web application instances in Availability Zone 1 and three web application instances in Availability Zone 2. To load test, you set up a software-based load tester in Availability Zone 2 to send traffic to the Elastic Load Balancer, as well as letting several hundred users browse to the ELB's hostname.

After a while, you notice that the users' sessions are spread evenly across the EC2 instances in both AZ's, but the software-based load tester's traffic is hitting only the instances in Availability Zone 2. What steps can you take to resolve this problem?

Choose 2 correct options from the below:

□ **A.** Create a software-based load tester in US-East-1 and test from there

□ **B.** Force the software-based load tester to re-resolve DNS before every request ✔

□ **C.** Use a third party load-testing service to send requests from globally distributed clients ✔

□ **D.** Switch to Application-Controlled sticky sessions

Explanation :

Answer – B and C

When you create an elastic load balancer, a default level of capacity is allocated and configured. As Elastic Load Balancing sees changes in the traffic profile, it will scale up or down. The time required for Elastic Load Balancing to scale can range from 1 to 7 minutes, depending on the changes in the traffic profile. When Elastic Load Balancing scales, it updates the DNS record with the new list of IP addresses. To ensure that clients are taking advantage of the increased capacity, Elastic Load Balancing uses a TTL setting on the DNS record of 60 seconds. It is critical that you factor this changing DNS record into your tests. If you do not ensure that DNS is re-resolved or use multiple test clients to simulate increased load, the test may continue to hit a single IP address when Elastic Load Balancing has actually allocated many more IP addresses. Because your end users will not all be resolving to that single IP address, your test will not be a realistic sampling of real-world behavior.

Option A is incorrect because creating load tester in US-East-1 will face the same problem of traffic hitting only the instances in that AZ.
Option B is CORRECT because if you do not ensure that DNS is re-resolved the test may continue to hit the single IP address.
Option C is CORRECT because if the requests come from globally distributed users, the DNS will not be resolved to a single IP address and the traffic would be distributed evenly across multiple instances.
Option D is incorrect because the traffic will be routed to the same back-end instances as the users continue to access your application. The load will not be evenly distributed across the AZs.

Please refer to the below article for more information:
http://aws.amazon.com/articles/1636185810492479
(http://aws.amazon.com/articles/1636185810492479)

Ask our Experts

👍 👎

QUESTION 77 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence. The database CPU is often above 80% usage and 90% of I/O operations on the database are reads. To improve the performance, you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results. In the next weeks the overall workload is expected to grow by 30%. Do you need to change anything in the architecture to maintain the high availability, or the application with the anticipated additional load and why?

○ **A.** Yes. You should deploy two Memcached ElastiCache Clusters in different AZs, because the RDS Instance will not be able to handle the load if the cache node fails. ✔

○ **B.** No. If the cache node fails, the automated ElastiCache node recovery feature will prevent any availability impact.

○ **C.** Yes. You should deploy the Memcached ElastiCache Cluster with two nodes in the same AZ as the RDS DB master instance to handle the load if one cache node fails.

○ **D.** No. If the cache node fails you can always get the same data from the DB without having any availability impact.

Explanation :

Answer - A

Option A is CORRECT because having two clusters in different AZs provide high availability of the cache nodes which removes the single point of failure. It will help caching the data; hence, reducing the overload on the database, maintaining the availability and reducing the impact.

Option B is incorrect because, even though AWS will automatically recover the failed node, there are no other nodes in the cluster once the failure happens. So, the data from the cluster would be lost once that single node fails. For higher availability, there should be multiple nodes. Also, once the cache node fails all the cached read load will go to the database which will not be able to handle the load with 30% increase to current levels. This means there will be availability impact.

Option C is incorrect because provisioning the nodes in the same AZ does not provide the tolerance for an AZ failure. For higher availability, the nodes should be spread across multiple AZs.

Option D is incorrect because the very purpose of the cache node was to reduce the impact on the database by not overloading it. If the cache node fails, the database will not be able to handle the 30% increase in the load; so, it will have an availability impact.

More information on this topic from AWS Documentation:

http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/BestPractices.html (http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/BestPractices.html)

Mitigating Node Failures

To mitigate the impact of a node failure, spread your cached data over more nodes. Because Memcached does not support replication, a node failure will always result in some data loss from your cluster.

When you create your Memcached cluster you can create it with 1 to 20 nodes, or more by special request. Partitioning your data across a greater number of nodes means you'll lose less data if a node fails. For example, if you partition your data across 10 nodes, any single node stores approximately 10% of your cached data. In this case, a node failure loses approximately 10% of your cache which needs to be replaced when a replacement node is created and provisioned.

Mitigating Availability Zone Failures

To mitigate the impact of an availability zone failure, locate your nodes in as many availability zones as possible. In the unlikely event of an AZ failure, you will lose only the data cached in that AZ, not the data cached in the other AZs.

Ask our Experts

👍 👎

QUESTION 78 UNATTEMPTED SCALABILITY & ELASTICITY

You are an architect for a new sharing mobile application. Anywhere in the world, your users can see local news on topics they chose. They can post pictures and videos from inside the application. Since the application is being used on a mobile phone, connection stability is required for uploading content and delivery should be quick.

Content is accessed a lot in the first minutes after it has been posted but is quickly replaced by new content before disappearing. The local nature of the news means that 90% of the uploaded content is then read locally.

What solution will optimize the user experience when users upload and view content (by minimizing page load times and minimizing upload times)?

○ **A.** Upload and store in S3, and use CloudFront.

○ **B.** Upload and store in S3 in the region closest to the user and then use multiple distributions of CloudFront.

○ **C.** Upload to EC2 in regions closer to the user, send content to S3, use CloudFront.

○ **D.** Use CloudFront for uploading the content to S3 bucket and for content delivery. ✓

Explanation :

Answer – D

Option A is incorrect because, even though it is a workable solution, a better approach is to use CloudFront for both uploading as well as distributing the content (not just distributing) - which is done in option D.
Option B and C are both incorrect because you do not need to upload the content to the source that is coser to the user. CloudFront will take care of that.
Option D is CORRECT because it uses CloudFront for both uploading as well as distributing the content (not just distributing) which is the most efficient use of the service.

For more information on Cloudfront please refer to the below URL
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GettingStarted.html
(http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GettingStarted.html)

Ask our Experts

👍 👎

QUESTION 79 UNATTEMPTED SCALABILITY & ELASTICITY

You are maintaining an application that is spread across multiple web servers and has incoming traffic balanced by ELB. The application allows users to upload pictures. Currently, each web server stores the image and a background task synchronizes the data between servers. However, the synchronization task can no longer keep up with the number of images uploaded

What change could you make so that all web servers have a place to store and read images at the same time?

Choose an option from the below:

○ **A.** Store the images in Amazon S3. ✓

○ **B.** Store the images on Amazon CloudFront.

○ **C.** Store the images on Amazon EBS.

○ **D.** Store the images on the ELB.

Explanation :

Answer – A

Option A is CORRECT because S3 provides a durable, secure, cost effective, and highly available storage service for the uploaded pictures.
Option B is incorrect because the application needs just a storage solution, not a global content distribution service. CloudFront is also costlier solution compared to S3.
Option C is incorrect because you cannot share EBS volumes among multiple EC2 instances.
Option D is incorrect because ELB cannot be used as a storage service.

For more information on AWS S3, please refer to the below url:
http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html)

Ask our Experts

QUESTION 80 UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

The company runs a complex customer system and consists of 10 different software components all backed up by RDS. You adopted Opswork to simplify management and deployment of that application and created a stack and layers for each component.

A security policy requires that all instances should run on the latest AMI and that instances must be replaced within one month after the latest AMI has been released. AMI replacements should be done without incurring application downtime or capacity problems. You decide to write a script to be run as soon as the new AMI is released.

Choose 2 options which meet your requirements:

□ **A.** Assign a custom recipe to each layer which replaces the underlying AMI. Use OpsWorks life-cycle events to incrementally execute this custom recipe and update the instances with the new AMI.

□ **B.** Specify the latest AMI as the custom AMI at the stack level terminates instances of the stack and let OpsWork launch new instances with the new AMI.

□ **C.** Identify all EC2 instances of your OpsWork stack, stop each instance, replace the AMI ID property with the latest AMI ID, and restart the instance. To avoid down time, make sure no more than one instance is stopped at the same time.

□ **D.** Create a new stack and layers with identical configuration, add instances with the latest AMI specified as a custom AMI to the new layers, switch DNS to the new stack, and tear down the old stack. ✓

□ **E.** Add new instances with the latest Amazon AMI as a custom AMI to all OpsWork layers of your stack and terminate the old ones. ✓

Explanation :

Answer - D and E

Option A is incorrect because to change the AMI you would have to re-launch new instances and you can't do that with chef recipes only.
Option B is incorrect because the AMI replacements should be done without incurring application downtime or capacity problems. So if you shutdown the stack, all applications will be stopped.
Option C is incorrect because the application could face the problem of insufficient capacity.
Option D is CORRECT because it represents a common practice of Blue-Green Deployment which is carried out for reducing the downtime and risk by running two identical production environments called Blue and Green. Please see "More information.." section for additional details.
Option E is CORRECT because you can only add new instances at the layer level by specifying to

use Custom AMI at the stack level.

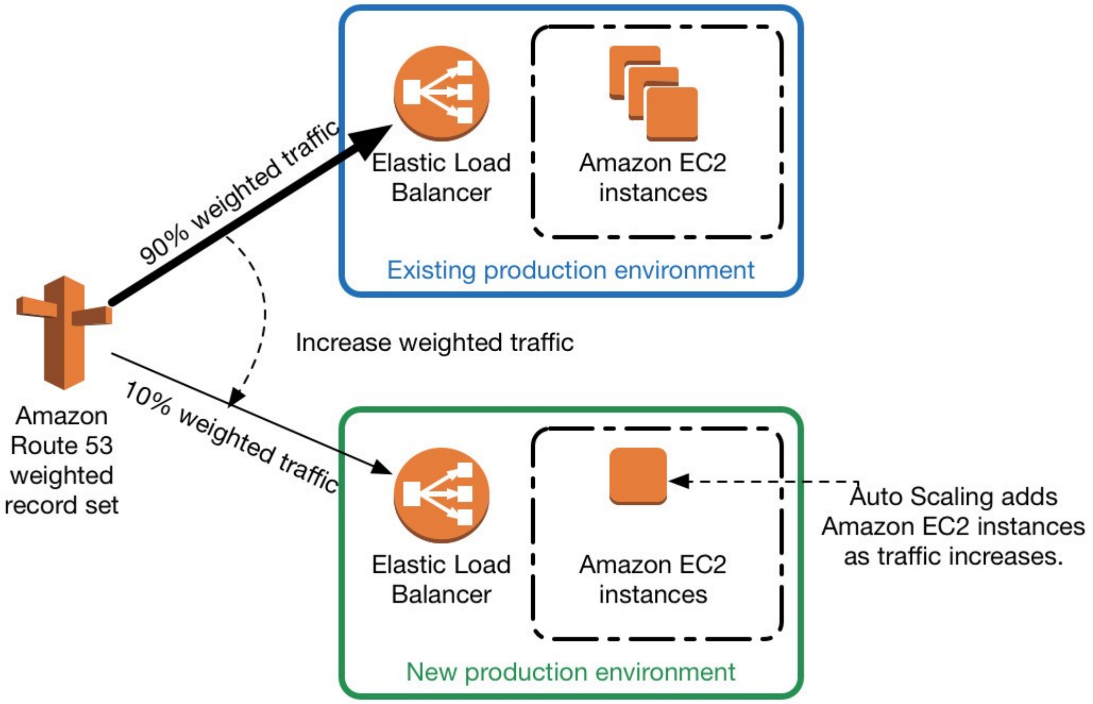
More information on Blue-Green Deployment:

Blue-green deployment is a technique that reduces downtime and risk by running two identical production environments called Blue and Green.

At any time, only one of the environments is live, with the live environment serving all production traffic. For this example, Blue is currently live and Green is idle.

As you prepare a new version of your software, deployment and the final stage of testing takes place in the environment that is not live: in this example, Green. Once you have deployed and fully tested the software in Green, you switch the router so all incoming requests now go to Green instead of Blue. Green is now live, and Blue is idle.

This technique can eliminate downtime due to application deployment. In addition, blue-green deployment reduces risk: if something unexpected happens with your new version on Green, you can immediately roll back to the last version by switching back to Blue.


90% weighted traffic
Elastic Load Balancer
Amazon EC2 instances
Existing production environment
Increase weighted traffic
Amazon Route 53 weighted record set
10% weighted traffic
Elastic Load Balancer
Amazon EC2 instances
Auto Scaling adds Amazon EC2 instances as traffic increases.
New production environment

Please refer to the below URL for more details

https://d0.awsstatic.com/whitepapers/AWS_Blue_Green_Deployments.pdf (https://d0.awsstatic.com/whitepapers/AWS_Blue_Green_Deployments.pdf)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13606)

Certification

- Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)
- Java Certification (https://www.whizlabs.com/oracle-java-certifications/)
- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Company

- Support (https://help.whizlabs.com/hc/en-us)
- Discussions (http://ask.whizlabs.com/)
- Blog (https://www.whizlabs.com/blog/)

Mobile App

Android Coming Soon

iOS Coming Soon

Follow us

f

(https://www.facebook.com/whizlabs.software/)

in

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

G+

(https://plus.google.com/+WhizlabsSoftware)