AWS Certified Advanced Networking - Specialty ANS-C01: AWS Certified Advanced Networking - Specialty ANS-C01

[202610]

Question #1 Topic 1

A company is planning to create a service that requires encryption in transit. The traffic must not be decrypted between the client and the backend of the service. The company will implement the service by using the gRPC protocol over TCP port 443. The service will scale up to thousands of simultaneous connections. The backend of the service will be hosted on an Amazon Elastic Kubernetes Service (Amazon EKS) duster with the Kubernetes Cluster Autoscaler and the Horizontal Pod Autoscaler configured. The company needs to use mutual TLS for two-way authentication between the client and the backend.
Which solution will meet these requirements?

A. Install the AWS Load Balancer Controller for Kubernetes. Using that controller, configure a Network Load Balancer with a TCP listener on port 443 to forward traffic to the IP addresses of the backend service Pods. **Most Voted**

B. Install the AWS Load Balancer Controller for Kubernetes. Using that controller, configure an Application Load Balancer with an HTTPS listener on port 443 to forward traffic to the IP addresses of the backend service Pods.

C. Create a target group. Add the EKS managed node group's Auto Scaling group as a target Create an Application Load Balancer with an HTTPS listener on port 443 to forward traffic to the target group.

D. Create a target group. Add the EKS managed node group’s Auto Scaling group as a target. Create a Network Load Balancer with a TLS listener on port 443 to forward traffic to the target group.

Correct Answer: A

Community vote distribution



Comments

emmanuelodenyire **Highly Voted** 2 years, 11 months ago

Selected Answer: A

Option B is incorrect because an Application Load Balancer (ALB) does not support TLS passthrough and decrypts the traffic before forwarding it to the backend servers. Option C is incorrect because an Application Load Balancer (ALB) does not support mutual TLS authentication (mTLS), which is required for this use case. Option D is incorrect because a TLS listener is not suitable for this use case. TLS passthrough is required, and the correct listener type for NLB is TCP.

Fengyu **Highly Voted** 2 years, 8 months ago

Selected Answer: A

ALB does not support mutual TLS and will decrypt the traffic
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

Primmy 1 week, 2 days ago

Selected Answer: A

Guess it

8ifherckhs 3 weeks, 2 days ago

Selected Answer: A

a is correct answer

8ifherckhs 3 weeks, 2 days ago

Selected Answer: A

a is correct answer

begmustkim4313 2 months ago

Selected Answer: A

option a is correct answer

2aldous 4 months, 2 weeks ago

Selected Answer: A

- The main requirement is for the encryption and mutual TLS (mTLS) to be handled end-to-end between the client and the backend pod, without being decrypted anywhere in between. - gRPC uses HTTP/2 over TCP, and mTLS must terminate in the backend, not at the load balancer. - Network Load Balancer (NLB) with TCP passthrough on port 443 forwards packets transparently at layer 4, so the load balancer does NOT terminate TLS. This means the backend pods handle all TLS handshakes and mTLS authentication. - Application Load Balancer (ALB) and NLB with a TLS listener both terminate TLS at the load balancer, breaking end-to-end encryption as required in the question. Using the AWS Load Balancer Controller is the correct way to manage load balancers for Kubernetes services on EKS.

jhondenielcarag 6 months ago

Selected Answer: A

A is correct because a Network Load Balancer with a TCP listener forwards encrypted traffic without terminating TLS, allowing the client and backend Pods to perform end-to-end mutual TLS directly.

Malcnorth59 8 months ago

Selected Answer: B

Alb supports mutual tls validation and tls passthrough.
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/configuring-mtls-with-elb.html

2aldous 4 months, 2 weeks ago

Ok, ALB support mTLS, but if you create HTTPS listener on port 443 the load balancer will terminate the TLS at the load balancer, breaking the end to end encrypted as required in the question. B is wrong, A is correct.

chris46 1 year, 4 months ago

Selected Answer: C

The questions talks about the need for auto scaling, setting the LB's Target group to a specific IP will remove the ability to auto scale. gRPC via HTTPS is supported and ALB's support mTLS
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/deploy-a-grpc-based-application-on-an-amazon-eks-cluster-and-access-it-with-an-application-load-balancer.html

minhpn28 1 year, 6 months ago

Selected Answer: B

ption B is incorrect because an Application Load Balancer (ALB) does not support TLS passthrough and decrypts the traffic before for

minhpn28 1 year, 6 months ago

Selected Answer: A

Option B is incorrect because an Application Load Balancer (ALB) does not support TLS passthrough and decrypts the traffic before forwarding it to the backend servers.

Ravan 1 year, 6 months ago

Selected Answer: A

Option B (ALB with HTTPS): ALB operates at Layer 7 and terminates TLS connections, which would decrypt traffic at the load balancer, violating the requirement that traffic must remain encrypted between the client and backend.

Jonalb 1 year, 7 months ago

Selected Answer: A

100% A correct "

KienCT 1 year, 8 months ago

Selected Answer: A

I TINK A

ExamFrontier 1 year, 8 months ago

FYI. There are many new questions in the exam taken in June.

ksdpmx 1 year, 9 months ago

Selected Answer: B

gRPC is not supported by NLB natively til now (2024/6)

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #2 Topic 1

A company is deploying a new application in the AWS Cloud. The company wants a highly available web server that will sit behind an Elastic Load Balancer. The load balancer will route requests to multiple target groups based on the URL in the request. All traffic must use HTTPS. TLS processing must be offloaded to the load balancer. The web server must know the user's IP address so that the company can keep accurate logs for security purposes.
Which solution will meet these requirements?

A. Deploy an Application Load Balancer with an HTTPS listener. Use path-based routing rules to forward the traffic to the correct target group. Include the X-Forwarded-For request header with traffic to the targets. **Most Voted**

B. Deploy an Application Load Balancer with an HTTPS listener for each domain. Use host-based routing rules to forward the traffic to the correct target group for each domain. Include the X-Forwarded-For request header with traffic to the targets.

C. Deploy a Network Load Balancer with a TLS listener. Use path-based routing rules to forward the traffic to the correct target group. Configure client IP address preservation for traffic to the targets.

D. Deploy a Network Load Balancer with a TLS listener for each domain. Use host-based routing rules to forward the traffic to the correct target group for each domain. Configure client IP address preservation for traffic to the targets.

Correct Answer: A

Community vote distribution



Comments

zaazanuna **Highly Voted** 3 years ago

A - correct. Here's why: An Application Load Balancer (ALB) can be used to route traffic to multiple target groups based on the URL in the request. The ALB can be configured with an HTTPS listener to ensure all traffic uses HTTPS. TLS processing can be offloaded to the ALB, which reduces the load on the web server. Path-based routing rules can be used to route traffic to the correct target group based on the URL in the request. The X-Forwarded-For request header can be included with traffic to the targets, which will allow the web server to know the user's IP address and keep accurate logs for security purposes.

Fengyu **Highly Voted** 2 years, 8 months ago

Selected Answer: A

A should be correct. For B, host routing is based on domain name, it's also could route based on URL. But we don't need listener for each domain.

begmustkim4313 2 months ago

Selected Answer: A

option a is correct

chris46 1 year, 4 months ago

Selected Answer: C

The questions talks about auto scaling, setting the LB's Target group to a specific IP will remove the ability to scale. gRPC via HTTPS is supported and ALB's support mTLS https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/deploy-a-grpc-based-application-on-an-amazon-eks-cluster-and-access-it-with-an-application-load-balancer.html

chris46 1 year, 4 months ago

Posted in the Wrong Question, this is for answer 1.

Raphaello 1 year, 11 months ago

Selected Answer: A

A is the correct answer. ALB with HTTPS listener, and X-Forwarded-For is added by default.

Marfee400704 2 years, 1 month ago

I think that It's correct answer is A according to the SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is A.

merajk 2 years, 4 months ago

Selected Answer: A

ALB: TLS termination, path based listener configuration and X-Forwarded-For request header

task_7 2 years, 5 months ago

Selected Answer: A

https://aws.amazon.com/blogs/networking-and-content-delivery/accessing-private-application-load-balancers-and-instances-through-aws-global-accelerator/

Andrea13 2 years, 5 months ago

The correct answer is A. Deploy an Application Load Balancer with an HTTPS listener. Use path-based routing rules to forward the traffic to the correct target group. Include the X-Forwarded-For request header with traffic to the targets.

MEDES 2 years, 6 months ago

1 week ago A - correct. Here's why: An Application Load Balancer (ALB) can be used to route traffic to multiple target groups based on the URL in the request. The ALB can be configured with an HTTPS listener to ensure all traffic uses HTTPS. TLS processing can be offloaded to the ALB, which reduces the load on the web server. Path-based routing rules can be used to route traffic to the correct target group based on the URL in the request. The X-Forwarded-For request header can be included with traffic to the targets, which will allow the web server to know the user's IP address and keep accurate logs for security purposes.

Mishranihal737 2 years, 7 months ago

A & C both can be correct but the company wants highly available design so C should be correct as it provides zonal isolation. ALB does not support Zonal Isolation for HA.

ishaikh 2 years, 11 months ago

ALB & Path based routing is the correct answer

ranac 2 years, 11 months ago

Selected Answer: A

An Application Load Balancer (ALB) can be used to meet the requirement of routing requests to multiple target groups based on the URL in the request. Path-based routing rules can be used to forward traffic to the correct target group. The ALB also supports HTTPS listener and offloads TLS processing, which meets the requirement of using HTTPS for all traffic. The X-Forwarded-For request header can be included with traffic to the targets to preserve the user's IP address for logging purposes.

Untamables 2 years, 11 months ago

Selected Answer: A

A https://repost.aws/knowledge-center/elb-achieve-path-based-routing-alb
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/x-forwarded-headers.html

fallkore 2 years, 11 months ago

“ The load balancer will route requests to multiple target groups based on the URL in the request” Answer should be A.

ILOVEVODKA 3 years ago

Selected Answer: B

A is wrong answer, because path is like: /api in URL. Nowhere in question is mentioned about routing to specific path. So B i right answer.

ILOVEVODKA 2 years, 11 months ago

my bad - A is the right answer.

https://zhangxuetu.online

[202610]

Question #3 Topic 1

A company has developed an application on AWS that will track inventory levels of vending machines and initiate the restocking process automatically. The company plans to integrate this application with vending machines and deploy the vending machines in several markets around the world. The application resides in a VPC in the us-east-1 Region. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster behind an Application Load Balancer (ALB). The communication from the vending machines to the application happens over HTTPS.
The company is planning to use an AWS Global Accelerator accelerator and configure static IP addresses of the accelerator in the vending machines for application endpoint access. The application must be accessible only through the accelerator and not through a direct connection over the internet to the ALB endpoint.
Which solution will meet these requirements?

A. Configure the ALB in a private subnet of the VPC. Attach an internet gateway without adding routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the internet on the ALB listener port. **Most Voted**

B. Configure the ALB in a private subnet of the VPC. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the internet on the ALB listener port.

C. Configure the ALB in a public subnet of the VPAttach an internet gateway. Add routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.

D. Configure the ALB in a private subnet of the VPC. Attach an internet gateway. Add routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.

Correct Answer: A

Community vote distribution



Comments

study_aws1 **Highly Voted** 3 years ago

This is not a normal scenario of attaching IGW to EC2 instance by creating a route in subnet. Please read the below link typically describing ELB integration with AWS Global accelator (and the last line of the extract) - https://docs.aws.amazon.com/global-accelerator/latest/dg/secure-vpc-connections.html "When you add an internal Application Load Balancer or an Amazon EC2 instance endpoint in AWS Global Accelerator, you enable internet traffic to flow directly to and from the endpoint in Virtual Private Clouds (VPCs) by targeting it in a private subnet. The VPC that contains the load balancer or EC2 instance must have an internet gateway attached to it, to indicate that the VPC accepts internet traffic. However, you don't need public IP addresses on the load balancer or EC2 instance. You also don't need an associated internet gateway route for the subnet."

Joselito79 2 months, 2 weeks ago

Selected Answer: C

ALB on public subnet + IGW + routes SG only allows traffic from Global Accelerator IPs ✔ ALB internet-facing (GA technical requirement) ✔ The only allowed source is Global Accelerator ✔ Even though the ALB has a public DNS: It is not directly accessible because SG blocks it ✔ It meets the requirement: “The application must be accessible only through the accelerator”

Kraftzman 5 months, 4 weeks ago

Selected Answer: C

Let's double-check why an internal ALB might be problematic. It's not. It's the better solution. So why isn't it an option? The options are poorly written. But we must choose the best one. Option C describes a complete, working system. Option A/B describes a better architecture but with flawed/incomplete rules. In a multiple-choice context, you choose the most complete and correct description. C is a self-contained, working, if not ideal, solution.

LeoSantos121212121212121 6 months, 2 weeks ago

Selected Answer: C

It's C. ALB is public, but you restrict access with a security group so that only GA’s static IP addresses can reach it. That way, vending machines must go through GA, and direct ALB access is blocked.

sarutc 6 months, 3 weeks ago

Selected Answer: C

Options Analysis A) ALB in private subnet + IGW but no route -> X Doesn't make sense. Private subnets + IGW with no routes -> unreachable B) ALB in private subnet + accelerator --> SG allows Internet traffic -> X Wrong. That would allow direct Internet access , breaking the requirement C) ALB in public subnet + IGW + routes + SG allows traffic only from GA IPs --> / Correct. Public ALB (so GA can reach it), but inbound restricted to GA --> vending machines can only come via GA static IPs D) ALB in private subnet + IGW + routes + SG allows GA IPs -> X ALB must be in public subnets (not private) to receive traffic directly from GA. Private subnet ALBs can't serve GA endpoints.

73f8ac3 1 year, 5 months ago

Selected Answer: D

Private subnet: Placing the ALB in a private subnet ensures that it is not directly accessible from the internet, enhancing security. Internet gateway: The internet gateway allows outbound traffic from the private subnet to reach the internet, which is necessary for the ALB to communicate with the AWS Global Accelerator. Route tables: The routes in the subnet route tables point to the internet gateway, ensuring that traffic from the ALB can reach the internet. Endpoint groups: The endpoint groups in the AWS Global Accelerator associate the ALB endpoint with the accelerator, allowing the vending machines to connect to the ALB through the accelerator's static IP address. Security group: The ALB's security group restricts inbound traffic to only the IP addresses of the AWS Global Accelerator, preventing direct internet access to the ALB.

vikasj1in 1 year, 6 months ago

Selected Answer: A

Placing the ALB in a private subnet ensures that it is not directly accessible from the internet. Adding an internet gateway without adding routes in the subnet route tables prevents direct internet traffic to the ALB. Configuring the AWS Global Accelerator with endpoint groups that include the ALB endpoint allows controlled access to the application through the accelerator. Configuring the ALB's security group to only allow inbound traffic from the internet on the ALB listener port further restricts direct access, ensuring that the application is accessed only through the AWS Global Accelerator.

Ravan 1 year, 6 months ago

Selected Answer: D

ALB in a private subnet: Ensures that the ALB cannot be accessed directly from the internet, protecting it from unauthorized access. Internet gateway: Allows the ALB to communicate with the internet, even though it's in a private subnet. Routes pointing to the internet gateway: Enables the ALB to send responses back to the internet through the Global Accelerator. Global Accelerator: Provides a globally distributed load balancer that can be accessed through static IP addresses, making it ideal for applications that need to be accessible from multiple locations worldwide. Endpoint groups: Associate the ALB with the Global Accelerator, allowing traffic to be routed to it. Security group: Restricts inbound traffic to the ALB, ensuring only traffic from the Global Accelerator can reach the application.

seochan 1 year, 10 months ago

D is wrong. When using internal ALB, you must use Preserve Client IP on the Global Accelerator. In that case, the security group in your ALB should allow all internet traffic (because you should allow the IP addresses of your clients), not Global Accelerator's IP. Plus, the target VPC of the Global Accelerator must attach an Internet gateway.

Raphaello 1 year, 11 months ago

Selected Answer: D

Correct answer is D. The request is to allow flow ONLY through the accelerator and not through a direct connection over the internet to the ALB endpoint. So clearly option A (Configure the ALB’s security group to only allow inbound traffic from the internet on the ALB listener port) is not the answer. D is correct.

xTrayusx 1 year, 11 months ago

Selected Answer: D

Placing the ALB in a private subnet ensures that it is not directly accessible from the internet.The ALB's security group should be configured to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port. This ensures that only traffic originating from the accelerator is allowed to access the ALB.

merajk 2 years, 4 months ago

Selected Answer: A

Well described here: https://docs.aws.amazon.com/global-accelerator/latest/dg/secure-vpc-connections.html

ChinkSantana 2 years, 2 months ago

Well explained here: When you add an internal Application Load Balancer or an Amazon EC2 instance endpoint in AWS Global Accelerator, you enable internet traffic to flow directly to and from the endpoint in Virtual Private Clouds (VPCs) by targeting it in a private subnet. The VPC that contains the load balancer or EC2 instance must have an internet gateway attached to it, to indicate that the VPC accepts internet traffic. However, you don't need public IP addresses on the load balancer or EC2 instance. You also don't need an associated internet gateway route for the subnet.

Andrea13 2 years, 5 months ago

The correct answer is C. Configure the ALB in a public subnet of the VPC. Attach an internet gateway. Add routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include

the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.

scofield101 2 years, 7 months ago

Option C is the correct option. Every other option suggested created ALB in a private subnet without internet gateway. The ALB won't be accessible from the internet including the accelerator which isn't a VPC component. You create an ALB in a private subnet if you want the ALB to be accessed internally (within the vpc) and the accelerator is a global and not a vpc based component.

PhilMultiCloud 2 years, 8 months ago

The requirement here is that the application must be accessible only through the Global Accelerator, and not via a direct connection over the internet to the ALB endpoint. Hence, the ALB should be placed in a private subnet and should be configured such that only traffic coming from the Global Accelerator can reach the ALB. Option A: This won't work because we're allowing inbound traffic from the internet on the ALB listener port. We need to restrict the traffic to the ALB only from the Global Accelerator's IP addresses. Option B: This won't work for the same reason as option A - we're allowing traffic from the entire internet to reach the ALB. Option C: This won't work because placing the ALB in a public subnet will allow it to be accessible from the internet, which we don't want. Option D: This is the correct option. Here, we're placing the ALB in a private subnet, which prevents direct access from the internet. The traffic is allowed only from the IP addresses of the Global Accelerator. Thus, access to the ALB is only possible through the Global Accelerator, fulfilling the requirement.

emmanuelodenyire 2 years, 11 months ago

Selected Answer: D

Configure the ALB in a private subnet of the VPC. Attach an internet gateway. Add routes in the subnet route tables to point to the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.

ranac 2 years, 11 months ago

Selected Answer: D

The ALB can be configured in a private subnet of the VPC to ensure that the application is not directly accessible from the internet. An internet gateway needs to be attached to the VPC and routes added in the subnet route tables to point to the internet gateway to enable connectivity with the AWS Global Accelerator.

https://zhangxuetu.online

[202610]

Question #4 Topic 1

A global delivery company is modernizing its fleet management system. The company has several business units. Each business unit designs and maintains applications that are hosted in its own AWS account in separate application VPCs in the same AWS Region. Each business unit's applications are designed to get data from a central shared services VPC.
The company wants the network connectivity architecture to provide granular security controls. The architecture also must be able to scale as more business units consume data from the central shared services VPC in the future.
Which solution will meet these requirements in the MOST secure manner?

A. Create a central transit gateway. Create a VPC attachment to each application VPC. Provide full mesh connectivity between all the VPCs by using the transit gateway.

B. Create VPC peering connections between the central shared services VPC and each application VPC in each business unit's AWS account.

C. Create VPC endpoint services powered by AWS PrivateLink in the central shared services VPCreate VPC endpoints in each application VPC. **Most Voted**

D. Create a central transit VPC with a VPN appliance from AWS Marketplace. Create a VPN attachment from each VPC to the transit VPC. Provide full mesh connectivity among all the VPCs.

Correct Answer: C

Community vote distribution



Comments

tel_veer 3 months, 1 week ago

Selected Answer: C

In this specific context, C - PrivateLink meets all the requirements. Apps can "get" from shared services VPC, and apps in different business accounts can not talk to each other

deepakno 8 months, 3 weeks ago

Selected Answer: A

TG good for hub and spoke model(central VPC to VPC connections). VPC endpoint services not right for inter-vpc communication

deepakno 8 months, 3 weeks ago

C only. Mesh connectivity not required and inside a region VPC endpoint should be right

beanxyz 1 year, 11 months ago

Selected Answer: C

vpc endpoints provides granualr control in service level, while tgw in network level

Raphaello 1 year, 11 months ago

Selected Answer: C

Correct answer is C. Key words: granular security controls. Option A allows "full mesh", and therefore does not fulfill the requirement.

tromyunpak 2 years ago

The most secure option is C as privatelink is one way. A is too permissive due to transit gateway full mesh configuration. B is good but traffic is 2 way whilst D doesn't make sense

vikasj1in 2 years, 1 month ago

Selected Answer: C

AWS PrivateLink: This solution enables you to access services over a private connection between your VPC and the service, keeping traffic within the AWS network. VPC Endpoint Services: By creating an endpoint service in the central shared services VPC, you can expose specific services privately to other VPCs using AWS PrivateLink. Each application VPC can then create VPC endpoints to connect to the shared services privately.

decieredavidolo 2 years, 5 months ago

Greetings to all, i bring you good news today. Those of you who are into IT and wanna venture into cybersecurity and having difficulties to study and how to go through are hereby advice to get directories from the global certification support center. They orientate you on how to get and pass certifications with lots of ease making you competent and master in the field. Reach them using the site globalcertcenter.org Good luck

Andrea13 2 years, 5 months ago

The best solution for this scenario is option C: Create VPC endpoint services powered by AWS PrivateLink in the central shared services VPC. Create VPC endpoints in each application VPC.

MEDES 2 years, 6 months ago

A is correct. Option C is not the most secure solution because it does not provide granular security controls. AWS PrivateLink is a service that enables you to access services hosted on AWS in a highly available and scalable manner. It provides a convenient way to connect to applications/services by name with added security.

Fukat 2 years, 8 months ago

Option C https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-share-your-services.html Option A is also correct but it mentions “Provide full mesh connectivity between all the VPCs” which is not required as per the cx need

emmanuelodenyire 2 years, 11 months ago

Selected Answer: C

Option C suggests creating VPC endpoint services powered by AWS PrivateLink in the central shared services VPC and creating VPC endpoints in each application VPC. This solution is a secure way to provide connectivity between the central shared services VPC and each business unit's VPC. It provides granular security controls as the VPC endpoints are private and can only be accessed by the VPC that created them. It also addresses the requirement for scalability as adding new VPCs only requires creating new VPC endpoints. Therefore, this option is a possible correct answer.

ranac 2 years, 11 months ago

Selected Answer: C

VPC endpoint services powered by AWS PrivateLink will provide the highest level of security by keeping all network traffic within the AWS network. It allows for granular security controls by allowing only authorized traffic from the application VPC to the central shared services VPC, reducing the attack surface area.

gpt_test 2 years, 11 months ago

Selected Answer: B

By reviewing the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress, the network engineer can identify which VIF is causing the sudden increase in throughput. Upgrading the bandwidth of the existing dedicated connection to 10 Gbps will help mitigate the issue of slowness due to saturation, ensuring that resources hosted on AWS can be accessed more efficiently.

gpt_test 2 years, 11 months ago

Incorrect answers with explanations: A. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift traffic from the existing dedicated connection to the new dedicated connection. Explanation: Creating a new dedicated connection and shifting traffic to it will introduce additional complexity and cost. It's more efficient to upgrade the bandwidth of the existing connection, as described in option B.

Untamables 2 years, 11 months ago

Selected Answer: C

C https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/aws-privatelink.html Option B also works but has a limitation for scaling due to the quota of VPC peering. Option A and D are wrong. the full mesh connectivity is not needed because each VPCs only need to connect to the central shared VPC.

study_aws1 3 years ago

Should be option C). There is no requirement for Transitive routing here for East-West traffic flow between VPCs or North-South traffic inspection here, hence, Transit Gateway would not be required here. PrivateLink does the job and is scalable solution also, provides access to only the Shared Services without exposing other services in VPC.

SIX 3 years ago

A-Correct it is important to note that using AWS PrivateLink alone may not provide the same level of granular control over network traffic as using AWS Transit Gateway, VPC peering, and security groups.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #5 Topic 1

A company uses a 4 Gbps AWS Direct Connect dedicated connection with a link aggregation group (LAG) bundle to connect to five VPCs that are deployed in the us-east-1 Region. Each VPC serves a different business unit and uses its own private VIF for connectivity to the on-premises environment. Users are reporting slowness when they access resources that are hosted on AWS.
A network engineer finds that there are sudden increases in throughput and that the Direct Connect connection becomes saturated at the same time for about an hour each business day. The company wants to know which business unit is causing the sudden increase in throughput. The network engineer must find out this information and implement a solution to resolve the problem.
Which solution will meet these requirements?

A. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift traffic from the existing dedicated connection to the new dedicated connection. **Most Voted**

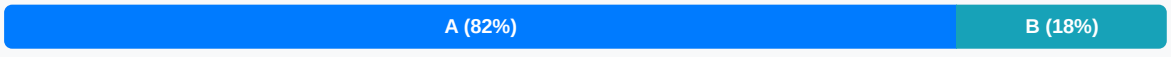
B. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Upgrade the bandwidth of the existing dedicated connection to 10 Gbps.

C. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Upgrade the existing dedicated connection to a 5 Gbps hosted connection.

D. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending the highest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift traffic from the existing dedicated connection to the new dedicated connection.

Correct Answer: A

Community vote distribution



Comments

that1guy **Highly Voted** 2 years, 12 months ago

Selected Answer: A

A, From: https://docs.aws.amazon.com/directconnect/latest/UserGuide/dedicated_connection.html > "You cannot change the port speed after you create the connection request. To change the port speed, you must create and

configure a new connection."

tel_veer 3 months, 1 week ago

Selected Answer: A

Existing DX can not be changed (or increased, because it already reached limit of 4 links in the LAG). After observing CW VIF traffic metrics, nothing much to do except upgrade to 10G and migrate to it (A)

Untamables 1 year, 6 months ago

Selected Answer: A

A The company has configured the Direct Connect connection stacked with LAG like the below AWS document in this scenario. It seems that there are 4 1-GB dedicated connections. https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html Hence, you must monitor the entire traffic, not each dedicated connection traffic. Option C and D are wrong for this reason. https://docs.aws.amazon.com/directconnect/latest/UserGuide/monitoring-cloudwatch.html Option B is wrong. To change the port speed, you must create and configure a new connection. https://docs.aws.amazon.com/directconnect/latest/UserGuide/dedicated_connection.html

clphan 1 year, 7 months ago

Option A, - From https://docs.aws.amazon.com/directconnect/latest/UserGuide/dedicated_connection.html, you can't upgrade the current port speed. hosted connection support 1, 10, 100, 400. Current LAG 4GBPS mean that 4 connection / LAG => If need 10 seem need create a new because LAG require same port speed.

Raphaello 1 year, 11 months ago

Selected Answer: A

A is the correct answer. Need to create a new DX connection with the new speed.

MEDES 2 years, 6 months ago

A, From: https://docs.aws.amazon.com/directconnect/latest/UserGuide/dedicated_connection.html > "You cannot change the port speed after you create the connection request. To change the port speed, you must create and configure a new connection."

emmanuelodenyire 2 years, 11 months ago

Selected Answer: B

Option B suggests upgrading the bandwidth of the existing dedicated connection to 10 Gbps after reviewing the CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period of slowness. This solution would help identify which VIF is causing the problem and increase the bandwidth to alleviate the issue.

ranac 2 years, 11 months ago

Selected Answer: B

since the company is already using a 4 Gbps Direct Connect dedicated connection with a LAG bundle, upgrading the bandwidth of the existing dedicated connection to 10 Gbps will be a more cost-effective solution than creating a new 10 Gbps dedicated connection.

slackbot 2 years, 11 months ago

Selected Answer: A

Obviously - DX connections cannot be upgraded. They can migrate the VIFs to the new DX conn

gpt_test 2 years, 11 months ago

Selected Answer: B

By reviewing the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress, the network engineer can identify which VIF is causing the sudden increase in throughput. Upgrading the bandwidth of the existing dedicated connection to 10 Gbps will help mitigate the issue of slowness due to saturation, ensuring that resources hosted on AWS can be accessed more efficiently.

SIX 3 years ago

A-Correct Answer In AWS Direct Connect, you cannot upgrade an existing 4 x 1Gbps connection to a 10Gbps connection. Instead, you will need to create a new 10Gbps connection and move the traffic to the new connection. https://repost.aws/questions/QUxprf4oUTRHyvs-SylrzNRw/can-aws-direct-connect-ports-be-upgraded-from-1-gbps-to-10-gbps.

ITgeek 3 years ago

Selected Answer: B

AWS Direct Connect offers different port speeds, including 1 Gbps, 10 Gbps, and 100 Gbps. If you are currently using a 4 Gbps connection, it means you are likely using a 10 Gbps connection, but it is provisioned at 4 Gbps.

Cappy46789 3 years ago

There is LAG involved so likely 4 x 1Gbps connections

study_aws1 3 years ago

A is correct. However, the apprpriate parameter will be VirtualInterfacePpsEgress and VirtualInterfacePpsIngress, as it is related to packet rate i.e. throughput

deepakno 9 months, 3 weeks ago

Packet rate(pps) is how many packets (regardless of size) are sent and bit rate (bps) is how much data (by volume) is flowing out from a specific virtual interface. So, correct parameters i believe.

https://zhangxuetu.online

[202610]

Question #6 Topic 1

A software-as-a-service (SaaS) provider hosts its solution on Amazon EC2 instances within a VPC in the AWS Cloud. All of the provider's customers also have their environments in the AWS Cloud.
A recent design meeting revealed that the customers have IP address overlap with the provider's AWS deployment. The customers have stated that they will not share their internal IP addresses and that they do not want to connect to the provider's SaaS service over the internet.
Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy the SaaS service endpoint behind a Network Load Balancer. **Most Voted**

B. Configure an endpoint service, and grant the customers permission to create a connection to the endpoint service. **Most Voted**

C. Deploy the SaaS service endpoint behind an Application Load Balancer.

D. Configure a VPC peering connection to the customer VPCs. Route traffic through NAT gateways.

E. Deploy an AWS Transit Gateway, and connect the SaaS VPC to it. Share the transit gateway with the customers. Configure routing on the transit gateway.

Correct Answer: AB

Community vote distribution

AB (100%)

Comments

emmanuelodenyire **Highly Voted** 2 years, 4 months ago

Selected Answer: AB

The correct answer is A and B. Option A, deploying the SaaS service endpoint behind a Network Load Balancer (NLB), allows the provider to present a single IP address to customers, while maintaining a highly available and scalable architecture. This is achieved by mapping the NLB's IP address to the SaaS service endpoint. Option B, configuring an endpoint service, enables customers to connect to the SaaS service endpoint using their own private IP addresses. This allows customers to avoid IP address overlap with the provider's AWS deployment and provides a secure, private connection to the SaaS service without traversing the internet.

bogehad181 **Highly Voted** 2 years, 5 months ago

Selected Answer: AB

A&B: https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-access-saas.html

begmustkim4313 2 months ago

Selected Answer: AB

a and b is right answer

tel_veer 3 months, 1 week ago

Selected Answer: AB

Because the ask is to choose Two, I picked A and B. Exposing a service through a PrivateLink is sufficient otherwise because NLB is a pre-req for exposing service through PrivateLink

siheom 9 months ago

Selected Answer: AB

vote AB

Raphaello 1 year, 5 months ago

Selected Answer: AB

AB are the correct answers. Ideal use case for VPC service endpoint (PrivateLink)

tromyunpak 1 year, 6 months ago

A and B that is the configuration to setup a private link

patanjali 1 year, 6 months ago

Answer are A and B D cant be the answer as per https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-basics.html#vpc-peering-limitations, You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 or IPv6 CIDR blocks.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is AB according to SPOTO products.

Marfee400704 1 year, 7 months ago

I think that It's correct answer is AB according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is A & B.

Hisayuki 1 year, 8 months ago

Selected Answer: AB

With a PrivateLink, you can expose your own services to another VPC. But you can not choose the ALB as an endpoint for PrivateLink. Instead, Use the NLB for the PrivateLink.

FayeG 1 year, 11 months ago

Selected Answer: AB

The correct answer is A and B

MEDES 1 year, 12 months ago

The correct answer is A and B. Option A, deploying the SaaS service endpoint behind a Network Load Balancer (NLB), allows the provider to present a single IP address to customers, while maintaining a highly available and scalable architecture. This is achieved by mapping the NLB's IP address to the SaaS service endpoint. Option B, configuring an endpoint service, enables customers to connect to the SaaS service endpoint using their own private IP addresses. This allows customers to avoid IP address overlap with the provider's AWS deployment and provides a secure, private connection to the SaaS service without traversing the internet.

dvaidya 2 years ago

Selected Answer: AB

this is standard use case of privatelink

PhilMultiCloud 2 years, 1 month ago

The correct choices are: A. Deploy the SaaS service endpoint behind a Network Load Balancer. B. Configure an endpoint service, and grant the customers permission to create a connection to the endpoint service. The problem here is that there is an IP address overlap between the SaaS provider's deployment and the customers' environments. Given this, we need a solution that allows private connectivity without the need for specific IP addresses. Deploying the SaaS service behind a Network Load Balancer (NLB) will allow the service to scale and handle traffic in a reliable way. Also, NLB supports IP targets, which would allow the SaaS service to connect directly to the EC2 instances. AWS PrivateLink, which includes endpoint services, provides private connectivity between VPCs, AWS services, and on-premises applications, without exposing the traffic to the public internet. This is precisely the functionality we need in this scenario. When we create an endpoint service, the customers can create a connection to the service, which allows them to connect to the SaaS application privately.

4bed5ff 2 years, 2 months ago

I chose C instead of A, because "Elastic Load Balancing now supports forwarding traffic directly from Network Load Balancer (NLB) to Application Load Balancer (ALB). With this feature, you can now use AWS PrivateLink and expose static IP addresses for applications built on ALB." https://aws.amazon.com/about-aws/whats-new/2021/09/application-load-balancer-aws-privatelink-static-ip-addresses-network-load-balancer/

https://zhangxuetu.online

[202610]

Question #7 Topic 1

A network engineer is designing the architecture for a healthcare company's workload that is moving to the AWS Cloud. All data to and from the on-premises environment must be encrypted in transit. All traffic also must be inspected in the cloud before the traffic is allowed to leave the cloud and travel to the on-premises environment or to the internet.
The company will expose components of the workload to the internet so that patients can reserve appointments. The architecture must secure these components and protect them against DDoS attacks. The architecture also must provide protection against financial liability for services that scale out during a DDoS event.
Which combination of steps should the network engineer take to meet all these requirements for the workload? (Choose three.)

A. Use Traffic Mirroring to copy all traffic to a fleet of traffic capture appliances.

B. Set up AWS WAF on all network components.

C. Configure an AWS Lambda function to create Deny rules in security groups to block malicious IP addresses.

D. Use AWS Direct Connect with MACsec support for connectivity to the cloud. **Most Voted**

E. Use Gateway Load Balancers to insert third-party firewalls for inline traffic inspection. **Most Voted**

F. Configure AWS Shield Advanced and ensure that it is configured on all public assets. **Most Voted**

Correct Answer: DEF

Community vote distribution



Comments

study_aws1 **Highly Voted** 3 years ago

D) - All data to and from the on-premises environment must be encrypted in transit. (Use AWS Direct Connect with MACsec support for connectivity to the cloud.) E) - All traffic also must be inspected in the cloud before the traffic is allowed to leave the cloud and travel to the on-premises environment (Use Gateway Load Balancers to insert third-party firewalls for inline traffic inspection.) F) - The architecture also must provide protection against financial liability for services that scale out during a DDoS event.(Configure AWS Shield Advanced and ensure that it is configured on all public assets) F) -

zendevloper 2 years, 4 months ago

Correct B E F shield advanced requires WAF (to protect against DDoS)
https://docs.aws.amazon.com/waf/latest/developerguide/waf-api-using.html

zendevloper 2 years, 4 months ago

Here is a more relevant link https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-adv-web-app.html

seochan 1 year, 10 months ago

F is a definite answer. The architecture also must provide protection against financial liability for services that scale out during a DDoS event. With Shield Advanced, AWS provides AWS credits to cover the costs incurred by DDoS attacks (e.g., costs caused by auto scaling groups). https://docs.aws.amazon.com/waf/latest/developerguide/ddos-request-service-credit.html

Untamables Highly Voted 2 years, 11 months ago

Selected Answer: DEF

D https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html E https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/introduction.html F https://docs.aws.amazon.com/waf/latest/developerguide/ddos-advanced-summary.html

begmustkim4313 2 months ago

Selected Answer: DEF

d e and f is correct answer

zyademad 9 months, 4 weeks ago

Selected Answer: D

D) - All data to and from the on-premises environment must be encrypted in transit. (Use AWS Direct Connect with MACsec support for connectivity to the cloud.) E) - All traffic also must be inspected in the cloud before the traffic is allowed to leave the cloud and travel to the on-premises environment (Use Gateway Load Balancers to insert third-party firewalls for inline traffic inspection.) F) - The architecture also must provide protection against financial liability for services that scale out during a DDoS event.(Configure AWS Shield Advanced and ensure that it is configured on all public assets) F) -

Akivox 1 year, 6 months ago

Selected Answer: DEF

D: All traffic must be encrypted in transit, need to use Direct connect with MACSec E: For inspection of traffic before it is allowed to leave the cloud and travel to the on-prem, need to use GWLB with third party firewall for insepction. F: For DDOS event, AWS Shield Advanced must be used.

Raphaello 1 year, 11 months ago

Selected Answer: DEF

DEF are the correct answers. D >> DX connection with MASSec to provide required encryption. E >> GWLB to provide inspection of the flow F >> Shield Advanced to provide DDoS protection and cover for scale out expenses if happened.

tromyunpak 2 years ago

F is needed to protect from DDOS attacks E is needed to inspect the traffic before leaving the cloud D is needed to encrypt the direct connect connection

patanjali 2 years ago

Correct answer is DEF B is not correct because you can associate WAF rules with ALB only and not all network component of VPC

JoellaLi 1 year, 11 months ago

yes. WAF can protect Amazon CloudFront, Amazon API Gateway, Application Load Balancer, and AWS AppSync resources.

vikasj1in 2 years, 1 month ago

Selected Answer: BEF

The other options are not directly related to the specified security requirements: A. Use Traffic Mirroring to copy all traffic to a fleet of traffic capture appliances: Traffic Mirroring is useful for capturing and analyzing network traffic but may not be directly related to inline inspection or DDoS protection. C. Configure an AWS Lambda function to create Deny rules in security groups to block malicious IP addresses: While Lambda functions can automate certain tasks, using them to create Deny rules in security groups might not provide the same level of comprehensive protection as dedicated security services like AWS WAF and AWS Shield Advanced. D. Use AWS Direct Connect with MACsec support for connectivity to the cloud: AWS Direct Connect with MACsec provides secure connectivity but does not directly address the requirements for traffic inspection or DDoS protection in this context.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is DEF according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is B & D & F.

yanhiro 2 years, 3 months ago

I can confirm that DEF is the correct answer. AWS WAF doesn't answer the requirement of having financial protection against cost induced by DDoS attacks. Also Shield Advanced doesn't require AWS WAF and can be activated on itself.

MEDES 2 years, 6 months ago

D) - All data to and from the on-premises environment must be encrypted in transit. (Use AWS Direct Connect with MACsec support for connectivity to the cloud.) E) - All traffic also must be inspected in the cloud before the traffic is allowed to leave the cloud and travel to the on-premises environment (Use Gateway Load Balancers to insert third-party firewalls for inline traffic inspection.) F) - The architecture also must provide protection against financial liability for services that scale out during a DDoS event.(Configure AWS Shield Advanced and ensure that it is configured on all public assets) F) -

Simili 2 years, 6 months ago

D) AWS Direct Connect with MACsec support for connectivity to the cloud. >> all the data to and from the on-premises environment must be encrypted in transit. E) Gateway Load Balancers to insert third-party firewalls for inline traffic inspection. >> all the traffic also must be inspected in the cloud before the traffic is allowed to leave the cloud and travel to the on-premises environment F) Configure AWS Shield Advanced and ensure that it is configured on all public assets. >> The architecture also must provide protection against financial liability for services that scale out during a DDoS event

Mishranihal737 2 years, 7 months ago

Yes DEF is correct.

PhilMultiCloud 2 years, 8 months ago

D. Use AWS Direct Connect with MACsec support for connectivity to the cloud. MACsec (Media Access Control Security) provides encryption in transit over the network for the Direct Connect link between the on-premises environment and AWS, ensuring that all data is encrypted as required. E. Use Gateway Load Balancers to insert third-party firewalls for inline traffic inspection. AWS Gateway Load Balancer makes it easy to deploy, scale, and manage third-party virtual network appliances. Using Gateway Load Balancer, you can easily insert, scale, and manage firewalls in the path of internet traffic for inspection purposes. F. Configure AWS Shield Advanced and ensure that it is configured on all public assets. AWS Shield Advanced provides advanced DDoS (Distributed Denial of Service)

protection. It not only defends your application against DDoS attacks but also provides cost protection, which can protect your business from additional charges incurred during a DDoS attack. Therefore, the answers are D, E, and F.

RVD 2 years, 10 months ago

Selected Answer: DEF

ANS: DEF DX now support MACSec for encryption, GWLb with Third-party for Network Inspection, Advance shield for Ddos as WAF can not protect.

https://zhangxuetu.online

[202610]

Question #8 Topic 1

A retail company is running its service on AWS. The company's architecture includes Application Load Balancers (ALBs) in public subnets. The ALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can call externally hosted services over the internet by using a NAT gateway.
The company has noticed in its billing that NAT gateway usage has increased significantly. A network engineer needs to find out the source of this increased usage.
Which options can the network engineer use to investigate the traffic through the NAT gateway? (Choose two.)

A. Enable VPC flow logs on the NAT gateway's elastic network interface. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query and analyze the logs. Most Voted

B. Enable NAT gateway access logs. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query and analyze the logs.

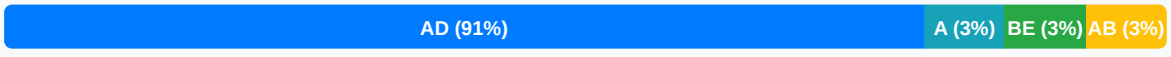
C. Configure Traffic Mirroring on the NAT gateway's elastic network interface. Send the traffic to an additional EC2 instance. Use tools such as tcpdump and Wireshark to query and analyze the mirrored traffic.

D. Enable VPC flow logs on the NAT gateway's elastic network interface. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs. Most Voted

E. Enable NAT gateway access logs. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs.

Correct Answer: AD

Community vote distribution



Comments

devilman222 Highly Voted 3 years ago

Selected Answer: AD

A. Yes, this would work. B. Not a real thing, wrong C. We don't need to do packet inspection to analyze costs. This won't help with costs at all. D. The most obvious right answer. E. Like B, not a real thing.

begmustkim4313 2 months ago

Selected Answer: AD

a and d is correct answer

zyademad 9 months, 4 weeks ago

Selected Answer: A

A. Yes, this would work. B. Not a real thing, wrong C. We don't need to do packet inspection to analyze costs. This won't help with costs at all. D. The most obvious right answer. E. Like B, not a real thing.

RavikantKumarRavi 1 year, 2 months ago

Selected Answer: BE

NAT gateways do not have their own elastic network interfaces (ENIs) . In such A & D is not correct hence it should be

andctygr 9 months ago

NAT Gateways have their own elastic network interfaces. https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-basics.html

AlirezaNetWorld 1 year, 6 months ago

A and C are the best answers based on the requirements

rltk8029 1 year, 11 months ago

C -- also working answer. In Wireshark you can generate reports for traffic usage.

Raphaello 1 year, 11 months ago

Selected Answer: AD

AD seem to be the correct answers. Enabling "NAT gateway access logs" is not a valid feature.

Marfee400704 2 years ago

I think that it's answer is AD according to SPOTO products.

halukd 2 years, 2 months ago

https://repost.aws/knowledge-center/vpc-find-traffic-sources-nat-gateway Check this re:Post, it seems like A-E

cumzle_com 2 years, 3 months ago

A and D - you can only enable VPC flow logs on ENIs rather than on the services in that case NAT Gateway

FayeG 2 years, 4 months ago

Selected Answer: AD

A & D are the real answer

MEDES 2 years, 6 months ago

Went with A,D given that we want to track which IPs are source of the problem. given that NAT gateway access logs only provide information about connections that are initiated by the NAT gateway. VPC flow logs provide more detailed information about the traffic that passes through the NAT gateway.

prajkash 2 years, 8 months ago

Selected Answer: AD

emmanuelodenyire 2 years, 10 months ago

Selected Answer: AB

Overall, Options A and B are the most relevant and efficient approaches to investigate the traffic through the NAT gateway and identify the source of increased NAT gateway usage. Although also C and D are correct, but we do not want deeper analysis of the logs. Again remember, both VPC flow logs and NAT gateway access logs can provide network information about the traffic going through the NAT gateway.

Manh 2 years, 10 months ago

AWS NAT gateway access logs are not available as a native feature of AWS NAT gateway. you can use VPC Flow Logs to capture information about the IP traffic going to and from network interfaces in your VPC

slackbot 2 years, 11 months ago

Selected Answer: AD

packet captures will require inspection per TCP connection, which is not reasonable, so - A&D

ITgeek 3 years ago

Selected Answer: AD

These are correct

zaazanuna 3 years ago

my guess was not entirely correct. i am leaning towards to A, B and D, Option D is also a valid approach to investigate the traffic through the NAT gateway. By enabling VPC flow logs on the NAT gateway's elastic network interface and publishing the logs to an S3 bucket, a network engineer can create a custom table for the S3 bucket in Amazon Athena to describe the log structure and use Athena to query and analyze the logs. This approach provides a lot of flexibility in terms of data analysis and long-term storage of the log data. So, technically, options A, B, and D are all valid ways to investigate NAT gateway usage. However, options A and B are probably more efficient because they allow you to query and analyze the logs directly in CloudWatch Logs without having to set up additional infrastructure. so either - AB or AD

titi_r 2 years, 12 months ago

Such thing - a "NAT gateway access logs" - seems to not exist at all. Read the last sentence in the question like "Which are the VALID options a network Engineer can..." So, A and D.

https://zhangxuetu.online

[202610]

Question #9 Topic 1

A banking company is successfully operating its public mobile banking stack on AWS. The mobile banking stack is deployed in a VPC that includes private subnets and public subnets. The company is using IPv4 networking and has not deployed or supported IPv6 in the environment. The company has decided to adopt a third-party service provider's API and must integrate the API with the existing environment. The service provider's API requires the use of IPv6.
A network engineer must turn on IPv6 connectivity for the existing workload that is deployed in a private subnet. The company does not want to permit IPv6 traffic from the public internet and mandates that the company's servers must initiate all IPv6 connectivity. The network engineer turns on IPv6 in the VPC and in the private subnets.
Which solution will meet these requirements?

A. Create an internet gateway and a NAT gateway in the VPC. Add a route to the existing subnet route tables to point IPv6 traffic to the NAT gateway.

B. Create an internet gateway and a NAT instance in the VPC. Add a route to the existing subnet route tables to point IPv6 traffic to the NAT instance.

C. Create an egress-only Internet gateway in the VPAdd a route to the existing subnet route tables to point IPv6 traffic to the egress-only internet gateway. **Most Voted**

D. Create an egress-only internet gateway in the VPC. Configure a security group that denies all inbound traffic. Associate the security group with the egress-only internet gateway.

Correct Answer: C

Community vote distribution



Comments

study_aws1 Highly Voted 3 years ago
Answer is C

NoAwsSupport Highly Voted 2 years, 9 months ago
A. NAT Gateway does not support IPv6 B. NAT Instance will be on Public subnet where IPv6 is not enabled. c. Works d. You don't to explicitly deny inbound access to EO GW. It is its default functionality.

vinay777 2 years, 7 months ago
Incorrect, NAT gateway support ipv6 traffic https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

WMF0187 2 years, 6 months ago

NAT64 enables your IPv6-only services in Amazon VPCs to communicate with IPv4-only services within the same VPC (in different subnets) or connected VPCs, in your on-premises networks, or over the internet. NAT64 helps your IPv6 AWS resources communicate with IPv4 resources in the same VPC or a different VPC, in your on-premises network or over the internet.

begmustkim4313 2 months ago

Selected Answer: C

NAT gateways and NAT instances do not support IPv6. EIGW is the correct AWS service for IPv6 outbound-only access.

zyademad 9 months, 4 weeks ago

Selected Answer: C

A. NAT Gateway does not support IPv6 B. NAT Instance will be on Public subnet where IPv6 is not enabled. c. Works d. You don't to explicitly deny inbound access to EO GW. It is its default functionality.

AlirezaNetWorld 1 year, 6 months ago

C is the right answer 100%

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. Egress-only internet gw.

patanjali 2 years ago

Answer is C As per https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html - An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the internet, and prevents the internet from initiating an IPv6 connection with your instances. - An egress-only internet gateway is for use with IPv6 traffic only. To enable outbound-only internet communication over IPv4, use a NAT gateway instead.

vikasj1in 2 years, 1 month ago

Selected Answer: C

To meet the requirements of allowing the company's servers to initiate all IPv6 connectivity and not permitting IPv6 traffic from the public internet, you can use an egress-only Internet gateway. The egress-only Internet gateway is used for outbound communication initiated by the instances in the private subnet over IPv6. It allows the instances in the private subnet to communicate with the IPv6-enabled service provider's API while preventing incoming IPv6 traffic from the public internet.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

FayeG 2 years, 4 months ago

Selected Answer: C

C is the correct answer

MEDES 2 years, 6 months ago

NAT64 enables your IPv6-only services in Amazon VPCs to communicate with IPv4-only services within the same VPC (in different subnets) or connected VPCs, in your on-premises networks, or over the internet. NAT64 helps your IPv6 AWS resources communicate with IPv4 resources in the same VPC or a different VPC, in your on-premises network or over the internet.

cmthiru 2 years, 8 months ago

Answer C

demoras 2 years, 9 months ago

Selected Answer: C

Answer is C

notwhoyouthink 2 years, 10 months ago

New here, but discouraged since it seems like the answers are mostly wrong or misleading.

emmanuelodenyire 2 years, 10 months ago

Selected Answer: C

Option C is the correct answer because it suggests creating an egress-only Internet gateway in the VPC and adding a route to the existing subnet route tables to point IPv6 traffic to the egress-only internet gateway. This meets the requirement of not allowing IPv6 traffic from the public internet and mandates that the company's servers must initiate all IPv6 connectivity. The egress-only Internet gateway allows outbound communication over IPv6, but blocks inbound traffic.

bogehad181 2 years, 11 months ago

Selected Answer: C

C: https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

Untamables 2 years, 11 months ago

Selected Answer: C

No doubt C. The egress-only internet gateway is a typical solution for IPv6.

https://zhangxuetu.online

[202610]

Question #10 Topic 1

A company has deployed an AWS Network Firewall firewall into a VPC. A network engineer needs to implement a solution to deliver Network Firewall flow logs to the company's Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster in the shortest possible time.
Which solution will meet these requirements?

A. Create an Amazon S3 bucket. Create an AWS Lambda function to load logs into the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Enable Amazon Simple Notification Service (Amazon SNS) notifications on the S3 bucket to invoke the Lambda function. Configure flow logs for the firewall. Set the S3 bucket as the destination.

B. Create an Amazon Kinesis Data Firehose delivery stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination. Configure flow logs for the firewall Set the Kinesis Data Firehose delivery stream as the destination for the Network Firewall flow logs. **Most Voted**

C. Configure flow logs for the firewall. Set the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination for the Network Firewall flow logs.

D. Create an Amazon Kinesis data stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination. Configure flow logs for the firewall. Set the Kinesis data stream as the destination for the Network Firewall flow logs.

Correct Answer: B

Community vote distribution

B (100%)

Comments

flowers00 Highly Voted 2 years, 6 months ago

B - correct. https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-analyze-aws-network-firewall-logs-using-amazon-opensearch-service-part-1/

begmustkim4313 2 months ago

Selected Answer: B

b is correct answer Create an Amazon Kinesis Data Firehose delivery stream with Amazon OpenSearch Service as the destination. Configure Network Firewall flow logs to send logs to the Firehose delivery stream.

zyademad 9 months, 4 weeks ago

Selected Answer: B

B - correct. https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-analyze-aws-network-firewall-logs-using-amazon-opensearch-service-part-1/

Raphaello 1 year, 5 months ago

Selected Answer: B

B is the correct answer. Forward NF logs to KDF and from there to opensearch.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is B according to SPOTO products.

MEDES 1 year, 12 months ago

B Because request is shortest possible time. Firehose is one of the shortest destination and has better integration with OpenSearch. The timing of Network Firewall log delivery varies by location type, averaging 3-6 minutes for Amazon CloudWatch Logs and Amazon Kinesis Data Firehose and 8-12 minutes for Amazon Simple Storage Service buckets. https://docs.aws.amazon.com/network-firewall/latest/developerguide/firewall-logging.html

DPDK 2 years, 2 months ago

B Because request is shortest possible time. Firehose is one of the shortest destination and has better integration with OpenSearch. The timing of Network Firewall log delivery varies by location type, averaging 3-6 minutes for Amazon CloudWatch Logs and Amazon Kinesis Data Firehose and 8-12 minutes for Amazon Simple Storage Service buckets. https://docs.aws.amazon.com/network-firewall/latest/developerguide/firewall-logging.html

emmanuelodenyire 2 years, 4 months ago

Selected Answer: B

Option B is the correct answer. Explanation: The question asks for a solution to deliver Network Firewall flow logs to the company's Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster in the shortest possible time. Option B suggests creating an Amazon Kinesis Data Firehose delivery stream that includes the Amazon OpenSearch Service cluster as the destination. This solution is the most efficient because Kinesis Data Firehose can stream data in near real-time to the Amazon OpenSearch Service cluster. This means that logs will be delivered to the Elasticsearch cluster in the shortest possible time.

Untamables 2 years, 5 months ago

Selected Answer: B

B Network Firewall supports Amazon Kinesis Data Firehose as one of the logging destinations. The timing of Network Firewall log delivery varies by location type, averaging 3-6 minutes for Amazon CloudWatch Logs and Amazon Kinesis Data Firehose and 8-12 minutes for Amazon Simple Storage Service buckets. https://docs.aws.amazon.com/network-firewall/latest/developerguide/firewall-logging.html

Cappy46789 2 years, 6 months ago

B - Firehose

zaazanuna 2 years, 6 months ago

B - correct

https://zhangxuetu.online

[202610]

Question #11 Topic 1

A company is using custom DNS servers that run BIND for name resolution in its VPCs. The VPCs are deployed across multiple AWS accounts that are part of the same organization in AWS Organizations. All the VPCs are connected to a transit gateway. The BIND servers are running in a central VPC and are configured to forward all queries for an on-premises DNS domain to DNS servers that are hosted in an on-premises data center. To ensure that all the VPCs use the custom DNS servers, a network engineer has configured a VPC DHCP options set in all the VPCs that specifies the custom DNS servers to be used as domain name servers.
Multiple development teams in the company want to use Amazon Elastic File System (Amazon EFS). A development team has created a new EFS file system but cannot mount the file system to one of its Amazon EC2 instances. The network engineer discovers that the EC2 instance cannot resolve the IP address for the EFS mount point fs-33444567d.efs.us-east-1.amazonaws.com. The network engineer needs to implement a solution so that development teams throughout the organization can mount EFS file systems.
Which combination of steps will meet these requirements? (Choose two.)

A. Configure the BIND DNS servers in the central VPC to forward queries for efs.us-east-1.amazonaws.com to the Amazon provided DNS server (169.254.169.253).

B. Create an Amazon Route 53 Resolver outbound endpoint in the central VPC. Update all the VPC DHCP options sets to use AmazonProvidedDNS for name resolution. **Most Voted**

C. Create an Amazon Route 53 Resolver inbound endpoint in the central VPUpdate all the VPC DHCP options sets to use the Route 53 Resolver inbound endpoint in the central VPC for name resolution.

D. Create an Amazon Route 53 Resolver rule to forward queries for the on-premises domain to the on-premises DNS servers. Share the rule with the organization by using AWS Resource Access Manager (AWS RAM). Associate the rule with all the VPCs. **Most Voted**

E. Create an Amazon Route 53 private hosted zone for the efs.us-east-1.amazonaws.com domain. Associate the private hosted zone with the VPC where the EC2 instance is deployed. Create an A record for fs-33444567d.efs.us-east-1.amazonaws.com in the private hosted zone. Configure the A record to return the mount target of the EFS mount point.

Correct Answer: BD

Community vote distribution



Comments

study_aws1 **Highly Voted** 2 years, 12 months ago

Please refer the below extract taken from the link - https://aws.amazon.com/blogs/security/simplify-dns-management-in-a-multiaccount-environment-with-route-53-resolver/ "You can mount an Amazon EFS file system on an Amazon EC2 instance using DNS names. The file system DNS name automatically resolves to the mount target's IP address in the Availability Zone of the connecting Amazon EC2 instance. To be able to do that, the VPC must use the default DNS provided by Amazon to resolve EFS DNS names. If you plan to use EFS in your environment, I recommend that you resolve EFS DNS names locally and avoid sending these queries to central DNS because clients in that case would not receive answers optimized for their availability zone, which might result in higher operation latencies and less durability." So, option B) answers EFS resolution from VPC. Combination of Option B) and D) explains resolution from on-prem

steli0 6 months ago

The only issue with option B is that is indicating an update to existing DHCP options which is not possible https://docs.aws.amazon.com/directoryservice/latest/admin-guide/dhcp_options_set.html Moreover doesn't mention the shutdown of BIND servers to avoid redundant costs.

Untamables Highly Voted 2 years, 11 months ago

Selected Answer: BD

I vote B and D. What the company want to to is as following. https://docs.aws.amazon.com/whitepapers/latest/hybrid-cloud-dns-options-for-vpc/route-53-resolver-endpoints-and-forwarding-rules.html The combination of A and E also seems to work. But the maintenance overhead for the custom DNS server remains. That is not a good practice.

begmustkim4313 2 months ago

Selected Answer: BD

b and d is correct answer

Joselito79 2 months, 2 weeks ago

Selected Answer: AD

 Option A — CORRECT A. Configure the BIND DNS servers in the central VPC to forward queries for efs.us-east-1.amazonaws.com to the Amazon-provided DNS server (169.254.169.253). This is the recommended pattern when using custom DNS + AWS services. Option D — CORRECT It's the modern and scalable approach compared to bind-only forwarding.

2aldous 4 months, 2 weeks ago

Selected Answer: AD

ambiguous question. The questions should be more clear, for example: "The company wants to eliminate the BIND servers and use AWS-managed services" in that case the answer should be B and D, or if the question says "Resolve the issue with the minimal effort", probably the answer should be only A, or A and D if we planning to remove BIND servers in the future.

steli0 6 months ago

Selected Answer: AD

I vote AD because option B indicates an update to existing DHCP options which is not possible according to the bellow; you can change the associated option-set but not update the existing one. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/dhcp_options_set.html Even if we assume that by update it means to create new ones and assign them, then with option B the BIND servers will be redundant and will create extra cost (resolver endpoints & the EC2s for DNS).

DucSiu 8 months, 3 weeks ago

Selected Answer: AC

AC is correct

zyademad 9 months, 4 weeks ago

Selected Answer: BD

Please refer the below extract taken from the link - https://aws.amazon.com/blogs/security/simplify-dns-management-in-a-multiaccount-environment-with-route-53-resolver/ "You can mount an Amazon EFS file system on an Amazon EC2 instance using DNS names. The file system DNS name automatically resolves to the mount target's IP address in the Availability Zone of the connecting Amazon EC2 instance. To be able to do that, the VPC must use the default DNS provided by Amazon to resolve EFS DNS names. If you plan to use EFS in your environment, I recommend that you resolve EFS DNS names locally and avoid sending these queries to central DNS because clients in that case would not receive answers optimized for their availability zone, which might result in higher operation latencies and less durability." So, option B) answers EFS resolution from VPC. Combination of Option B) and D) explains resolution from on-prem

dspd 1 year, 2 months ago

Selected Answer: D

Question itself is not clearly define

RavikantKumarRavi 1 year, 2 months ago

Selected Answer: AE

Update all the VPC DHCP option : DHCP option set never get updated , it created and associated with VPC hence B & C is incorrect .

Raphaello 1 year, 11 months ago

Selected Answer: BD

BD are the correct answer. Need to switch to "AWSProvidedDNS" in DHCP Options sets to enable resolving EFS endpoint URLs. In addition, a DNS outbound endpoint is required in the central VPC to allow forwarding queries to on-prem DNS as required, which needs to create forwarding rules and share them among AWS Org member accounts.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is BD according to SPOTO products.

nuzz 2 years, 3 months ago

Combo options is what makes it difficult to understand these type of questions - an option should support another option if you need to select two. then by the process of elimination of what two options can be combined - A D. B is wrong it says update DHCP option set, you cannot update DHCP option set - you would need to delete and recreate it.

drake2020 2 years, 3 months ago

all i can say is BC is wrong because you cannot update DHCP Option set once created..

ca82cda 2 years, 3 months ago

yes you can i just saw that options on the console

Nel07 1 year, 4 months ago

The question say update the VPC DHCP Option set and not update DHCP Option set. So the VPC can update his DHCP Option set to use the default one with AmazonProvidedDNS. B D

task_7 2 years, 3 months ago

Selected Answer: BC

A & E-- wrong D -AWS Resource Access Manager (AWS RAM). This is also not required. While creating rule we can just select all the required VPC to share the rule. Left with B& C • B. Create an Amazon Route 53 Resolver outbound endpoint in the central VPC. Update all the VPC DHCP options sets to use AmazonProvidedDNS for name resolution.

• C. Create an Amazon Route 53 Resolver inbound endpoint in the central VPUpdate all the VPC DHCP options sets to use the Route 53 Resolver inbound endpoint in the central VPC for name resolution.

MarcosSantos 2 years, 4 months ago

Hello everyone, given all the discussion and alternatives, the only options are the letters A and D. Incorrect B and C, we were unable to update the DHCp Option Set, only create a new one. Letter E, it is not possible to create a hosted zone with amazonaws.com, it is restricted. So, leaving only the other options, my particular answer was D and E.

MEDES 2 years, 6 months ago

I vote B and D. What the company want to to is as following. https://docs.aws.amazon.com/whitepapers/latest/hybrid-cloud-dns-options-for-vpc/route-53-resolver-endpoints-and-forwarding-rules.html The combination of A and E also seems to work. But the maintenance overhead for the custom DNS server remains. That is not a good practice.

https://zhangxuetu.online

[202610]

Question #12 Topic 1

An ecommerce company is hosting a web application on Amazon EC2 instances to handle continuously changing customer demand. The EC2 instances are part of an Auto Scaling group. The company wants to implement a solution to distribute traffic from customers to the EC2 instances. The company must encrypt all traffic at all stages between the customers and the application servers. No decryption at intermediate points is allowed.
Which solution will meet these requirements?

A. Create an Application Load Balancer (ALB). Add an HTTPS listener to the ALB. Configure the Auto Scaling group to register instances with the ALB's target group.

B. Create an Amazon CloudFront distribution. Configure the distribution with a custom SSL/TLS certificate. Set the Auto Scaling group as the distribution's origin.

C. Create a Network Load Balancer (NLB). Add a TCP listener to the NLB. Configure the Auto Scaling group to register instances with the NLB's target group. **Most Voted**

D. Create a Gateway Load Balancer (GLB). Configure the Auto Scaling group to register instances with the GLB's target group.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Untamables **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C If you need to pass encrypted traffic to the targets without the load balancer decrypting it, create a TCP listener on port 443 instead of creating a TLS listener. https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html

begmustkim4313 2 months ago

Selected Answer: C

c is correct

exampb007 1 year, 4 months ago

Option B ...Encryption at all stages: The requirement specifies that all traffic must be encrypted at all stages, with no decryption at intermediate points. Amazon CloudFront is a content delivery network (CDN) that supports end-to-end encryption (from the customer to the application). By configuring CloudFront with a custom SSL/TLS certificate, traffic between the customer and CloudFront (as well as between CloudFront and the origin) can be fully encrypted. No

decryption at intermediate points: With CloudFront, you can ensure that traffic remains encrypted, and CloudFront acts as a proxy for the traffic without decrypting it. It only forwards the traffic (still encrypted) to the application servers.

Raphaello 1 year, 11 months ago

Selected Answer: C

With ALB HTTPS listener will have ALB itself to intercept and terminate SSL/TLS connection. NLB will TCP listener will allow SSL/TLS connections to passthrough to backend app. servers where they can decrypt the flow.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

Snape 2 years, 2 months ago

Selected Answer: C

'No decryption at intermediate points is allowed.'

MEDES 2 years, 6 months ago

C If you need to pass encrypted traffic to the targets without the load balancer decrypting it, create a TCP listener on port 443 instead of creating a TLS listener. https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html

JoeAWS 2 years, 10 months ago

ALB is wrong because entire network packet needs to be forwarded

emmanuelodenyire 2 years, 10 months ago

Selected Answer: C

C is the correct answer here Based on the requirements given in the question, option C is the most suitable and correct solution. The Network Load Balancer (NLB) can handle TCP and UDP traffic, and it can also encrypt traffic with SSL/TLS encryption. Additionally, NLB is designed for high performance, low latency traffic and can handle millions of requests per second, making it well-suited for handling the continuously changing customer demand mentioned in the question. Option A, creating an Application Load Balancer (ALB), is also a viable solution for load balancing traffic to the EC2 instances, but it may not be the best option for handling high volumes of TCP and UDP traffic, especially when it comes to real-time applications.

slackbot 2 years, 11 months ago

Selected Answer: C

C covers the requirement for end-to-end encryption

ohcan 2 years, 12 months ago

Selected Answer: C

C is the only option that provides the connection from client not to be terminated in any intermediate point but the application server

helloworldabc 3 years ago

AAAAAAAAAAAAA

zaazanuna 3 years ago

Option C may be a valid solution, but it only provides transport layer security (TLS) encryption, not end-to-end encryption. Additionally, TCP listeners cannot inspect the contents of traffic, so the Network Load Balancer would not be able to ensure that traffic is not decrypted at intermediate points.

zaazanuna 3 years ago

Option C, creating a Network Load Balancer (NLB), is a Layer 4 load balancer that can distribute incoming traffic to EC2 instances based on IP protocol data such as TCP, UDP, or SSL. However, it does not provide the same routing and load balancing capabilities as an ALB, which can route traffic based on application layer data such as HTTP headers.

study_aws1 3 years ago

Should be option C). Requirement is for end-end encryption in transit between customer & instances (EC2), and hence requires NLB with TCP passthrough.

flowers00 3 years ago

C - correct.

https://zhangxuetu.online

[202610]

Question #13 Topic 1

A company has two on-premises data center locations. There is a company-managed router at each data center. Each data center has a dedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface. The router for the first location is advertising 110 routes to the Direct Connect gateway by using BGP, and the router for the second location is advertising 60 routes to the Direct Connect gateway by using BGP. The Direct Connect gateway is attached to a company VPC through a virtual private gateway.
A network engineer receives reports that resources in the VPC are not reachable from various locations in either data center. The network engineer checks the VPC route table and sees that the routes from the first data center location are not being populated into the route table. The network engineer must resolve this issue in the most operationally efficient manner.
What should the network engineer do to meet these requirements?

A. Remove the Direct Connect gateway, and create a new private virtual interface from each company router to the virtual private gateway of the VPC.

B. Change the router configurations to summarize the advertised routes. Most Voted

C. Open a support ticket to increase the quota on advertised routes to the VPC route table.

D. Create an AWS Transit Gateway. Attach the transit gateway to the VPC, and connect the Direct Connect gateway to the transit gateway.

Correct Answer: B

Community vote distribution



Comments

study_aws1 Highly Voted 3 years ago

Option B) - You can announce a maximum of 100 prefixes to AWS.These routes can be automatically be propagated into subnet route tables • In order to advertise more than 100 prefixes, you should summarize the prefixes into larger range to reduce number of prefixes

emmanuelodenyire Highly Voted 2 years, 10 months ago

Selected Answer: B

The correct answer to this question is option B: Change the router configurations to summarize the advertised routes. Here's why: The issue described in the question is that the VPC route table is not receiving all of the advertised routes from the on-premises routers. The router at the first location is advertising 110 routes, but those routes are n

begmustkim4313 2 months ago

Selected Answer: B

b is correct answer

zyademad 9 months, 4 weeks ago

Selected Answer: B

Option B) - You can announce a maximum of 100 prefixes to AWS.These routes can be automatically be propagated into subnet route tables • In order to advertise more than 100 prefixes, you should summarize the prefixes into larger range to reduce number of prefixes

Ubermensch 10 months ago

Selected Answer: B

B: reason as already mentioned that virtual vif only supports only 100 prefixes and need to summarize the prefixes. D: Will not work for the same reason, you need TRANSIT VIF along with TGW to support Up to 20,000 prefixes, and is not mentioned in the option.

Akivox 1 year, 6 months ago

Selected Answer: B

B: Customer needs to summarise the routes and advertise. Not D, because a transit gateway requires a transit VIF, this point doesn't mention about transit VIF.

acloudguru 1 year, 10 months ago

Selected Answer: D

Operational Overhead: Implementing and maintaining route summarization configurations can introduce additional operational overhead and complexity, especially in dynamic environments where network changes are frequent.

Raphaello 1 year, 11 months ago

Selected Answer: B

Correct answer is B. Private VIF accept up to 100 prefixes. Need to summarize (merge) some advertised prefixes to lower those 110.

skjb 1 year, 12 months ago

The correct answer to this question is option B

patanjali 2 years ago

Selected Answer: B

Yes, there is a limit of 100 routes limit via Direct Connect with transit vif or privat vif (https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html), if your route advertise more than that, the BGP session will go idle (DOWN). You can do a route summarization if you can or consider using Transit Gateway Connect to build a overlay GRE tunnel with BGP session to advertise your routing information.

WherecanIstart 2 years ago

Selected Answer: B

Route summarization is the most efficient way for this circumstances.

vikasj1in 2 years, 1 month ago

Selected Answer: B

The issue appears to be related to the number of routes advertised from each data center location. AWS Direct Connect has a limit on the number of routes that can be advertised to a virtual private gateway in a VPC (100 routes by default). In this case, the router for the first data center is advertising 110 routes, which exceeds the default limit, leading to the routes not being populated into the VPC route table. To resolve this issue in the most operationally efficient manner, the network engineer should consider summarizing the advertised routes. Summarizing routes involves aggregating a set of routes into a single, more general route. In BGP, this is typically done using route

summarization. By changing the router configurations to summarize the advertised routes, the network engineer can reduce the number of routes being advertised to the Direct Connect gateway, ensuring that it stays within the route limit imposed by AWS.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is B according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is B.

nuzz 2 years, 3 months ago

Pick B because D is wrong. Q: Can I associate my AWS Transit Gateway to the AWS Direct Connect gateway attached to a private virtual interface? No, an AWS Transit Gateway can only be associated with the AWS Direct Connect gateway attached to transit virtual interface. https://aws.amazon.com/directconnect/faqs

yanhiro 2 years, 3 months ago

Selected Answer: B

Option B) See this link (https://repost.aws/questions/QURPt7zKeWSr6-JvM5YQSgvA/aws-direct-connect-route-limit)

FayeG 2 years, 4 months ago

Selected Answer: B

aggreation is the correct answer

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #14 Topic 1

A company has expanded its network to the AWS Cloud by using a hybrid architecture with multiple AWS accounts. The company has set up a shared AWS account for the connection to its on-premises data centers and the company offices. The workloads consist of private web-based services for internal use. These services run in different AWS accounts. Office-based employees consume these services by using a DNS name in an on-premises DNS zone that is named example.internal.

The process to register a new service that runs on AWS requires a manual and complicated change request to the internal DNS. The process involves many teams.

The company wants to update the DNS registration process by giving the service creators access that will allow them to register their DNS records. A network engineer must design a solution that will achieve this goal. The solution must maximize cost-effectiveness and must require the least possible number of configuration changes.

Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Create a record for each service in its local private hosted zone (serviceA.account1.aws.example.internal). Provide this DNS record to the employees who need access.

B. Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created. **Most Voted**

C. Create an Amazon Route 53 Resolver rule to forward any queries made to onprem.example.internal to the on-premises DNS servers.

D. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain. **Most Voted**

E. Launch two Amazon EC2 instances in the shared AWS account. Install BIND on each instance. Create a DNS conditional forwarder on each BIND server to forward queries for each subdomain under aws.example.internal to the appropriate private hosted zone in each AWS account. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the IP addresses of the BIND servers.

F. Create a private hosted zone in the shared AWS account for each account that runs the service. Configure the private hosted zone to contain aws.example.internal in the domain (account1.aws.example.internal). Associate the private hosted zone with the VPC that runs the service and the shared account VPC. **Most Voted**

Correct Answer: BDF

Community vote distribution



Comments

AdamWest Highly Voted 2 years, 4 months ago

Selected Answer: BDF

B. Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created. This will enable DNS resolution between on-premises networks and AWS. D. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain. This allows you to simplify DNS management for your AWS services and resources within your shared account. F. Create a private hosted zone in the shared AWS account for each account that runs the service. Configure the private hosted zone to contain aws.example.internal in the domain (account1.aws.example.internal). Associate the private hosted zone with the VPC that runs the service and the shared account VPC. This allows individual AWS accounts to maintain their DNS entries.

devopsbro Highly Voted 2 years, 6 months ago

BDF - Inbound resolver endpoint and forwarder rule in on-premises DNS Servers, Private Hosted Zones for aws.example.internal and sub domain delegation to respective services (service<x>.aws.example.internal), and association the sub domain private hosted zones with respective VPCs in other accounts.

begmustkim4313 2 months ago

Selected Answer: BDF

b,d,f is correct answer

Joselito79 2 months, 2 weeks ago

Selected Answer: BDF

 B. Create an Amazon Route 53 Resolve inbound endpoint in the shared account VPC. Create a conditional forwarder for aws.example.internal on the on-premises DNS servers. It is essential for hybrid integration. D. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account Base of the self-service model. F. Create a private hosted zone in the shared AWS account for each account that runs the service (account1.aws.example.internal). Associate it with both VPCs. Best practice AWS for multi-account DNS

zyademad 9 months, 4 weeks ago

Selected Answer: BDF

B. Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created. This will enable DNS resolution between on-premises networks and AWS. D. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain. This allows you to simplify DNS management for your AWS services and resources within your shared account. F. Create a private hosted zone in the shared AWS account for each account that runs the service. Configure the private hosted zone to contain aws.example.internal in the domain (account1.aws.example.internal). Associate the private hosted zone with the VPC that runs the service and the shared account VPC. This allows individual AWS accounts to maintain their DNS entries.

Raphaello 1 year, 5 months ago

Selected Answer: BDF

BDF are the correct answers. In order.. D. create a private hosted zone for aws-hosted domain. F. create sub-domains in each of the associated accounts. B. create resolver inbound endpoint in the shared account, and forwarding rules.

michele_scar 1 year, 7 months ago

Selected Answer: BDF

B and D are correct for sure. The question is between A and F. Initial I was gone with A but the last phrase of D that specify the "VPC Association" let me change the answer to F. The A is more smart but it's missing the VPC Association that without that you can't make the inbound resolver resolve the traffic.

michele_scar 1 year, 7 months ago

the last phrase of F **

Marfee400704 1 year, 7 months ago

I think that it's correct answer is ABD according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is B & D & F.

Snape 1 year, 8 months ago

Selected Answer: ABF

https://docs.aws.amazon.com/whitepapers/latest/hybrid-cloud-dns-options-for-vpc/scaling-dns-management-across-multiple-accounts-and-vpcs.html

Anbukumar1984 1 year, 9 months ago

BCD is the correct answer

cumzle_com 1 year, 10 months ago

ABD: Explanation To meet the requirements of updating the DNS registration process while maximizing costeffectiveness and minimizing configuration changes, the network engineer should take the following steps: Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created (Option B). Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain (Option D). Create a record for each service in its local private hosted zone (serviceA.account1.aws.example.internal). Provide this DNS record to the employees who need access (Option A). These steps will allow service creators to register their DNS records while keeping costs low and minimizing configuration changes.

Vinsmoke 2 years ago

Selected Answer: BDF

Following architecture verifies: https://aws.amazon.com/blogs/architecture/using-route-53-private-hosted-zones-for-cross-account-multi-region-architectures/

prajkash 2 years, 2 months ago

Selected Answer BCF

alextl 2 years, 3 months ago

Selected Answer: ABC

A for giving the service creators access that will allow them to register their DNS records. B for Office-based employees consume these services. C for The company has set up a shared AWS account for the connection to its on-premises data centers and the company offices.

trap 2 years, 4 months ago

b,d,f is the correct D: You create aws.example.internal private dns zone in the shared account. The goal is to move the dns record management to the service creators in the aws F: You create a separate aws.example.internal sub

domain zone for each aws account. e.g account1.aws.example.internal, account2.aws.example.internal e.t.c. You can give separate permissions for each zone so the service creators can manage their own service dns records. B:You create a route 53 inbound resolver in the shared account and you create conditional forwarding rules for the aws.example.internal domain (it includes its subdomains) to the route 53 in the on premise dns servers so the office users will be able to resolve internally all the shared account's route 53 private zone's dns entries

trap 2 years, 4 months ago

Not A: service creators must be able to register their own dns records, Not C: AWS services don't need to resolve the example.internal domain from the onprem DNS Not E:Amazon ec2 instances cost more and require more configuration changes The link below gives all the needed info: https://docs.aws.amazon.com/whitepapers/latest/hybrid-cloud-dns-options-for-vpc/scaling-dns-management-across-multiple-accounts-and-vpcs.html

devopsbro 2 years, 4 months ago

BDF - This is the use case for inbound resolver endpoint and sub domain delegations. Inbound resolver can be used to forward the requests from on-premise to AWS and aws.example.internal hosted zone can delegate the requests to various sub domains (AccountX.aws.example.internal) by having respective entries.

https://zhangxuetu.online

[202610]

Question #15 Topic 1

A company has multiple AWS accounts. Each account contains one or more VPCs. A new security guideline requires the inspection of all traffic between VPCs.
The company has deployed a transit gateway that provides connectivity between all VPCs. The company also has deployed a shared services VPC with Amazon EC2 instances that include IDS services for stateful inspection. The EC2 instances are deployed across three Availability Zones. The company has set up VPC associations and routing on the transit gateway. The company has migrated a few test VPCs to the new solution for traffic inspection.
Soon after the configuration of routing, the company receives reports of intermittent connections for traffic that crosses Availability Zones.
What should a network engineer do to resolve this issue?

A. Modify the transit gateway VPC attachment on the shared services VPC by enabling cross-Availability Zone load balancing.

B. Modify the transit gateway VPC attachment on the shared services VPC by enabling appliance mode support. Most Voted

C. Modify the transit gateway by selecting VPN equal-cost multi-path (ECMP) routing support.

D. Modify the transit gateway by selecting multicast support.

Correct Answer: B

Community vote distribution



Comments

study_aws1 Highly Voted 2 years, 6 months ago

Please note "IDS services for stateful inspection" - this implies the same appliance is followed for the life of the connection. This is only achieved by on the shared services VPC by enabling appliance mode support

navi7 Highly Voted 2 years, 6 months ago

Selected Answer: B

Appliance mode should be enabled to ensure that the returning traffic (in case of stateful connections) takes the same path as incoming traffic, otherwise it might go to different AZs

begmustkim4313 2 months ago

Selected Answer: B

b is correct

prad_kum1 7 months, 3 weeks ago

Selected Answer: B

stateful inspection and appliance mode

zyademad 9 months, 4 weeks ago

Selected Answer: B

Please note "IDS services for stateful inspection" - this implies the same appliance is followed for the life of the connection. This is only achieved by on the shared services VPC by enabling appliance mode support

Raphaello 1 year, 5 months ago

Selected Answer: B

B is the correct answer. Need to ensure that Appliance mode is enabled for traffic to remain on the same inspecting IDS, regardless of the source and destination AZ's (to overcome AZ affinity).

patanjali 1 year, 6 months ago

Selected Answer: B

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html#transit-gateway-appliance-support

vikasj1in 1 year, 7 months ago

Selected Answer: B

The issue described suggests a problem with the inspection of traffic that crosses Availability Zones. To resolve this, you should enable "appliance mode" on the transit gateway attachment for the shared services VPC. In the context of AWS Transit Gateway, appliance mode is a feature designed for network appliances, such as intrusion detection or prevention systems (IDS/IPS). When appliance mode is enabled, the transit gateway forwards traffic to the appliance instances in a more predictable manner, ensuring that the same flow of traffic goes consistently to the same appliance.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is B according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is A.

prajkash 2 years, 2 months ago

Selected answer: B

emmanuelodenyire 2 years, 4 months ago

Selected Answer: A

To resolve the issue of intermittent connections for traffic that crosses Availability Zones in a transit gateway setup that provides connectivity between multiple VPCs, the correct answer is A. Modify the transit gateway VPC attachment on the shared services VPC by enabling cross-Availability Zone load balancing. Option A is the correct answer because enabling cross-Availability Zone load balancing will distribute the traffic across multiple Availability Zones, thereby preventing the issue of intermittent connections. This solution will ensure that traffic is not bottlenecked on a single Availability Zone, reducing the likelihood of connection issues.

Cappy46789 2 years, 6 months ago

Selected Answer: B

B - https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

zaazanuna 2 years, 6 months ago

I know I answered B earlier but after some digging, I am kind of leaning towards A. Would not modifying the transit gateway VPC attachment on the shared services VPC by enabling cross-Availability Zone load balancing will ensure that traffic is evenly distributed across all Availability Zones, improving the overall performance and availability of the solution

slackbot 2 years, 5 months ago

there is no such thing

flowers00 2 years, 6 months ago

B - correct.

zaazanuna 2 years, 6 months ago

B - correct

https://zhangxuetu.online

[202610]

Question #16 Topic 1

A company is using a NAT gateway to allow internet connectivity for private subnets in a VPC in the us-west-2 Region. After a security audit, the company needs to remove the NAT gateway.
In the private subnets, the company has resources that use the unified Amazon CloudWatch agent. A network engineer must create a solution to ensure that the unified CloudWatch agent continues to work after the removal of the NAT gateway.
Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Validate that private DNS is enabled on the VPC by setting the enableDnsHostnames VPC attribute and the enableDnsSupport VPC attribute to true. Most Voted

B. Create a new security group with an entry to allow outbound traffic that uses the TCP protocol on port 443 to destination 0.0.0.0/0

C. Create a new security group with entries to allow inbound traffic that uses the TCP protocol on port 443 from the IP prefixes of the private subnets. Most Voted

D. Create the following interface VPC endpoints in the VPC: com.amazonaws.us-west-2.logs and com.amazonaws.us-west-2.monitoring. Associate the new security group with the endpoint network interfaces. Most Voted

E. Create the following interface VPC endpoint in the VPC: com.amazonaws.us-west-2.cloudwatch. Associate the new security group with the endpoint network interfaces.

F. Associate the VPC endpoint or endpoints with route tables that the private subnets use.

Correct Answer: ACD

Community vote distribution



Comments

slackbot Highly Voted 2 years, 11 months ago

Selected Answer: ACD

A,C and D

Untamables Highly Voted 2 years, 11 months ago

Selected Answer: ACD

A, C, and D An interface VPC endpoint provides reliable, scalable connectivity to CloudWatch without requiring a NAT gateway. https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-and-interface-VPC.html

https://docs.aws.amazon.com/vpc/latest/privatelink/aws-services-privatelink-support.html To use private DNS, you must enable DNS hostnames and DNS resolution for your VPC. The security group for the interface endpoint must allow communication between the endpoint network interface and the resources in your VPC that must communicate with the service. https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

ddtn 2 years, 10 months ago

D) would be correct if the URL are not messed up: monitoring.eu-west-2.amazonaws.com and logs.eu-west-2.amazonaws.com

JoellaLi 2 years ago

No. The URL are correct. https://docs.aws.amazon.com/vpc/latest/privatelink/aws-services-privatelink-support.html

matanasov 11 months, 1 week ago

Selected Answer: ADF

A - Private DNS must be enabled for this to work in private subnets D - The unified CloudWatch agent needs to communicate with both CloudWatch Logs and CloudWatch Metrics (Monitoring). These two interface endpoints are required F -This ensures that traffic from the private subnets can reach the interface endpoints, enabling communication with CloudWatch services

zain1258 1 year, 7 months ago

Selected Answer: ACD

A, C and D

hedglin 1 year, 8 months ago

A,B and D. Option C is not needed because we're not concerned with inbound traffic for this scenario.

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

Raphaello 1 year, 11 months ago

Selected Answer: ACD

ACD are the correct answers. Service PrivateLink endpoints https://docs.aws.amazon.com/vpc/latest/privatelink/aws-services-privatelink-support.html

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

patanjali 2 years ago

Selected Answer: ACD

https://repost.aws/knowledge-center/cloudwatch-unified-agent-metrics-issues Confirm connectivity to the CloudWatch endpoints When traffic to CloudWatch should not transit the public internet, you can use VPC endpoints instead. If you are using VPC endpoints, check the following: If you are using private nameservers, confirm that DNS resolution provided accurate responses. Confirm that the CloudWatch endpoints resolve to private IP addresses. Confirm the security group associated with the VPC endpoint allows inbound traffic from the host.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is ACF according to SPOTO products.

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

marfee 2 years, 1 month ago

I think that it's correcty answer is A ＆ B ＆ D.

AmSpOkE 2 years, 1 month ago

Selected Answer: ACD

Answers are A, C and D 100% sure.

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

WMF0187 2 years, 6 months ago

The Unified CloudWatch Agent uses port 443, which is the default port for HTTPS traffic, for secure communication with CloudWatch. The endpoint name associated with CloudWatch is "monitoring.us-east-1.amazonaws.com" (for the US East region). The endpoint may vary depending on the AWS region where you are operating.

siiiww 2 years, 6 months ago

for sure A,B,D dont need inbound rules .... I tested 3 yrs ago. NEED ONLY OUTBOUND

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

sp237 2 years, 8 months ago

How is A a valid option for private subnet? enableDnsHostname (= DNS Hostname setting) Indicates whether instances with public IP addresses get corresponding public DNS hostnames. If this attribute is true, instances in the VPC get public DNS hostnames, but only if the enableDnsSupport attribute is also set to true .

AlohaEva 1 year, 7 months ago

enabling enableDnsHostnames and enableDnsSupport VPC attributes will allow using private DNS resolution, and it is a prerequisites for creating Interface Endpoint https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

emmanuelodenyire 2 years, 10 months ago

Selected Answer: ADF

There seems to be some disagreement among different individuals about the answer to this question. However, based on the requirements provided and the skills being tested, I believe the correct answer is A, D, and F. F is correct because associating the VPC endpoint with the route tables that the private subnets use is necessary to ensure that traffic is routed through the VPC endpoint. Option C is incorrect because it suggests creating inbound rules for the TCP protocol on port 443 from the IP prefixes of the private subnets. However, this is not necessary to allow the unified CloudWatch agent to continue working after the removal of the NAT gateway. In fact, creating inbound rules for port 443 is not related to the problem statement, since the issue is about ensuring the CloudWatch agent can communicate with AWS services without using a NAT gateway. Creating inbound rules would only be necessary if you wanted to allow external traffic to access resources within your VPC over HTTPS on port 443.

TravelKo 2 years, 8 months ago

I think it is other way round. If you need to route external traffic you need an entry in the route table. For external or internal you need an entry in the Security group.

task_7 2 years, 5 months ago

I agree A enableDnsSupport Determines whether the VPC supports DNS resolution through the Amazon provided DNS server. If this attribute is true, queries to the Amazon provided DNS server succeed. For more information, see Amazon DNS server. D VPC end points for logs and CW Metrics F Subnet can route traffic to VPC endpoint Since NAT was running SG rule for 443 would be in place

ILOVEVODKA 2 years, 12 months ago

https://repost.aws/knowledge-center/cloudwatch-unified-agent-metrics-issues ACD

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

navi7 3 years ago

Selected Answer: ACD

B is incorrect as we don't need to create outbound rules for interface endpoint. "Note: You don't need to create a rule in the outbound direction of the security group associated with the interface endpoint." https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint A is also partially correct as normally CloudWatch Agent uses public endpoints but it can be overridden. But since other options are incorrect so A is a right choice here.

AlohaEva 1 year, 7 months ago

The security group is for Endpoint Network Interface, so the traffic which comes from the private subnet (our VPC) is inbound for Endpoint Network Interface. That's why we need inbound traffic allowance https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

Cappy46789 3 years ago

Selected Answer: ABD

ABD - https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #17 Topic 1

An international company provides early warning about tsunamis. The company plans to use IoT devices to monitor sea waves around the world. The data that is collected by the IoT devices must reach the company's infrastructure on AWS as quickly as possible. The company is using three operation centers around the world. Each operation center is connected to AWS through Its own AWS Direct Connect connection. Each operation center is connected to the internet through at least two upstream internet service providers.
The company has its own provider-independent (PI) address space. The IoT devices use TCP protocols for reliable transmission of the data they collect. The IoT devices have both landline and mobile internet connectivity. The infrastructure and the solution will be deployed in multiple AWS Regions. The company will use Amazon Route 53 for DNS services.
A network engineer needs to design connectivity between the IoT devices and the services that run in the AWS Cloud.
Which solution will meet these requirements with the HIGHEST availability?

A. Set up an Amazon CloudFront distribution with origin failover. Create an origin group for each Region where the solution is deployed.

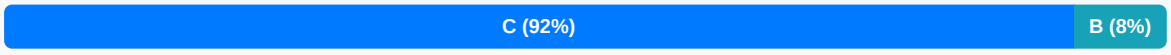
B. Set up Route 53 latency-based routing. Add latency alias records. For the latency alias records, set the value of Evaluate Target Health to Yes.

C. Set up an accelerator in AWS Global Accelerator. Configure Regional endpoint groups and health checks. **Most Voted**

D. Set up Bring Your Own IP (BYOIP) addresses. Use the same PI addresses for each Region where the solution is deployed.

Correct Answer: C

Community vote distribution



Comments

Untamables **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html
https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html

study_aws1 **Highly Voted** 3 years ago

Should be Option B) as per the architecture given in the link https://aws.amazon.com/blogs/iot/automate-global-device-provisioning-with-aws-iot-core-and-amazon-route-53/

6008af2 7 months, 2 weeks ago

Selected Answer: C

C. AWS Global Accelerator (plus Route 53 for DNS) is the AWS-recommended, highest-availability architecture for your scenario. Route 53 will still be used—for DNS management and to point IoT devices to Global Accelerator IPs. Global Accelerator is for highly available, TCP-based, multi-region, real-time failover routing.

clphan 1 year, 7 months ago

The queston is not really clear, they do not state the goal. though seem C with global accerlator can help improve HA

cerifyme85 1 year, 11 months ago

Selected Answer: B

"The solution must use route 53 dns" B

Raphaello 1 year, 11 months ago

Selected Answer: C

Long case scenario, giving snippets of information; but C (AGA) felt the most appropriate solution for high availability and delivering data so quickly (through AWS backbone).

vikasj1in 2 years, 1 month ago

Selected Answer: C

AWS Global Accelerator is designed to provide a highly available and performant solution for global applications. It uses anycast IP addresses to route traffic to optimal AWS endpoint locations. In this scenario, setting up an accelerator in AWS Global Accelerator with Regional endpoint groups is suitable for the distributed architecture of the IoT devices and the AWS infrastructure. Options A and B involve Amazon CloudFront and Route 53 latency-based routing, respectively, but AWS Global Accelerator is specifically designed to provide highly available, low-latency, and fault-tolerant global routing, making it a more suitable choice for this scenario. Option D, Bring Your Own IP (BYOIP) addresses, is not directly related to optimizing the connectivity for IoT devices and services in AWS, and it doesn't address the global distribution and routing requirements as effectively as AWS Global Accelerator.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is B.

marfee 2 years, 1 month ago

I think that it's correcty answer is B.

AmSpOkE 2 years, 1 month ago

Selected Answer: C

It says the "Highest" throughtput, anything with VPN is limited to 1.25 Gbps per tunnel.

Sourabh1703 2 years, 1 month ago

Selected Answer: B

Highest SLA requirement indicate that route 53 has to be used, it is the only service that gives 100% availability . https://aws.amazon.com/route53/sla/ , the same page for Global Accelerator lists 99.9% only. I would choose B over C for this reason.

ChinkSantana 2 years, 1 month ago

Quick hack: Once its a global service that involves TCP or UDP, Eliminate the options quickly by pointing to Global Accelerator

MarcosSantos 2 years, 2 months ago

Hello everyone, I saw some people talking about option B. But B is wrong. It can be used but the record it would create would be CNAME and not ALIAS record. https://aws.amazon.com/blogs/iot/automate-global-device-provisioning-with-aws-iot-core-and-amazon-route-53/ The option explicitly talks about using Alias and iots cannot be configured as a registry for an alias. Option C is correct!

Arad 2 years, 4 months ago

Selected Answer: C

Definitely C

payelix795 2 years, 7 months ago

The wording of this question is kinda odd.So bouncing between B and C For me the following makes me think C is the right option "A network engineer needs to design connectivity between the IoT devices and the services that run in the AWS Cloud" Kind of a tricky one this.

awsguru1998 2 years, 12 months ago

C Using AWS Global Accelerator with regional endpoint groups provides the highest availability as it allows traffic to be routed to healthy endpoints in different regions. Additionally, health checks can ensure that traffic is not directed to unhealthy endpoints.

https://zhangxuetu.online

[202610]

Question #18 Topic 1

A company is planning a migration of its critical workloads from an on-premises data center to Amazon EC2 instances. The plan includes a new 10 Gbps AWS Direct Connect dedicated connection from the on-premises data center to a VPC that is attached to a transit gateway. The migration must occur over encrypted paths between the on-premises data center and the AWS Cloud.
Which solution will meet these requirements while providing the HIGHEST throughput?

A. Configure a public VIF on the Direct Connect connection. Configure an AWS Site-to-Site VPN connection to the transit gateway as a VPN attachment.

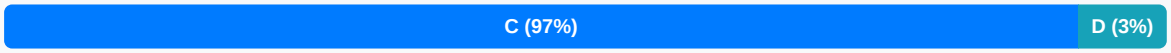
B. Configure a transit VIF on the Direct Connect connection. Configure an IPsec VPN connection to an EC2 instance that is running third-party VPN software.

C. Configure MACsec for the Direct Connect connection. Configure a transit VIF to a Direct Connect gateway that is associated with the transit gateway. **Most Voted**

D. Configure a public VIF on the Direct Connect connection. Configure two AWS Site-to-Site VPN connections to the transit gateway. Enable equal-cost multi-path (ECMP) routing.

Correct Answer: C

Community vote distribution



Comments

Untamables **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html

silviahdz **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C is correct, highest bps plus encryption

ForDummies 1 year, 7 months ago

I really hope not find some question like that, because I only can see mistakes. Macsec is used on L2L using layer 02 or direct connection (collocation feat AWS), like clear channel circuit, because you can see another mac address. But if you're using MPLS connection by AWS partner, it's not possible to use it. You can use VPN over DX, and you'll not suffer with latency or throughput, but it's necessary to use a virtual private gateway.
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html Related: AWS Direct Connect and AWS Site-to-Site VPN

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer here. MACSec at L2 provides highest throughput when compared to IPSEC VPN tunnels.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

AmSpOkE 2 years, 1 month ago

C as it says "Highest" throughtput, anything with VPN is limited to 1,25Gbps per tunnel

Snape 2 years, 2 months ago

Selected Answer: C

Options A and D are wrong because involvement of using VPN which can add admin overhead Option B IPsec VPN connection + third-party VPN software not as performant as MACsec-encrypted connection directly on the Direct Connect link.

Arad 2 years, 4 months ago

Selected Answer: C

For sure C

WMF0187 2 years, 6 months ago

Option C is the solution that will provide the highest throughput while meeting the requirement for an encrypted path between the on-premises data center and the AWS Cloud. Here's why: MACsec (Media Access Control Security): MACsec provides a layer 2 encryption mechanism, encrypting the entire Ethernet frame between the on-premises data center and the AWS Cloud. It offers high throughput while encrypting the data at the link layer. Transit VIF and Direct Connect Gateway: By configuring a transit VIF on the Direct Connect connection, you can connect it directly to a Direct Connect gateway associated with the transit gateway. This architecture allows you to efficiently route traffic to multiple VPCs attached to the transit gateway. Option D: While using AWS Site-to-Site VPN connections with ECMP routing can provide redundancy, it may not offer the highest throughput compared to MACsec over a dedicated 10 Gbps Direct Connect connection.

DPDK 2 years, 8 months ago

C because VPN's throughput is far lower than DX. We should not use VPN to achieve HIGHEST throughput

demoras 2 years, 9 months ago

Selected Answer: C

C is correct, highest bps plus encryption

dman 2 years, 11 months ago

Macsec does not extend until TGW its point to point, its would be only until the AWS DX router. Tricky one im more inclined to D

albertkr 2 years, 11 months ago

it does not say it has to extend until the VPC. it just says until AWS Cloud for which i assume it is until AWS DX router where it is the boundary to AWS Cloud

ohcan 2 years, 11 months ago

Selected Answer: C

MacSEC always provide more throughput than two IPsec tunnels that will reach only 1.5Gb each

tcp22 2 years, 9 months ago

it's 1.25 total of 2.5 for 2 tunnels

ITgeek 2 years, 12 months ago

Selected Answer: C

is Correct

study_aws1 2 years, 12 months ago

Does MACSec work with Transit VIF is the key here.

that1guy 2 years, 11 months ago

The only requirements for MACsec are that you have a dedicated Direct Connect connection and that the customer device supports it, see: https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html

https://zhangxuetu.online

[202610]

Question #19 Topic 1

A network engineer must develop an AWS CloudFormation template that can create a virtual private gateway, a customer gateway, a VPN connection, and static routes in a route table. During testing of the template, the network engineer notes that the CloudFormation template has encountered an error and is rolling back.
What should the network engineer do to resolve the error?

A. Change the order of resource creation in the CloudFormation template.

B. Add the DependsOn attribute to the resource declaration for the virtual private gateway. Specify the route table entry resource.

C. Add a wait condition in the template to wait for the creation of the virtual private gateway.

D. Add the DependsOn attribute to the resource declaration for the route table entry. Specify the virtual private gateway resource. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

devopsbro **Highly Voted** 3 years ago

D - Correct. Route table route entry can't reference the VPG if it is not available.

Untamables **Highly Voted** 2 years, 11 months ago

Selected Answer: D

D Reading all options, It seems that there is a problem of the run order for creating resources. According to the below AWS document, you must configure your route table to include the routes used by your Site-to-Site VPN connection and point them to your virtual private gateway.
https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html That means you must create the virtual private gateway before creating the route table. AWS CloudFormation does not support configuring detailed run order of creating resources. However, when you add a DependsOn attribute to a resource, that resource is created only after the creation of the resource specified in the DependsOn attribute.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html

Spaurito 1 year, 4 months ago

B - The stack should provision something like this VPGW -> CGW -> VPN -> RTs

Spaurito 1 year, 4 months ago

Revisited - could be A but option D is correct
https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html

Spaurito 1 year, 4 months ago

D -You can't add routes unless the route table is created first.

Raphaello 1 year, 11 months ago

Selected Answer: D

D is the correct answer.

patanjali 2 years ago

Selected Answer: D

You will DependsOn attribute is used in an AWS CloudFormation template. So, A and C cannot be answers. Option B is wrong because you will make route table change after you finish creating VPN tunnel. Hence, Option D is correct

vikasj1in 2 years, 1 month ago

Selected Answer: D

The DependsOn attribute is used in an AWS CloudFormation template to specify the order of resource creation. When you specify a resource in the DependsOn attribute of another resource, AWS CloudFormation creates the specified resource first before creating the resource with the DependsOn attribute. In this case, the error might be occurring because the CloudFormation template is attempting to create the route table entry before the virtual private gateway is created. By adding the DependsOn attribute to the resource declaration for the route table entry and specifying the virtual private gateway resource, you ensure that the virtual private gateway is created before the route table entry. Option B is incorrect because adding DependsOn to the route table entry for the virtual private gateway is more appropriate than specifying the route table entry for the virtual private gateway.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is D according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is D.

Arad 2 years, 4 months ago

Selected Answer: D

VGW must be created before RTB getting updated.

Certified101 2 years, 8 months ago

Selected Answer: D

Option B suggests adding a "DependsOn" attribute to the VGW resource declaration with the route table entry as the dependency. However, this would mean that the VGW wouldn't be created until after the route table entry, which isn't possible because the route table entry points to the VGW. On the other hand, option D suggests adding a "DependsOn" attribute to the route table entry resource declaration with the VGW as the dependency. This means the route table entry wouldn't be created until after the VGW, which is the correct order of operations. Therefore, D is the correct answer because the route table entry should depend on the VGW, not the other way around.

dyaz208 2 years, 9 months ago

Selected Answer: B

I think B is correct. "When you add a DependsOn attribute to a resource, that resource is created only after the creation of the resource specified in the DependsOn attribute."
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html

dyaz208 2 years, 9 months ago

Sorry. D is correct.

takecoffe 2 years, 10 months ago

Selected Answer: B

Adding the DependsOn attribute to the resource declaration for the route table entry (option D) would not resolve the error because the issue lies with the creation of the virtual private gateway, not the route table entry.

ITgeek 2 years, 10 months ago

Selected Answer: B

Answer is B

ohcan 2 years, 11 months ago

Selected Answer: D

D. The resource that takes more time to be created is the VPG, and there rest depends on it

Mandar 2 years, 12 months ago

Answer is B) If you create a route that references a transit gateway in the same template where you create the transit gateway, you must declare a dependency on the transit gateway attachment. The route table cannot use the transit gateway until it has successfully attached to the VPC. Add a DependsOn Attribute in the AWS::EC2::Route resource to explicitly declare a dependency on the AWS::EC2::TransitGatewayAttachment resource.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-route.html

navi7 3 years ago

Selected Answer: D

VPG is a dependancy for route table in this case.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #20 Topic 1

A company operates its IT services through a multi-site hybrid infrastructure. The company deploys resources on AWS in the us-east-1 Region and in the eu-west-2 Region. The company also deploys resources in its own data centers that are located in the United States (US) and in the United Kingdom (UK). In both AWS Regions, the company uses a transit gateway to connect 15 VPCs to each other. The company has created a transit gateway peering connection between the two transit gateways. The VPC CIDR blocks do not overlap with each other or with IP addresses used within the data centers. The VPC CIDR prefixes can also be aggregated either on a Regional level or for the company's entire AWS environment.

The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through Interior BGP (iBGP) sessions. The data centers maintain connectivity to AWS through one AWS Direct Connect connection in the US and one Direct Connect connection in the UK. Each Direct Connect connection is terminated on a Direct Connect gateway and is associated with a local transit gateway through a transit VIF.

Traffic follows the shortest geographical path from source to destination. For example, packets from the UK data center that are targeted to resources in eu-west-2 travel across the local Direct Connect connection. In cases of cross-Region data transfers, such as from the UK data center to VPCs in us-east-1, the private WAN connection must be used to minimize costs on AWS. A network engineer has configured each transit gateway association on the Direct Connect gateway to advertise VPC-specific CIDR IP prefixes only from the local Region. The routes toward the other Region must be learned through BGP from the routers in the other data center in the original, non-aggregated form.

The company recently experienced a problem with cross-Region data transfers because of issues with its private WAN connection. The network engineer needs to modify the routing setup to prevent similar interruptions in the future. The solution cannot modify the original traffic routing goal when the network is operating normally.

Which modifications will meet these requirements? (Choose two.)

A. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add the company's entire AWS environment aggregate route to the list of subnets advertised through the local Direct Connect connection.

B. Add the CIDR prefixes from the other Region VPCs and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection. Configure data center routers to make routing decisions based on the BGP communities received.

C. Add the aggregate IP prefix for the other Region and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection. **Most Voted**

D. Add the aggregate IP prefix for the company's entire AWS environment and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection.

E. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add both Regional aggregate IP prefixes to the list of subnets advertised through the Direct

Connect connection on both sides of the network. Configure data center routers to make routing decisions based on the BGP communities received. Most Voted

Correct Answer: CE

Community vote distribution



Comments

Untamables Highly Voted 2 years, 11 months ago

Selected Answer: CE

C and E If the private WAN failed, the network engineer would swing the traffic to the other region through the local Direct Connect and the Transit Gateways. That is the requirement. The solution is that the local DC has 2 kinds of route to the other region VPCs. One is the existing CIDR-based routes via the private WAN, another is the advertised aggregated routes from the local Direct Connect connection. CIDR-based routes are prior to the aggregated routes advertised from Direct Connect connection due to the longest prefix match routing algorithm. The options which match this solution are C and E.

steli0 5 months, 1 week ago

E is wrong because according to the bellow documentation, Region Scope BGP communities are only advertised in peerings over a public VIF. The question specifies a transit VIF.

slackbot Highly Voted 2 years, 11 months ago

Selected Answer: CD

B and E dont make sense as private and transit VIFs do not carry any BGP communities from AWS towards CGW. only CGW can send communities which AWS will use to route traffic back to customer the idea is: each DX GW must advertise the local VPCs CIDRs (which are more specific) and the remote region summarized routes (over iBGP local routers signify more specific routes to home regions).

slackbot 2 years, 11 months ago

this is regarding routing and communities: https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html also - note that DX GW can advertise no more than 20 routes towards CGW. hence, you cannot add all 30 VPCs CIDRs - you have to summarize.

albertkr 2 years, 10 months ago

where does on the link that you showed above that mentions private and transit VIFs do not carry any BGP communities from AWS towards CGW? It actually mentions that "For outbound routing policies, AWS Direct Connect applies the following BGP communities to its advertised routes...", which means, regardless of what type of VIF is used, the the advertised route from AWS always carries a BGP community. It makes E making sense.

albertkr 2 years, 10 months ago

you are right. After second reading, private and transit VIF don't apply the BGP community strings by default. The default behaviour is using the distance from the local Region to the Direct Connect location.

a0e6696 7 months, 1 week ago

Selected Answer: CD

C and E

a0e6696 7 months, 1 week ago

C and D

RavikantKumarRavi 1 year ago

Selected Answer: AC

AWS attached BGP community incase of public VIF not in case of private or transit VIF hence answer consist BGP communicate is wrong

dspd 1 year, 2 months ago

Selected Answer: CE

never seen such a long questions with unclear answer and goal. Closest answer C and E. Need lot of cleanup on content

VerRi 1 year, 6 months ago

Selected Answer: CE

This question is just insane, over 500 words, and the wording is hard to understand. You must draw a diagram and translate the words into English to understand them. In short, cross-region traffic was originally handled by private WAN, but now it is down. We have to find another way to do that. We have DXG and TGW in each region and 2 TGWs are peered. C: Add IPs for local and other regions E: Remove static VPC CIDR prefixes and add cross-region IP prefixes

Jonalb 1 year, 6 months ago

Selected Answer: CD

C and D Option C: The approach of advertising aggregated prefixes for each Region and local CIDR blocks can help simplify the routing table and address specific inter-region connectivity issues. However, if the configuration does not include prefixes for the entire AWS environment, there may be gaps in coverage, especially if WAN connectivity fails. Option D: The approach of advertising an aggregated IP prefix for the entire AWS environment in addition to local CIDR blocks tends to be more comprehensive. This ensures that the entire AWS infrastructure is covered and can more robustly address routing issues, especially in situations where the WAN connection fails.

AlirezaNetWorld 1 year, 6 months ago

C and E. I think, we all agree on the C; why E is correct? Because removing the individual VPC CIDR prefixes and using regional aggregate IP prefixes simplifies the routing table and helps in preventing routing issues, especially during cross-region data transfer.

Jonalb 1 year, 9 months ago

Selected Answer: CD

CD its a true!

Raphaello 1 year, 11 months ago

Honestly, I do not get the request here! It says.. "The company recently experienced a problem with cross-Region data transfers because of issues with its private WAN connection. The network engineer needs to modify the routing setup to prevent similar interruptions in the future." Does that mean, the request is adding for example a route from UK DC to AWS US VPC through DX/DxGW/TGW in case private WAN between UK DC and US DC failed?

Raphaello 1 year, 11 months ago

Drew it, and it became much easier. Anything with "aggregate IP prefix for the company's entire AWS environment" is wrong. As simple as that. Why? Cause we need the UK-VPC's apart from US-VPC's, cause in the normal network operation flow should go through the inter-DC's WAN connection, then need to keep prefixes from the "other" region apart to assign different AS_PATH or Community tags (differentiate them from local region prefixes). Therefore, I'd go

with BC as correct answer. Please note, the question is not asking for a combination of actions, it simply asks what modification can accomplish the ask. Either B or C can do that.

vikasj1in 2 years, 1 month ago

Selected Answer: CD

C. This ensures that the BGP advertisements include both the aggregate IP prefix for the other Region and the specific CIDR blocks for the local VPCs. This is useful for ensuring optimal routing and maintaining connectivity during cross-Region data transfers. D. this approach ensures that BGP advertisements include both the aggregate IP prefix for the entire AWS environment and the specific CIDR blocks for the local VPCs. This provides a more comprehensive view of the AWS environment, allowing the data center routers to make routing decisions based on the received BGP advertisements. By combining these modifications, you create a setup that allows for optimal routing and fault tolerance during cross-Region data transfers while still respecting the original traffic routing goals when the network is operating normally.

marfee 2 years, 1 month ago

I think that it's correcty answer is C & E.

asiansensation 2 years, 3 months ago

C,D are correct. You cannot receive BGP communities over DX as there is no way of configuring this in AWS. The on prem routers need to the send the respective BGP communities and AWS will respond accordingly. A does not make sense as it overlaps with D.

Arad 2 years, 4 months ago

Selected Answer: CD

B and E do not make sense as private and transit VIFs do not carry any BGP communities from AWS to CGW. A and E are also very destructive while it is asked the solution cannot modify original traffic routing goals. So the only options which make sense are C & D.

[Removed] 2 years, 8 months ago

Selected Answer: DE

Given the constraint Option E is correct because it removes all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection and adds both Regional aggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network. It also configures data center routers to make routing decisions based on the BGP communities received. Option D is correct because it adds both Regional aggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network. It also configures data center routers to make routing decisions based on the BGP communities received https://aws.amazon.com/blogs/networking-and-content-delivery/setting-up-aws-direct-connect-gateway-to-route-dx-traffic-to-any-aws-region/

Wiss7 2 years, 8 months ago

Selected Answer: CE

Private virtual interface and transit virtual interface BGP communities AWS Direct Connect supports local preference BGP community tags to help control the route preference of traffic on private virtual interfaces and transit virtual interfaces. https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

Chinmoy 2 years, 10 months ago

Selected Answer: CD

CD is correct because of more specific routes are advertised over local connections

https://zhangxuetu.online

[202610]

Question #21 Topic 1

A company's network engineer needs to design a new solution to help troubleshoot and detect network anomalies. The network engineer has configured Traffic Mirroring. However, the mirrored traffic is overwhelming the Amazon EC2 instance that is the traffic mirror target. The EC2 instance hosts tools that the company's security team uses to analyze the traffic. The network engineer needs to design a highly available solution that can scale to meet the demand of the mirrored traffic.
Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) as the traffic mirror target. Behind the NLB. deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring as necessary. **Most Voted**

B. Deploy an Application Load Balancer (ALB) as the traffic mirror target. Behind the ALB, deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring only during non-business hours.

C. Deploy a Gateway Load Balancer (GLB) as the traffic mirror target. Behind the GLB. deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring as necessary.

D. Deploy an Application Load Balancer (ALB) with an HTTPS listener as the traffic mirror target. Behind the ALB. deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring only during active events or business hours.

Correct Answer: A

Community vote distribution



Comments

Cheam **Highly Voted** 2 years, 8 months ago

Selected Answer: A

Another tricky question and consider the wording in the answers choices - "as the traffic mirror target". I have selected A because the NLB is a valid mirror target, but the GWLB is not (Answer C). Yes, comments supporting Answer C say that GWLB must also mean/include GLWB-E. Then you have two valid answers to the question where you can only select one. Therefore, it is A for me. Ref: https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html All the best.

dremm **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C) Makes more sense for the updated exam, GWLB is relatively new. Read the release post for GWLB - https://aws.amazon.com/about-aws/whats-new/2022/05/amazon-vps-traffic-mirroring-supports-sending-mirrored-traffic-gateway-load-balancer-backed-monitoring-appliances/ "This helps simplify the monitoring of network traffic

across AWS accounts and VPCs in a highly scalable and operationally efficient manner by removing routing complexity and operational overhead."

Joselito79 2 months, 2 weeks ago

Selected Answer: C

C. Deploy a Gateway Load Balancer (GLB) as the traffic mirror target. Behind the GLB, deploy a fleet of EC2 instances in an Auto Scaling group. Use Traffic Mirroring as needed. What the GLB does here: Receives encapsulated Layer 3/Layer 4 traffic (GENEVE) from Traffic Mirroring Distributes it transparently to multiple appliances Supports Auto Scaling Does not terminate sessions or protocols Does not alter the traffic

6008af2 7 months, 2 weeks ago

Selected Answer: C

Gateway Load Balancer is the only supported AWS load balancer that can be a traffic mirror target (see AWS docs). This setup gives: High availability (via Auto Scaling group). Scale-out capability. Correct AWS service for mirrored traffic distribution.

dcantos 9 months, 1 week ago

Selected Answer: C

Is C....

matanasov 11 months, 1 week ago

Selected Answer: C

GWLB supports traffic mirroring natively as a target NLB cannot be used as a traffic mirroring target

1a17d1e 6 months, 3 weeks ago

AWS explicitly supports NLBs and Gateway Load Balancer endpoints as valid traffic mirror targets. GWLB requires the -E and its absence from the answer makes A my choice even though GWLB-E is the better option.

Wardove 11 months, 1 week ago

Selected Answer: C

NLB supports mirroring, but not ideal for raw packet processing — lacks L3/L4 transparency.. so even though C does not mention GWLBE, my bet would be on it anyway

RavikantKumarRavi 1 year ago

Selected Answer: A

NLB incase of EC2 and GLB incase of security appliance as destination or target

jyrajan69 1 year, 2 months ago

Selected Answer: C

It depends on when you answered this question because based on the latest the answer is C https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

AzureDP900 1 year, 2 months ago

Selected Answer: A

A is right To create a highly available solution that can scale to handle mirrored traffic while minimizing the impact on the EC2 instance hosting tools for analyzing traffic, we should use a load balancer to distribute the mirrored traffic across multiple instances.

Spaurito 1 year, 4 months ago

C - A listener for Gateway Load Balancers listens for all IP packets across all ports, and then forwards traffic to the target group.

btech24 1 year, 6 months ago

Answer is A, Gateway Load Balancer is not a valid traffic mirror target. There are 3 valid traffic mirror endpoints 1. Network Interface 2. Network Load Balancer 3. Gateway Load Balancer endpoints ref https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

AlirezaNetWorld 1 year, 6 months ago

The right answer is C without any doubts...

kourosh 1 year, 11 months ago

Selected Answer: A

A is the correct answer: https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

Jonalb 1 year, 11 months ago

Selected Answer: A

A is correct!

Raphaello 1 year, 11 months ago

Selected Answer: A

I'd go with A. Valid traffic mirror targets include "GWLB ENDPOINTS"..for this, I'd go with A. Traffic mirror target concepts A traffic mirror target is the destination for mirrored traffic. You can use the following resources as traffic mirror targets: Network interfaces of type interface Network Load Balancers Gateway Load Balancer endpoints <<<< https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

patanjali 2 years ago

Selected Answer: A

GWLB cant be the answer as you will need Firewall behind GWLB which understand GENEVE. Simple and BEst solution is to use NLB with TCP/UDP listner

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #22 Topic 1

A company uses a hybrid architecture and has an AWS Direct Connect connection between its on-premises data center and AWS. The company has production applications that run in the on-premises data center. The company also has production applications that run in a VPC. The applications that run in the on-premises data center need to communicate with the applications that run in the VPC. The company is using corp.example.com as the domain name for the on-premises resources and is using an Amazon Route 53 private hosted zone for aws.example.com to host the VPC resources.
The company is using an open-source recursive DNS resolver in a VPC subnet and is using a DNS resolver in the on-premises data center. The company's on-premises DNS resolver has a forwarder that directs requests for the aws.example.com domain name to the DNS resolver in the VPC. The DNS resolver in the VPC has a forwarder that directs requests for the corp.example.com domain name to the DNS resolver in the on-premises data center. The company has deckled to replace the open-source recursive DNS resolver with Amazon Route 53 Resolver endpoints.
Which combination of steps should a network engineer take to make this replacement? (Choose three.)

A. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the outbound endpoint.

B. Configure the on-premises DNS resolver to forward aws.example.com domain queries to the IP addresses of the inbound endpoint. **Most Voted**

C. Create a Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint. **Most Voted**

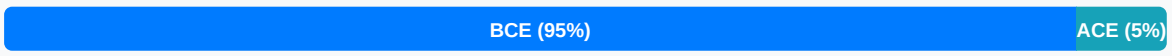
D. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.

E. Create a Route 53 Resolver rule to forward corp.example.com domain queries to the IP address of the on-premises DNS resolver. **Most Voted**

F. Configure the on-premises DNS resolver to forward aws.example.com queries to the IP addresses of the outbound endpoint.

Correct Answer: BCE

Community vote distribution



Comments

albertkr **Highly Voted** 2 years, 4 months ago

BCE is correct

dave777green Highly Voted 2 years, 5 months ago

B,C,E 100%

Raphaello 1 year, 5 months ago

Selected Answer: BCE

BCE are the correct answers. For this scenario we need both resolver inbound and outbound endpoints (C), then a forwarding rule toward on-prem DNS resolver for on-prem sub-domain (corp.example.com) (E), and finally configure on-pre DNS resolver to forward queries to inbound endpoint (B).

vikasj1in 1 year, 7 months ago

Selected Answer: ACE

A. This step is necessary to direct queries for the "aws.example.com" domain from the on-premises DNS resolver to the Route 53 Resolver outbound endpoint. C. The inbound and outbound endpoints allow communication between on-premises and AWS environments. The inbound endpoint is associated with the on-premises DNS resolver, and the outbound endpoint is associated with the DNS resolver in the VPC. E. This step ensures that queries for the "corp.example.com" domain originating from the DNS resolver in the VPC are forwarded to the on-premises DNS resolver. B incorrect because there is no need to configure the on-premises DNS resolver to forward "aws.example.com" domain queries to the IP addresses of the inbound endpoint. D is incorrect because there is no need to create a Route 53 Resolver rule to forward "aws.example.com" domain queries to the IP addresses of the inbound endpoint. F is incorrect

Marfee400704 1 year, 7 months ago

I think that it's correct answer is CDE according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is B & C & E.

AmSpOkE 1 year, 7 months ago

Selected Answer: BCE

No doubts.

Snape 1 year, 8 months ago

Selected Answer: BCE

CEB in THAT order. C: create bidirectional resolver endpoints E: DNS queries from VPC are forwarded to On-prem B: DNS queries from On-prem are forwarded to VPC

Arad 1 year, 11 months ago

Selected Answer: BCE

no doubt BCE.

prajkash 2 years, 2 months ago

BCE is correct

Untamables 2 years, 5 months ago

Selected Answer: BCE

B, C, E https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html

that1guy 2 years, 5 months ago

Selected Answer: BCE

b,c,e is correct

navi7 2 years, 6 months ago

Selected Answer: BCE

BCE is the answer

Cappy46789 2 years, 6 months ago

Selected Answer: BCE

Yip BCE

zaazanuna 2 years, 6 months ago

flowers00 - you are correct. BCE is the go.

study_aws1 2 years, 6 months ago

It is B, C, E

flowers00 2 years, 6 months ago

B,C,E - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #23 Topic 1

A government contractor is designing a multi-account environment with multiple VPCs for a customer. A network security policy requires all traffic between any two VPCs to be transparently inspected by a third-party appliance. The customer wants a solution that features AWS Transit Gateway. The setup must be highly available across multiple Availability Zones, and the solution needs to support automated failover. Furthermore, asymmetric routing is not supported by the inspection appliances.
Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect the inspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the target group. Create a Network Load Balancer (NLB), and set it up to forward to the newly created target group. Configure a default route in the inspection VPCs transit gateway subnet toward the NLB.

B. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect the inspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the target group. Create a Gateway Load Balancer, and set it up to forward to the newly created target group. Configure a default route in the inspection VPC's transit gateway subnet toward the Gateway Load Balancer endpoint. Most Voted

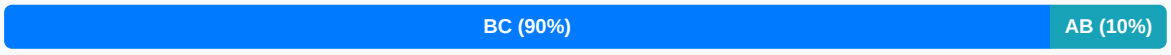
C. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs. Associate the other route table with the inspection VPC's attachment. Propagate all VPC attachments into the inspection route table. Define a static default route in the application route table. Enable appliance mode on the attachment that connects the inspection VPC. Most Voted

D. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs. Associate the other route table with the inspection VPCs attachment. Propagate all VPC attachments into the application route table. Define a static default route in the inspection route table. Enable appliance mode on the attachment that connects the inspection VPC.

E. Configure one route table on the transit gateway. Associate the route table with all the VPCs. Propagate all VPC attachments into the route table. Define a static default route in the route table.

Correct Answer: BC

Community vote distribution



Comments

zaazanuna Highly Voted 3 years ago

correction - BC - correct.

Untamables Highly Voted 2 years, 11 months ago

Selected Answer: BC

B and C https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/introduction.html https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-gwlb-with-tg-for-cns.html

mic8 1 year, 4 months ago

The critical issue with D is that it does not propagate the application VPC attachments into the inspection route table. Without this propagation, the inspection VPC will not know how to route traffic back to the originating application VPCs after it has been inspected.

Raphaello 1 year, 11 months ago

Selected Answer: BC

BC are the correct answers. We need to used GWLB to load-balance the traffic to a target group of inspection appliance. Routes toward Applications VPCs need to be propagated and being reachable through their respective TGW attachment. Enable appliance mode to avoid asymmetric routing due to zone affinity.

patanjali 2 years ago

Selected Answer: BC

When application VPC wants to reach other app VPC via TGW, there should be default route pointed to inspection TGW attchement and when traffic traffic comes back to TGW after inspection/GWLB, TGW needs specific routes to app VPC CIDRs.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is BD according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is B & C.

Arad 2 years, 4 months ago

Selected Answer: BC

Just B & C make sense, the rest are all wrong.

[Removed] 2 years, 8 months ago

Selected Answer: AB

you can create a multi-account environment with multiple VPCs for a customer by using AWS Transit Gateway. A transit gateway enables you to attach VPCs and VPN connections in the same Region and route traffic between them. A transit gateway works across AWS accounts, and you can use AWS RAM to share your transit gateway with other accounts 1. To meet the network security policy that requires all traffic between any two VPCs to be transparently inspected by a third-party appliance, you can deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. You can connect the inspection VPC to the transit gateway by using a VPC attachment. Then create a target group and register the appliances with the target group. After that, you can create a Network Load Balancer (NLB) and set it up to forward to the newly created target group. Finally, configure a default route in the inspection VPCs transit gateway subnet toward the NLB

ShinLi 2 years, 5 months ago

my understanding should be B C, as A is using NLB, and NLB is for EC2 instance. the GWLB is for VPC

prajkash 2 years, 8 months ago

vote for BC

sambb 2 years, 8 months ago

Selected Answer: BC

B - as an GWLB is more appropriate for monitoring appliances C - as D and E would allow the VPCs to communicate together directly,

albertkr 2 years, 10 months ago

vote for BC

bogehad181 2 years, 11 months ago

Selected Answer: BC

B & C, GLB better for 3rd party appliance, TGW RT associated to APP VPCs has a single route to the Inspection VPC and second TGW RT for the inspection VPC has all APP VPC CIDRs propagated to it.

Mandar 2 years, 12 months ago

NLB:To increase the fault tolerance of your applications, you can enable multiple Availability Zones for your load balancer and ensure that each target group has at least one target in each enabled Availability Zone. https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html GLB: Third party appliance https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/#:~:text=Gateway%20Load%20Balancer%20helps%20you,or%20down%2C%20based%20on%20demand. Answers A) B)

that1guy 2 years, 12 months ago

Selected Answer: BC

B and C

titi_r 2 years, 12 months ago

Selected Answer: BC

B and C.

flowers00 3 years ago

B,C - correct.

https://zhangxuetu.online

[202610]

Question #24 Topic 1

A company has deployed Amazon EC2 instances in private subnets in a VPC. The EC2 instances must initiate any requests that leave the VPC, including requests to the company's on-premises data center over an AWS Direct Connect connection. No resources outside the VPC can be allowed to open communications directly to the EC2 instances.
The on-premises data center's customer gateway is configured with a stateful firewall device that filters for incoming and outgoing requests to and from multiple VPCs. In addition, the company wants to use a single IP match rule to allow all the communications from the EC2 instances to its data center from a single IP address.
Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Create a VPN connection over the Direct Connect connection by using the on-premises firewall. Use the firewall to block all traffic from on premises to AWS. Allow a stateful connection from the EC2 instances to initiate the requests.

B. Configure the on-premises firewall to filter all requests from the on-premises network to the EC2 instances. Allow a stateful connection if the EC2 instances in the VPC initiate the traffic.

C. Deploy a NAT gateway into a private subnet in the VPC where the EC2 instances are deployed. Specify the NAT gateway type as private. Configure the on-premises firewall to allow connections from the IP address that is assigned to the NAT gateway. **Most Voted**

D. Deploy a NAT instance into a private subnet in the VPC where the EC2 instances are deployed. Configure the on-premises firewall to allow connections from the IP address that is assigned to the NAT instance.

Correct Answer: C

Community vote distribution



Comments

Cappy46789 **Highly Voted** 2 years, 6 months ago

Selected Answer: C

C - you need a NAT https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

RavikantKumarRavi 1 year, 2 months ago

Selected Answer: D

NAT Gateway never host inside Private subnet

Raphaello 1 year, 5 months ago

Selected Answer: C

Correct answer is C, private NAT Gw.

Marfee400704 1 year, 7 months ago

I think that it'sanswer is C according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is C.

Arad 1 year, 11 months ago

Selected Answer: C

Definitely C.

habros 1 year, 11 months ago

Selected Answer: C

It is C. Why? NAT Gateway is managed, hence it is LEAST operational effort. Not D. Why? NAT Instance is self-managed, self-patched.

Mandar 2 years, 5 months ago

Answer C) https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/private-nat-gateway.html

ITgeek 2 years, 5 months ago

Selected Answer: C

C is correct as a NAT gateway is already a service vs a NAT instance is just another EC2 with more overhead

awsguru1998 2 years, 5 months ago

D is the correct answer because it suggests deploying a NAT instance in a private subnet. The NAT instance can then be used to allow outbound traffic from the EC2 instances in the private subnet to the on-premises data center, while also blocking all incoming traffic from the data center to the EC2 instances.

flowers00 2 years, 6 months ago

C - correct.

zaazanuna 2 years, 6 months ago

B - correct. The solution that meets the requirements with the LEAST amount of operational overhead is option B: Configure the on-premises firewall to filter all requests from the on-premises network to the EC2 instances. Allow a stateful connection if the EC2 instances in the VPC initiate the traffic.

Cappy46789 2 years, 6 months ago

The EC2 insrance need to use the same IP when they hit onpremise, which means you need a NAT so C is correct

https://zhangxuetu.online

[202610]

Question #25 Topic 1

A global company operates all its non-production environments out of three AWS Regions: eu-west-1, us-east-1, and us-west-1. The company hosts all its production workloads in two on-premises data centers. The company has 60 AWS accounts and each account has two VPCs in each Region. Each VPC has a virtual private gateway where two VPN connections terminate for resilient connectivity to the data centers. The company has 360 VPN tunnels to each data center, resulting in high management overhead. The total VPN throughput for each Region is 500 Mbps.

The company wants to migrate the production environments to AWS. The company needs a solution that will simplify the network architecture and allow for future growth. The production environments will generate an additional 2 Gbps of traffic per Region back to the data centers. This traffic will increase over time.

Which solution will meet these requirements?

A. Set up an AWS Direct Connect connection from each data center to AWS in each Region. Create and attach private VIFs to a single Direct Connect gateway. Attach the Direct Connect gateway to all the VPCs. Remove the existing VPN connections that are attached directly to the virtual private gateways.

B. Create a single transit gateway with VPN connections from each data center. Share the transit gateway with each account by using AWS Resource Access Manager (AWS RAM). Attach the transit gateway to each VPC. Remove the existing VPN connections that are attached directly to the virtual private gateways.

C. Create a transit gateway in each Region with multiple newly commissioned VPN connections from each data center. Share the transit gateways with each account by using AWS Resource Access Manager (AWS RAM). In each Region, attach the transit gateway to each VPRemove the existing VPN connections that are attached directly to the virtual private gateways. Most Voted

D. Peer all the VPCs in each Region to a new VPC in each Region that will function as a centralized transit VPC. Create new VPN connections from each data center to the transit VPCs. Terminate the original VPN connections that are attached to all the original VPCs. Retain the new VPN connection to the new transit VPC in each Region.

Correct Answer: C

Community vote distribution

C (88%) B (13%)

Comments

study_aws1 Highly Voted 3 years ago

Option A) may be a stable solution considering other options, but will not be applicable to this scenario as a single Direct connect gateway can connect only upto 10 VPCs, where as the requirement states total 120 VPCs. This choice

would have been applicable had Transit Gateway been introduced to the architecture with Transit VIF (not private VIF). As Transit gateway is a regional resource, a single transit gateway will not function cross-region. Hence, option C)

zaazanuna 2 years, 12 months ago

Option C would involve creating a transit gateway in each region with multiple newly commissioned VPN connections from each data center, which would result in a high number of VPN tunnels. While AWS Transit Gateway is designed to handle multiple VPN connections, creating a separate transit gateway in each region would not be a scalable solution in the long term. Additionally, each AWS account has two VPCs in each region, so attaching a transit gateway to each VPC would result in a large number of VPC attachments, which would be difficult to manage. wrong?

albertkr 2 years, 10 months ago

How do you address 1 DX GW max 10 VPC connections limitation if you still insist A is the correct answer?

notwhoyouthink 2 years, 10 months ago

The question states there are 60 accounts with 2 vpc's per region. Answer A says 1 DX connection per account, so A would still be the answer.

Neo00 2 years, 8 months ago

It doesn't say 1 DX per account neither in the question nor answer A

Untamables Highly Voted 2 years, 11 months ago

Selected Answer: C

C An AWS Transit Gateway provides the option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet. A Transit Gateway is a regional resource. https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html You can use AWS Resource Access Manager (RAM) to share a transit gateway for VPC attachments across accounts or across your organization in AWS Organizations. That helps reducing the VPN connections. https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-share.html AWS Transit Gateway can scale up to 50 Gbps throughput aggregating multiple VPN tunnels. https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-quotas.html#bandwidth-quotas

clphan 1 year, 7 months ago

A/ but https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html mention VPGs (VPCs) per DX GW is 20. The company have 120 VPCs spread across 3 region (40 per region) > 20 ... B/ TGW is regional. C/ cost for maintainance (manage tgw routing) but it's work. D/ Transitive routing is not available VPC peering (On-premise - AWS).

Raphaello 1 year, 11 months ago

Selected Answer: C

There are 120 VPC's in each region. That being said, option A where a single Direct Connect gateway connect to all the VPCs via private VIF's (adnd VGW of course)..simply does not work. DxGW can only connect to 20 Virtual private gateways per AWS Direct Connect gateway. https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html Had it had TGW connected to DxGW, it would've been the best choice in terms of sufficient bandwidth. C is the answer.

vikasj1in 2 years, 1 month ago

Selected Answer: B

Simplifying Network Architecture: By using a single transit gateway, the company can centralize its VPN connections, reducing the complexity associated with managing multiple VPN tunnels directly attached to each VPC. Resilient Connectivity: The transit gateway can provide a more scalable and resilient solution for connectivity between AWS

and the on-premises data centers. Sharing Resources with AWS RAM: Using AWS Resource Access Manager (AWS RAM) to share the transit gateway across accounts helps in maintaining a centralized and standardized architecture. Scalability: The transit gateway can handle the additional 2 Gbps of traffic per region and is designed to scale as traffic increases over time. This solution offers a more centralized and scalable approach, reducing management overhead and providing the flexibility needed for future growth.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C accoring to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

sadovenk0 2 years, 4 months ago

I agree that A can't be used, because we have quotes - 20 VGW per 1 DX Gateway https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html but how we can handle the requirement of 2 Gbps output from aws to on-premise while we have throughput 500 Mbps (AWS VPN connectivity isn't very scalable since VPN tunnels are limited to a maximum bandwidth of 1.25 Gbps)?

seochan 1 year, 10 months ago

You can scale bandwidth up to 50Gbps using TGW thanks to the ECMP. https://aws.amazon.com/en/blogs/networking-and-content-delivery/scaling-vpn-throughput-using-aws-transit-gateway/

Simili 2 years, 6 months ago

Transit gateway is a regional resource, therefore a single transit gateway can not work. Option C is the correct choice

DeathFrmAbv 2 years, 8 months ago

While C is correct, D is also possible. In D the bandwidth will depend on the EC2 instance type you are choosing to run your VPN software

evargasbrz 2 years, 7 months ago

I think D is not possible, as it says "Peer all the VPCs in each Region to a new VPC in each Region that will function as a centralized transit VPC.", so you have this limitation: "If VPC A has a VPN connection to a corporate network, resources in VPC B can't use the VPN connection to communicate with the corporate network." You can see all the limitations here: https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-basics.html#vpc-peering-limitations

linuxek21 2 years, 11 months ago

Correct answer is C, B - calls for a single TGW but you cannot directly connect VPC from another region, you must have peering connection between TGWs

ITgeek 2 years, 12 months ago

Selected Answer: B

Is the simplest

Spaurito 1 year, 4 months ago

You have to have TGW per region, can't do with a single TGW.

titi_r 2 years, 12 months ago

Selected Answer: C

C - correct.

zaazanuna 3 years ago

Correction - A - correct.

titi_r 2 years, 12 months ago

The limit for VGWs per DX gateway is 10 and cannot be increased. https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html Obviously, you cannot attach 120 VPCs to it, so A is wrong. Answer C is correct.

flowers00 3 years ago

A or C ?

flowers00 3 years ago

C: I think

zaazanuna 3 years ago

B - correct

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #26 Topic 1

A company is building its website on AWS in a single VPC. The VPC has public subnets and private subnets in two Availability Zones. The website has static content such as images. The company is using Amazon S3 to store the content.
The company has deployed a fleet of Amazon EC2 instances as web servers in a private subnet. The EC2 instances are in an Auto Scaling group behind an Application Load Balancer. The EC2 instances will serve traffic, and they must pull content from an S3 bucket to render the webpages. The company is using AWS Direct Connect with a public VIF for on-premises connectivity to the S3 bucket.
A network engineer notices that traffic between the EC2 instances and Amazon S3 is routing through a NAT gateway. As traffic increases, the company's costs are increasing. The network engineer needs to change the connectivity to reduce the NAT gateway costs that result from the traffic between the EC2 instances and Amazon S3.
Which solution will meet these requirements?

A. Create a Direct Connect private VIF. Migrate the traffic from the public VIF to the private VIF.

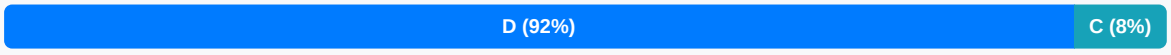
B. Create an AWS Site-to-Site VPN tunnel over the existing public VIF.

C. Implement interface VPC endpoints for Amazon S3. Update the VPC route table.

D. Implement gateway VPC endpoints for Amazon S3. Update the VPC route table. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

navi7 **Highly Voted** 2 years, 6 months ago

I think it should be D https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/ Determine whether the majority of your NAT gateway charges are from traffic to Amazon Simple Storage Service or Amazon DynamoDB in the same Region. If they are, then set up a gateway VPC endpoint. Route traffic to and from the AWS resource through the gateway VPC endpoint, rather than through the NAT gateway. There's no processing or hourly charges for using gateway VPC endpoints.

zaazanuna **Highly Voted** 2 years, 6 months ago

Correction - D - correct.

tushar321 10 months ago

Selected Answer: C

Key is The company is using AWS Direct Connect with a public VIF for on-premises connectivity to the S3 bucket.On premises access can be given by only interface endpoints

seochan 1 year, 3 months ago

C is not possible because you have to use the endpoint IP to connect to S3 if you are using VPC interface endpoint(PrivateLink). It cannot be configured by updating the VPC route table.

Raphaello 1 year, 5 months ago

Selected Answer: D

VPC Gateway endpoint to keep traffic for S3 within AWS backbone network. D is the correct answer.

Marfee400704 1 year, 7 months ago

I thin that it's correct answer is D according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is D.

dishu2511 1 year, 9 months ago

I think it is C and not D. Because, with S3 Gateway you are still using NAT GW yes it is cheaper than VPC endpoint. But the question specifically asks to reduce the cost of NAT GW. VPC endpoint provides a private IP, thus, the traffic between EC2 and S3 can be served without the NAT GW.

Arad 1 year, 11 months ago

Selected Answer: D

Definitely D.

habros 1 year, 11 months ago

Selected Answer: D

D. EC2 can call gateway endpoints, without the need for ENIs (interface) based endpoints. INterface endpoints cost $ by the hour and traffic charges. Gateway is free (s3/dynamodb)

alextl 2 years, 3 months ago

Selected Answer: D

Both C and D could reduce NAT Gateway cost, but D gateway endpoint no cost, C interface endpoint was priced at $0.01/per AZ/per hour , the cost depends on region. so D is better than C.
https://aws.amazon.com/cn/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

Untamables 2 years, 5 months ago

Selected Answer: D

D To reduce data transfer charges for NAT gateways, you can use an interface endpoint or a gateway endpoint. https://repost.aws/knowledge-center/vpc-reduce-nat-gateway-transfer-costs If your NAT gateway charges are from traffic to Amazon S3 or Amazon DynamoDB in the same Region, you should choose a gateway endpoint. There is no additional charge for using gateway endpoints. On the other hand, An interface endpoint charges apply for each Gigabyte processed through the endpoint. https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html https://aws.amazon.com/privatelink/pricing/

linuxek21 2 years, 5 months ago

Correct Answer is D, As per documentation: Amazon S3 supports both gateway endpoints and interface endpoints. With a gateway endpoint, you can access Amazon S3 from your VPC, without requiring an internet gateway or NAT device for your VPC, and with no additional cost. However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use

an interface endpoint, which is available for an additional cost.
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html For those concerned about on-prem, this is not an issue when you use a public VIF

ITgeek 2 years, 5 months ago

Selected Answer: D

correct answer to this question is D. Implement gateway VPC endpoints for Amazon S3 and update the VPC route table. This solution will allow the EC2 instances to access the S3 bucket directly without having to go through a NAT gateway, reducing costs. Additionally, gateway endpoints provide greater scalability and performance than interface endpoints, making them the preferred solution for high-traffic use cases such as this one.

ILOVEVODKA 2 years, 5 months ago

C is correct. Read carefully to get why: https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html

slackbot 2 years, 5 months ago

you need to read carefully, gateway endpoint is cheaper (you pay for traffic via interface endpoint, while traffic over gateway endpoint is free)

flowers00 2 years, 6 months ago

D - correct.

zaazanuna 2 years, 6 months ago

C - correct. Option D, implementing gateway VPC endpoints for Amazon S3 and updating the VPC route table, would not meet the requirements. Gateway endpoints allow communication with S3 via the S3 APIs and are intended for accessing S3 over the Internet Gateway or Virtual Private Gateway. They do not help reduce the NAT gateway costs or provide a cost-effective solution for the company's requirements.

smyndlo 2 years, 5 months ago

Interface endpoints do not require route table configuration, so option C is wrong on that aspect. Also, gateway endpoints have zero costs associated with them, while interface endpoints incur charges

ILOVEVODKA 2 years, 5 months ago

look: However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint, which is available for an additional cost

smyndlo 2 years, 5 months ago

Quoting the question "reduce the NAT gateway costs that result from the traffic between the EC2 instances and Amazon S3." The point of concern is between EC2 instances and s3, not on-prem...besides, the question does state that there is a public vif that is used by on-prem nodes

https://zhangxuetu.online

[202610]

Question #27 Topic 1

A company wants to improve visibility into its AWS environment. The AWS environment consists of multiple VPCs that are connected to a transit gateway. The transit gateway connects to an on-premises data center through an AWS Direct Connect gateway and a pair of redundant Direct Connect connections that use transit VIFs. The company must receive notification each time a new route is advertised to AWS from on premises over Direct Connect.
What should a network engineer do to meet these requirements?

A. Enable Amazon CloudWatch metrics on Direct Connect to track the received routes. Configure a CloudWatch alarm to send notifications when routes change.

B. Onboard Transit Gateway Network Manager to Amazon CloudWatch Logs Insights. Use Amazon EventBridge (Amazon CloudWatch Events) to send notifications when routes change. Most Voted

C. Configure an AWS Lambda function to periodically check the routes on the Direct Connect gateway and to send notifications when routes change.

D. Enable Amazon CloudWatch Logs on the transit VIFs to track the received routes. Create a metric filter Set an alarm on the filter to send notifications when routes change.

Correct Answer: B

Community vote distribution

B (100%)

Comments

zaazanuna Highly Voted 2 years, 6 months ago

B - correct Transit Gateway Network Manager provides a centralized view of global networks built on AWS Transit Gateway. It also provides the capability to monitor the routing tables associated with the transit gateway, and then forward routing information to CloudWatch Logs Insights. Once in CloudWatch Logs Insights, you can use EventBridge rules to trigger notifications based on routing changes. This will allow the company to receive notifications each time a new route is advertised to AWS from on-premises over Direct Connect, which meets the requirements. The other options either do not provide the necessary functionality or would not be the most efficient solution for this scenario.

slackbot Highly Voted 2 years, 5 months ago

Selected Answer: B

it is B - tested and confirmed. the problem is - if a static route exists and the same prefix gets advertised - it will not be flagged and no Event will trigger.

cerifyme85 1 year, 5 months ago

Selected Answer: B

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-monitoring.html#:~:text=CloudWatch%20Events%20using%20Network%20Manager

Marfee400704 1 year, 7 months ago

I think that it's correct answer is B according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is B.

Untamables 2 years, 5 months ago

Selected Answer: B

B https://docs.aws.amazon.com/network-manager/latest/cloudwan/cloudwan-visualize-tgw.html https://docs.aws.amazon.com/network-manager/latest/cloudwan/cloudwan-cloudwatch-events.html

helloworldabc 2 years, 6 months ago

BBBBBBBBB

study_aws1 2 years, 6 months ago

Should be B) Please refer below link - https://docs.aws.amazon.com/network-manager/latest/cloudwan/cloudwan-cloudwatch-events.html

flowers00 2 years, 6 months ago

B - correct.

https://zhangxuetu.online

[202610]

Question #28 Topic 1

A software company offers a software-as-a-service (SaaS) accounting application that is hosted in the AWS Cloud The application requires connectivity to the company's on-premises network. The company has two redundant 10 GB AWS Direct Connect connections between AWS and its on-premises network to accommodate the growing demand for the application.
The company already has encryption between its on-premises network and the colocation. The company needs to encrypt traffic between AWS and the edge routers in the colocation within the next few months. The company must maintain its current bandwidth.
What should a network engineer do to meet these requirements with the LEAST operational overhead?

A. Deploy a new public VIF with encryption on the existing Direct Connect connections. Reroute traffic through the new public VIF.

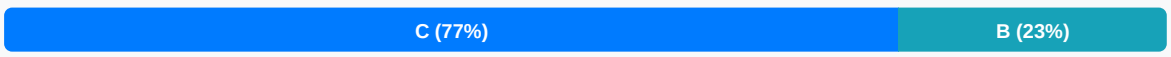
B. Create a virtual private gateway Deploy new AWS Site-to-Site VPN connections from on premises to the virtual private gateway Reroute traffic from the Direct Connect private VIF to the new VPNs.

C. Deploy a new pair of 10 GB Direct Connect connections with MACsec. Configure MACsec on the edge routers. Reroute traffic to the new Direct Connect connections. Decommission the original Direct Connect connections **Most Voted**

D. Deploy a new pair of 10 GB Direct Connect connections with MACsec. Deploy a new public VIF on the new Direct Connect connections. Deploy two AWS Site-to-Site VPN connections on top of the new public VIF. Reroute traffic from the existing private VIF to the new Site-to-Site connections. Decommission the original Direct Connect connections.

Correct Answer: C

Community vote distribution



Comments

linuxek21 **Highly Voted** 2 years, 11 months ago

Correct answer is C, B - you need a public VIF for VPN to VGW, only TGW VPNs can be used with a private VIF. Also, they are supposed to maintain current bandwidth. VPN limits their connection to 1.25Gbps Additional Notes: I am not a big fan of answer C as it assumes the edge router supports macsec.

kaush4u 2 years, 8 months ago

MacSec does not encrypt AWS to colocation ,hence B

Josh1217 2 years, 8 months ago

Site-to-Site VPN will not satisfy 'Maintain current Bandwidth'. Hence B is incorrect.

A_A_AB 2 years, 8 months ago

You mean C, right? B talks about VPC which doesn't satisfy the bandwidth requirement.

Akshay0403 1 year, 8 months ago

We are talking about LEAST operational overhead so we cannot use Site to Site VPN here.

Joselito79 2 months, 2 weeks ago

Selected Answer: C

Option C is the only one that: Meets the required encryption requirements Maintains full bandwidth Minimizes changes and complexity Follows AWS best practices for Direct Connect

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. MACSec is a L2 encryption, and best solution to maintain the current bandwidth.

tromyunpak 2 years ago

C is the correct answer due you need new DX connections to enable macsec. with macsec you will have throughput required A is wrong since you have cannot public vif with encryption D is wrong since it doesn't make sense to have macsec and ipsec also IPSEC throughput is 1.25Gb/s not 10Gb/s B is wrong due to the throughput is limited by the VPNs and with VPG ecmp is not supported unlike TGW

vikasj1in 2 years, 1 month ago

Selected Answer: C

MACsec (Media Access Control Security) is a standard for securing Ethernet connections at the link layer. It provides encryption for data traffic between the AWS Direct Connect routers and the edge routers in the colocation facility. In this scenario, deploying a new pair of 10 GB Direct Connect connections with MACsec provides encryption for the traffic between AWS and the colocation without changing the existing bandwidth. Configuring MACsec on the edge routers ensures that the traffic is encrypted over the new Direct Connect connections. Option C is the most appropriate solution as it introduces MACsec on dedicated high-speed Direct Connect connections, ensuring security without the need for additional VPNs or significant operational overhead.

vikasj1in 2 years, 1 month ago

Assuming the edge router supports MACsec (which is not mentioned in the question clearly).

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is B.

habros 2 years, 5 months ago

Selected Answer: C

C. Two pairs of DX is solid enough, S2SVPN adds even more redundancy, at 1.25Gbps max per line (way lesser than 10Gbps needed)

Mishranihal737 2 years, 7 months ago

C is correct, VPN connection will limit the BW to 1.25 GBps

Cheam 2 years, 7 months ago

Selected Answer: C

Another tricky question. 1) You cannot create a VPN tunnel via Private VIFs 2) The company must maintain its current bandwidth. VPN tunnels max throughput is up to 1.25Gbps. Answer is C All the best.

Certified101 2 years, 8 months ago

Selected Answer: C

C is correct

sen460 2 years, 8 months ago

Correct Answer is C - Refer to extracted piece of text from the link shared - "You can use AWS Direct Connect connections that support MACsec to encrypt your data from your on-premises network or collocated device to your chosen AWS Direct Connect point of presence". Link for Reference - https://aws.amazon.com/directconnect/faqs/

Untamables 2 years, 11 months ago

Selected Answer: C

C https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html

ITgeek 2 years, 12 months ago

Selected Answer: B

This option suggests creating a virtual private gateway and deploying new AWS Site-to-Site VPN connections from on premises to the virtual private gateway. Then, rerouting traffic from the Direct Connect private VIF to the new VPNs. This option requires less operational overhead than option A because it does not require creating a new VIF, but it does require BBB configuring a new VPN connection. This option would also meet the requirement of maintaining the current bandwidth. Please explain your answer of why C?

zaazanuna 2 years, 11 months ago

Q: What throughput can I get with Private IP VPN? A: Just like regular Site-to-site VPN connections, each private IP VPN connection supports 1.25Gbps of bandwidth. You can use ECMP (Equal Cost Multi-path) across multiple private IP VPN connections to increase effective bandwidth. As an example, to send 10Gbps of DX traffic over a private IP VPN, you can use 4 private IP VPN connections (4 connections x 2 tunnels x 1.25Gbps bandwidth) with ECMP between a pair of Transit gateway and Customer gateway.

albertkr 2 years, 10 months ago

B only says create "a" VPN tunnel, which means the max bw is only 1.25Gbps

flowers00 3 years ago

C - correct.

ITgeek 2 years, 12 months ago

why do you think deploying new direct connection would be easier, given the time constrain ? the connection are already in place

zaazanuna 3 years ago

C - correct.

https://zhangxuetu.online

[202610]

Question #29 Topic 1

A company hosts an application on Amazon EC2 instances behind an Application Load Balancer (ALB). The company recently experienced a network security breach. A network engineer must collect and analyze logs that include the client IP address, target IP address, target port, and user agent of each user that accesses the application.
What is the MOST operationally efficient solution that meets these requirements?

A. Configure the ALB to store logs in an Amazon S3 bucket. Download the files from Amazon S3, and use a spreadsheet application to analyze the logs.

B. Configure the ALB to push logs to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Analytics to analyze the logs.

C. Configure Amazon Kinesis Data Streams to stream data from the ALB to Amazon OpenSearch Service (Amazon Elasticsearch Service). Use search operations in Amazon OpenSearch Service (Amazon Elasticsearch Service) to analyze the data.

D. Configure the ALB to store logs in an Amazon S3 bucket. Use Amazon Athena to analyze the logs in Amazon S3. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

WMF0187 **Highly Voted** 2 years ago

I originally picked C but after CAREFUL reading I see D is the answer as the keyword for me was "experienced" which means past (historical) data which AWS Athena queries vs Kinesis that does real-time

Raphaello 1 year, 5 months ago

Selected Answer: D

D is the correct answer.

marfee 1 year, 7 months ago

I think that it's correcty answer is D.

habros 1 year, 11 months ago

Selected Answer: D

D. Deposit the logs in an S3 destination, and use Athena to partition on the go when needed.

Untamables 2 years, 5 months ago

Selected Answer: D

D https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html
https://repost.aws/knowledge-center/athena-analyze-access-logs

helloworldabc 2 years, 6 months ago

DDDDDD

study_aws1 2 years, 6 months ago

Yes its D)

zaazanuna 2 years, 6 months ago

D - correct.

flowers00 2 years, 6 months ago

D - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #30 Topic 1

A media company is implementing a news website for a global audience. The website uses Amazon CloudFront as its content delivery network. The backend runs on Amazon EC2 Windows instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The company's customers access the website by using service example com as the CloudFront custom domain name. The CloudFront origin points to an ALB that uses service-alb.example.com as the domain name.
The company's security policy requires the traffic to be encrypted in transit at all times between the users and the backend.
Which combination of changes must the company make to meet this security requirement? (Choose three.)

A. Create a self-signed certificate for service.example.com. Import the certificate into AWS Certificate Manager (ACM). Configure CloudFront to use this imported SSL/TLS certificate. Change the default behavior to redirect HTTP to HTTPS.

B. Create a certificate for service.example.com by using AWS Certificate Manager (ACM). Configure CloudFront to use this custom SSL/TLS certificate. Change the default behavior to redirect HTTP to HTTPS. Most Voted

C. Create a certificate with any domain name by using AWS Certificate Manager (ACM) for the EC2 instances. Configure the backend to use this certificate for its HTTPS listener. Specify the instance target type during the creation of a new target group that uses the HTTPS protocol for its targets. Attach the existing Auto Scaling group to this new target group.

D. Create a public certificate from a third-party certificate provider with any domain name for the EC2 instances. Configure the backend to use this certificate for its HTTPS listener. Specify the instance target type during the creation of a new target group that uses the HTTPS protocol for its targets. Attach the existing Auto Scaling group to this new target group. Most Voted

E. Create a certificate for service-alb.example.com by using AWS Certificate Manager (ACM). On the ALB add a new HTTPS listener that uses the new target group and the service-alb.example.com ACM certificate. Modify the CloudFront origin to use the HTTPS protocol only. Delete the HTTP listener on the ALB. Most Voted

F. Create a self-signed certificate for service-alb.example.com. Import the certificate into AWS Certificate Manager (ACM). On the ALB add a new HTTPS listener that uses the new target group and the imported service-alb.example.com ACM certificate. Modify the CloudFront origin to use the HTTPS protocol only. Delete the HTTP listener on the ALB.

Correct Answer: BDE

Community vote distribution



Comments

study_aws1 Highly Voted 2 years, 6 months ago

Yes it is B, D, E. C is not correct as - Public ACM certificates can be installed on Amazon EC2 instances that are connected to a Nitro Enclave, but not to other Amazon EC2 instances. The question does not mention any use of Nitro enclave here

Untamables Highly Voted 2 years, 5 months ago

Selected Answer: BDE

B, D, E ACM removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates. https://aws.amazon.com/certificate-manager/ https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html You can configure one or more cache behaviors in your CloudFront distribution to require HTTPS for communication between viewers and CloudFront. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html Option C is wrong. You cannot associate ACM certificates with an EC2 instance that is not connected to a Nitro Enclave. https://docs.aws.amazon.com/acm/latest/userguide/acm-services.html

168cd9d 12 months ago

Selected Answer: BDE

Cloudfront doesn't work with self-signed certs. ALB needs a cert provided by ACM. ACM is not supported on EC2 or either 3rd party or self signed cert can be used.

Raphaello 1 year, 5 months ago

Selected Answer: BCE

BCE are the correct answers. ACM-issued PUBLIC certs cannot be installed on EC2 instances.

Raphaello 1 year, 5 months ago

BDE are the correct answers. My mistake. ACM-issued PUBLIC certs cannot be installed on EC2 instances. That makes D a correct answer..not C.

Marfee400704 1 year, 7 months ago

I think that it's correcty answer is ABD according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is B & D & E.

WMF0187 2 years ago

C is incorrect because if you need to secure communication between users and EC2 instances, you would typically use SSL/TLS certificates at the load balancer level (e.g., Application Load Balancer or Network Load Balancer) or terminate SSL/TLS at the web server running on the EC2 instance itself.

Mishranihal737 2 years, 1 month ago

Yes Correct ans is B,D,E. A-> Incorrect as self signed certs are not supported for Cloud Front C-> Incorrect as ACM doesnot support Certificate export, ACM is not supported on EC2 F-> Incorrect as self signed certs are not supported for Cloud Front.

ITgeek 2 years, 5 months ago

Selected Answer: BDE

by eliminating the self signed answers BDE

jdsingh 2 years, 6 months ago

Selected Answer: BDE

BDE correct

helloworldabc 2 years, 6 months ago

BDE correct

flowers00 2 years, 6 months ago

B,D,E - correct.

zaazanuna 2 years, 6 months ago

B, E, F - correct.

https://zhangxuetu.online

[202610]

Question #31 Topic 1

A company is hosting an application on Amazon EC2 instances behind a Network Load Balancer (NLB). A solutions architect added EC2 instances in a second Availability Zone to improve the availability of the application. The solutions architect added the instances to the NLB target group.
The company's operations team notices that traffic is being routed only to the instances in the first Availability Zone.
What is the MOST operationally efficient solution to resolve this issue?

A. Enable the new Availability Zone on the NLB **Most Voted**

B. Create a new NLB for the instances in the second Availability Zone

C. Enable proxy protocol on the NLB

D. Create a new target group with the instances in both Availability Zones

Correct Answer: A

Community vote distribution

A (100%)

Comments

Untamables **Highly Voted** 2 years, 5 months ago

Selected Answer: A

A https://docs.aws.amazon.com/elasticloadbalancing/latest/network/network-load-balancers.html#availability-zones

steli0 6 months, 1 week ago

Selected Answer: A

Right documentation reference is here https://docs.aws.amazon.com/elasticloadbalancing/latest/network/network-load-balancers.html#cross-zone-load-balancing

Raphaello 1 year, 5 months ago

Selected Answer: A

A is the correct answer, Need to enable new AZ into NLB.

vikasj1in 1 year, 7 months ago

Selected Answer: A

The Network Load Balancer (NLB) needs to be configured to recognize and utilize the new Availability Zone. By enabling the new Availability Zone on the NLB, the load balancer will start distributing traffic to instances in both Availability Zones, providing improved availability and load balancing. Option B suggests creating a new NLB, which is not necessary in this scenario. NLBs are designed to distribute traffic across instances in multiple Availability Zones, and adding the new Availability Zone to the existing NLB is the appropriate step. Options C and D are not directly

addressing the issue. Enabling proxy protocol (Option C) is useful for passing client information to the backend servers, but it doesn't resolve the issue of traffic not being routed to instances in the second Availability Zone. Creating a new target group (Option D) might be necessary for specific use cases, but it doesn't directly address the problem in this context.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is A according to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is A.

Arad 1 year, 11 months ago

Selected Answer: A

for sure A.

sen460 2 years, 2 months ago

Correct Answer is - A. Please refer to the extracted text from the link shared - "You can't disable Availability Zones for a Network Load Balancer after you create it, but you can enable additional Availability Zones." Reference Link - https://docs.aws.amazon.com/elasticloadbalancing/latest/network/network-load-balancers.html#availability-zones

helloworldabc 2 years, 6 months ago

AAAAAAAAAA

flowers00 2 years, 6 months ago

A - correct.

zaazanuna 2 years, 6 months ago

A - correct

https://zhangxuetu.online

[202610]

Question #32 Topic 1

A network engineer needs to set up an Amazon EC2 Auto Scaling group to run a Linux-based network appliance in a highly available architecture. The network engineer is configuring the new launch template for the Auto Scaling group.
In addition to the primary network interface the network appliance requires a second network interface that will be used exclusively by the application to exchange traffic with hosts over the internet. The company has set up a Bring Your Own IP (BYOIP) pool that includes an Elastic IP address that should be used as the public IP address for the second network interface.
How can the network engineer implement the required architecture?

A. Configure the two network interfaces in the launch template. Define the primary network interface to be created in one of the private subnets. For the second network interface, select one of the public subnets. Choose the BYOIP pool ID as the source of public IP addresses.

B. Configure the primary network interface in a private subnet in the launch template. Use the user data option to run a cloud-init script after boot to attach the second network interface from a subnet with auto-assign public IP addressing enabled.

C. Create an AWS Lambda function to run as a lifecycle hook of the Auto Scaling group when an instance is launching. In the Lambda function, assign a network interface to an AWS Global Accelerator endpoint.

D. During creation of the Auto Scaling group, select subnets for the primary network interface. Use the user data option to run a cloud-init script to allocate a second network interface and to associate an Elastic IP address from the BYOIP pool. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

rhinozD **Highly Voted** 2 years, 11 months ago

A is incorrect. EC2 Auto Scaling supports attaching a second elastic network interface automatically when Auto Scaling spins up a new instance. However, both elastic network interfaces attached to the instance are in the same subnet. So you can: 1. Combine Lambda + Lifecycle hook + eventbridge to assign the second elastic network interface 2. or use cloud-init. -> D is correct.

vikasj1in 2 years, 1 month ago

Selected Answer: D

During the creation of the Auto Scaling group, you can select the subnets for the primary network interface. Using user data, you can run a cloud-init script to allocate and configure the second network interface during the instance launch process. The cloud-init script can also handle the association of an Elastic IP address from the BYOIP pool to the second network interface. This approach ensures that each instance launched by the Auto Scaling group has the necessary network configuration, including the second network interface with a public IP address from the BYOIP pool.

MBO92 1 year, 8 months ago

Have you any official documentation that say that is not possible to use launch template in these question uses case?

Marfee400704 2 years, 1 month ago

I think that it' correct answer is D accoring to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is D.

i4papa 2 years, 2 months ago

Selected Answer: A

A is incorrect

MBO92 1 year, 8 months ago

Based on which condition you eliminated the answer A?

CertNerd1234 2 years, 7 months ago

Reason why not option A: it is not possible to choose BYOIP when creating launch template

MBO92 1 year, 8 months ago

Have you any documentation say this statement that we can not assign BYOIP with launch template? in the launch template we can manually enter the IP while provisioning the different ENIs there is no restriction !

tycho 2 years, 8 months ago

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/best-practices-for-configuring-network-interfaces.html

Tofu13 2 years, 9 months ago

Selected Answer: D

RhinozD answer with links https://aws.amazon.com/about-aws/whats-new/2020/11/amazon-ec2-auto-scaling-supports-attaching-multiple-network-interfaces-at-launch/ https://repost.aws/knowledge-center/ec2-auto-scaling-multiple-network-interfaces

MBO92 1 year, 8 months ago

In the first link you provided said : Previously, customers had to write custom scripts and run lifecycle hooks to attach multiple network interfaces. You can now define multiple network interfaces in a launch template and your Auto Scaling group will automatically attach them to instances as they launch. So answer A is valid. There is no such information in both link said that we cannot use BYOIP inside the Launch template !!

YEBINNNNN 2 years, 10 months ago

Selected Answer: D

AAAAAAAA

dman 2 years, 11 months ago

A, not D because ASG with multiple network interfaces, it cannot auto assign Public IPV4 address.

ohcan 2 years, 11 months ago

I think both A and D are correct, but A is easier and more efficient

ohcan 2 years, 11 months ago

sorry. I change to D

navi7 3 years ago

why is A incorrect?

slackbot 2 years, 11 months ago

there does not seem to be a way to select the BYOIP pool in the template

helloworldabc 3 years ago

DDDDDDDD

study_aws1 3 years ago

A - correct

study_aws1 2 years, 12 months ago

Justification for A) - Launch templates can be used to create custom networking configurations. Within a launch template you can add multiple Elastic Network Interfaces (ENIs) and specify settings such as the availability zones they should be connected to. Note that you cannot attach multiple ENIs to an Amazon EC2 instance connected to subnets in different availability zones. Each ENI must be connected to a subnet in the same availability zone.

navi7 2 years, 11 months ago

is it possible to select BYOIP pool-"id" during creation of launch template? I didn't any. such option.

slackbot 2 years, 11 months ago

i did not find either. i guess this is why A is incorrect

flowers00 3 years ago

A - correct.

flowers00 3 years ago

Change to D.

zaazanuna 3 years ago

D - correct.

https://zhangxuetu.online

[202610]

Question #33 Topic 1

A company delivers applications over the internet. An Amazon Route 53 public hosted zone is the authoritative DNS service for the company and its internet applications, all of which are offered from the same domain name. A network engineer is working on a new version of one of the applications. All the application's components are hosted in the AWS Cloud. The application has a three-tier design. The front end is delivered through Amazon EC2 instances that are deployed in public subnets with Elastic IP addresses assigned. The backend components are deployed in private subnets from RFC1918.
Components of the application need to be able to access other components of the application within the application's VPC by using the same host names as the host names that are used over the public internet. The network engineer also needs to accommodate future DNS changes, such as the introduction of new host names or the retirement of DNS entries.
Which combination of steps will meet these requirements? (Choose three.)

A. Add a geoproximity routing policy in Route 53.

B. Create a Route 53 private hosted zone for the same domain name Associate the application's VPC with the new private hosted zone. **Most Voted**

C. Enable DNS hostnames for the application's VPC. **Most Voted**

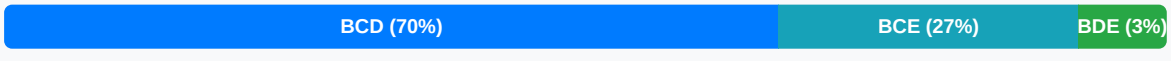
D. Create entries in the private hosted zone for each name in the public hosted zone by using the corresponding private IP addresses. **Most Voted**

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs when AWS CloudTrail logs a Route 53 API call to the public hosted zone. Create an AWS Lambda function as the target of the rule. Configure the function to use the event information to update the private hosted zone.

F. Add the private IP addresses in the existing Route 53 public hosted zone.

Correct Answer: BCD

Community vote distribution



Comments

linuxek21 **Highly Voted** 2 years, 11 months ago

Selected Answer: BCD

Correct Answer: BCD B - you need a priavte hosted zone to resolve the same names to private IPs C - this one is tricky but you really need both of the DNS options enbaled in the VPC (enableDnsHostnames and enableDnsSupport) https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-hostnames "If you use custom DNS domain

names defined in a private hosted zone in Amazon Route 53, or use private DNS with interface VPC endpoints (AWS PrivateLink), you must set both the enableDnsHostnames and enableDnsSupport attributes to true." D - This is correct A - wrong - no need to explain E - Nobody is asking to autmoate the process F - This will simply not work as you need records to resolve to both private nad poublic, yu must have two zones

rhinozD 2 years, 11 months ago

What about this: "The network engineer also needs to accommodate future DNS changes, such as the introduction of new host names or the retirement of DNS entries."

albertkr 2 years, 10 months ago

Agree. The question asks to automate the process.

habros 2 years, 5 months ago

Accommodate != automate

DPDK Highly Voted 2 years, 8 months ago

Selected Answer: BCD

BC are sure. I think the tricky options are D & E. Description mentions future changes, D means change manually. E means change automatically. D mentions add private IP in private hosted zone. E mentions change private hosted zone based on change on public hosted zone. Here, how does E accommodate the value in private hosted zone? Request information of public hosted zone only has public IP, we should not use this in private hosted zone. E doesn't mentioned accommodation even it has automation. So I prefer D.

Joselito79 2 months, 2 weeks ago

Selected Answer: BCE

Step Function B Private hosted zone for internal resolution of the same hostnames C Enable DNS in the VPC for internal resolution E Automate synchronization with the public zone using EventBridge + Lambda

Raphaello 1 year, 11 months ago

Selected Answer: BCD

DNS Split View.. BCD are the correct answers.

vikasj1in 2 years, 1 month ago

Selected Answer: BCE

B. Creating a Route 53 private hosted zone for the same domain name and associating the application's VPC with the new private hosted zone allows internal DNS resolution within the VPC. C. Enabling DNS hostnames for the application's VPC is necessary for DNS resolution within the VPC. E. Creating an Amazon EventBridge rule triggered by AWS CloudTrail logs for Route 53 API calls and using an AWS Lambda function allows for automated updates to the private hosted zone when changes occur in the public hosted zone. This ensures that changes in the public DNS are reflected in the private DNS for internal resolution.

chang4li 1 year, 2 months ago

There's big operation issue for E, unless you create another script to extract public hosted zone records and generate corresponding private zone records at the beginning. Otherwise, you have to keep running the app, potentially w/ errors each time, until all the private DNS names are populated.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is BCD according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is B & C & E.

Arad 2 years, 4 months ago

Selected Answer: BCD

just BCD make sense.

Certified101 2 years, 7 months ago

Selected Answer: BCE

The network engineer also needs to accommodate future DNS changes, such as the introduction of new host names or the retirement of DNS entries. There needs to be an automated process to update new records - BCE is correct

WMF0187 2 years, 6 months ago

While E might allow for some level of automation in updating DNS records, it's complex and involves CloudWatch Events and Lambda functions. Additionally, it doesn't address the core requirement of allowing components within the same VPC to access each other using the same hostnames.

udo2020 2 years, 8 months ago

I think the correct answers are BCD. Regarding the discussion about E. There is no requirement to do that automatically. If this is the case (but it's not stated in the Q), then E is required for automation process.

Tofu13 2 years, 9 months ago

Selected Answer: BCE

Same as Linxek21 beside E instead of D, as automation is needed. E should work: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/logging-using-cloudtrail.html#route-53-info-in-cloudtrail

kalitwol 2 years, 2 months ago

E will not work properly because it is copying public IP addresses from the public hosted zone and adding it to private hosted zone. Private hosted zone should use internal private IPs not public

Spaurito 1 year, 4 months ago

This could work. Would take some testing to make sure your assigning to the Private Zone even though the event is based on the Public Zone.

rhinozD 2 years, 11 months ago

B is correct C is correct D is correct E is also correct But the question has this part: "The network engineer also needs to accommodate future DNS changes, such as the introduction of new host names or the retirement of DNS entries." so I think I'll go with BCE

kalitwol 2 years, 2 months ago

E will not work properly because it is copying public IP addresses from the public hosted zone and adding it to private hosted zone. Private hosted zone should use internal private IPs not public

that1guy 2 years, 11 months ago

Selected Answer: BDE

Not sure why others are going with option C. The question states that they are using custom dns records for external resolving and they want to use the same records for internal. > "Enable DNS hostnames for the application's VPC." This would not result in using the same records as external. > "Components of the application need to be able to access other components of the application within the application's VPC by using the same host names as the host names that are used over the public internet." Unless you are using the same hostnames of the EC2 instances for external resolving it doesn't make sense.

rhinozD 2 years, 11 months ago

"If you use custom DNS domain names defined in a private hosted zone in Amazon Route 53, or use private DNS with interface VPC endpoints (AWS PrivateLink), you must set both the enableDnsHostnames and enableDnsSupport attributes to true." https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

WMF0187 2 years, 6 months ago

Enabling DNS hostnames for the VPC is a prerequisite for using private hosted zones in Route 53. It ensures that instances within the VPC can resolve DNS queries using Route 53.

ohcan 2 years, 11 months ago

B, D, E

ohcan 2 years, 11 months ago

I think C is not needed because is not asking to resolve he hosts names, but the application DNS records. Meanwhile, E is needed to automated the updates

nsei 2 years, 11 months ago

BCE, Option E will meet the requirement for future DNS changes

WMF0187 2 years, 6 months ago

While E approach might allow for some level of automation in updating DNS records, it's complex and involves CloudWatch Events and Lambda functions. Additionally, it doesn't address the core requirement of allowing components within the same VPC to access each other using the same hostnames.

ITgeek 2 years, 11 months ago

Selected Answer: BCD

B C D are my correct answers

helloworldabc 3 years ago

BBBBCCCCDDDD

https://zhangxuetu.online

[202610]

Question #34 Topic 1

A company is deploying an application. The application is implemented in a series of containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use the Fargate launch type for its tasks. The containers will run workloads that require connectivity initiated over an SSL connection. Traffic must be able to flow to the application from other AWS accounts over private connectivity. The application must scale in a manageable way as more consumers use the application.
Which solution will meet these requirements?

A. Choose a Gateway Load Balancer (GLB) as the type of load balancer for the ECS service. Create a lifecycle hook to add new tasks to the target group from Amazon ECS as required to handle scaling. Specify the GLB in the service definition. Create a VPC peer for external AWS accounts. Update the route tables so that the AWS accounts can reach the GLB.

B. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allow the application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPC endpoint service for the ALB Share the VPC endpoint service with other AWS accounts.

C. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allow the application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPC peer for the external AWS accounts. Update the route tables so that the AWS accounts can reach the ALB.

D. Choose a Network Load Balancer (NLB) as the type of load balancer for the ECS service. Specify the NLB in the service definition. Create a VPC endpoint service for the NLB. Share the VPC endpoint service with other AWS accounts. **Most Voted**

Correct Answer: D

Community vote distribution

D (89%) B (11%)

Comments

study_aws1 **Highly Voted** 3 years ago

Path based routing is not required here. Requirement is "Traffic must be able to flow to the application from other AWS accounts over private connectivity. " - which is a case for PrivateLink. It is option D)

linuxek21 **Highly Voted** 2 years, 11 months ago

Selected Answer: D

Correct answer is: D B - You cannot create a service endpoint for an ALB Endpoint services require either a Network Load Balancer or a Gateway Load Balancer. The load balancer receives requests from service consumers and routes them to your service. https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html You can have the ALB behind the NLB but not directly as a service endpoint

Ravan 1 year, 6 months ago

Selected Answer: B

Network Load Balancer: NLBs are not designed for application-level traffic management and might not provide the required features for this scenario.

Raphaello 1 year, 11 months ago

Selected Answer: D

VPC service endpoint using NLB. D is correct.

vikasj1in 2 years, 1 month ago

Selected Answer: B

Choosing an Application Load Balancer (ALB) is suitable for handling SSL connections and path-based routing, providing flexibility in directing traffic to different containers based on paths. Creating path-based routing rules allows the application to target specific containers within the ECS service. Creating a VPC endpoint service for the ALB allows other AWS accounts to access the ALB over private connectivity. Sharing the VPC endpoint service enables traffic from other AWS accounts to flow to the ALB securely.

Marfee400704 2 years, 1 month ago

I think that it's answer is D according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is D.

halukd 2 years, 2 months ago

seems B *Create a target group for the tasks and define it as a listener target in an Application Load Balancer (ALB). Configure the ALB with SSL certificates for the secure connections. Yes, it is possible to use a VPC endpoint with an Application Load Balancer (ALB). A VPC endpoint allows private connectivity between resources in your VPC and another AWS service without requiring access over the public internet or NAT. Specifically, you can configure a VPC endpoint for services like API Gateway, S3, DynamoDB etc. and then associate that endpoint with a target group of your ALB. The ALB can then forward traffic privately to those services. https://repost.aws/questions/QUTXcNxnAuRo-YvGdOoKGy2g/can-an-application-load-balancer-invoke-an-api-gateway-http-api-via-a-vpc-endpoint-interface

Arad 2 years, 4 months ago

Selected Answer: D

Correct answer is D.

Pratap 2 years, 9 months ago

Selected Answer: D

D is the correct option

tcp22 2 years, 9 months ago

this is to exposing the service from ECS(provider) to other consumers, using NLB make sense to be used with private link, hence D

rhinozD 2 years, 11 months ago

Selected Answer: D

"Traffic must be able to flow to the application from other AWS accounts over private connectivity." You don't want to peer the whole VPC just for exposing a service. You can't create a endpoint service with an ALB. -> D

yowoo 2 years, 11 months ago

Selected Answer: D

C and D seem close to the answer, but if I have to choose one, D is Correct The question said that SSL communication between containers is necessary, and the end of SSL communication becomes Container, which means that there is a high possibility that ELB will not off-load In the end, in the case of C, ALB cannot see the decrypted packet, so the URL included in the payload is unknown, and URL-based routing is not possible Therefore, the closest view to the correct answer is D

that1guy 2 years, 11 months ago

Selected Answer: D

No reason to use ALB, SSL != HTTPS, while SSL does not strictly require HTTP, it is typically used in conjunction with HTTP to create HTTPS but it isn't required.

ITgeek 2 years, 11 months ago

Selected Answer: B

B, since you need an ALB for SSL/TLS

devopsbro 3 years ago

B is the correct answer. Use ALB as an endpoint for NLB in VPC Endpoint service. https://aws.amazon.com/about-aws/whats-new/2021/09/application-load-balancer-aws-privatelink-static-ip-addresses-network-load-balancer/

helloworldabc 3 years ago

CCCCCCCCC

https://zhangxuetu.online

[202610]

Question #35 Topic 1

A company's development team has created a new product recommendation web service. The web service is hosted in a VPC with a CIDR block of 192.168.224.0/19. The company has deployed the web service on Amazon EC2 instances and has configured an Auto Scaling group as the target of a Network Load Balancer (NLB).
The company wants to perform testing to determine whether users who receive product recommendations spend more money than users who do not receive product recommendations. The company has a big sales event in 5 days and needs to integrate its existing production environment with the recommendation engine by then. The existing production environment is hosted in a VPC with a CIDR block of 192.168.128 0/17.
A network engineer must integrate the systems by designing a solution that results in the least possible disruption to the existing environments.
Which solution will meet these requirements?

A. Create a VPC peering connection between the web service VPC and the existing production VPC. Add a routing rule to the appropriate route table to allow data to flow to 192.168.224.0/19 from the existing production environment and to flow to 192.168.128.0/17 from the web service environment. Configure the relevant security groups and ACLs to allow the systems to communicate.

B. Ask the development team of the web service to redeploy the web service into the production VPC and integrate the systems there.

C. Create a VPC endpoint service. Associate the VPC endpoint service with the NLB for the web service. Create an interface VPC endpoint for the web service in the existing production VPC. **Most Voted**

D. Create a transit gateway in the existing production environment. Create attachments to the production VPC and the web service VPC. Configure appropriate routing rules in the transit gateway and VPC route tables for 192.168.224.0/19 and 192.168.128.0/17. Configure the relevant security groups and ACLs to allow the systems to communicate.

Correct Answer: C

Community vote distribution

C (100%)

Comments

study_aws1 Highly Voted 2 years, 6 months ago

The CIDR ranges are overlapping, hence VPC peering or Transit Gateway will not work in this scenario. It is option C)

linuxek21 Highly Voted 2 years, 5 months ago

Selected Answer: C

Correct answer is: C This is the only way to overcome the overlap within the available answers ;)

Raphaello 1 year, 5 months ago

Selected Answer: C

Overlapping CIDR of the 2 VPCs, plus it is better not to open the entire 2 VPCs anyways. VPC service endpoint is the solution. C is the correct answer.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is A baccording to SPOTO products.

marfee 1 year, 7 months ago

I think that it's correcty answer is C.

MahmoudKh 1 year, 10 months ago

There is no overlap

Arad 1 year, 11 months ago

Selected Answer: C

no doubt C.

ITgeek 2 years, 5 months ago

The correct answer is C - Create a VPC endpoint service. Associate the VPC endpoint service with the NLB for the web service. Create an interface VPC endpoint for the web service in the existing production VPC. This is because the CIDR blocks of the two VPCs overlap, making VPC peering or a transit gateway not feasible. Option B to redeploy the web service into the production VPC would also be disruptive to the existing environment. Option A to create a VPC peering connection with routing rules to allow data flow is not feasible due to the overlapping CIDR blocks. Option C involves creating an interface VPC endpoint for the web service in the existing production VPC, which allows the web service to be accessed from the production environment without requiring a direct connection between the two VPCs.

titi_r 2 years, 5 months ago

Selected Answer: C

C - correct.

helloworldabc 2 years, 6 months ago

AAAAAAAAA

zaazanuna 2 years, 6 months ago

A - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #36 Topic 1

A network engineer needs to update a company's hybrid network to support IPv6 for the upcoming release of a new application. The application is hosted in a VPC in the AWS Cloud. The company's current AWS infrastructure includes VPCs that are connected by a transit gateway. The transit gateway is connected to the on-premises network by AWS Direct Connect and AWS Site-to-Site VPN. The company's on-premises devices have been updated to support the new IPv6 requirements.

The company has enabled IPv6 for the existing VPC by assigning a new IPv6 CIDR block to the VPC and by assigning IPv6 to the subnets for dual-stack support. The company has launched new Amazon EC2 instances for the new application in the updated subnets.

When updating the hybrid network to support IPv6 the network engineer must avoid making any changes to the current infrastructure. The network engineer also must block direct access to the instances' new IPv6 addresses from the internet. However, the network engineer must allow outbound internet access from the instances.

What is the MOST operationally efficient solution that meets these requirements?

A. Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Create a new VPN connection that supports IPv6 connectivity. Add an egress-only internet gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices

B. Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Update the existing VPN connection to support IPv6 connectivity. Add an egress-only internet gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.

C. Create a Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Create a new VPN connection that supports IPv6 connectivity. Add an egress-only internet gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices. **Most Voted**

D. Create a Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address. Create a new VPN connection that supports IPv6 connectivity. Add a NAT gateway. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.

Correct Answer: C

Community vote distribution



Comments

study_aws1 Highly Voted 3 years ago

https://aws.amazon.com/blogs/networking-and-content-delivery/dual-stack-ipv6-architectures-for-aws-an d-hybrid-networks/ For dual-stack connectivity on the Site-to-Site VPN connection via a Transit Gateway, you need to create two VPN connections, one for the IPv4 stack and one for the IPv6 stack. D. For AWS Direct Connect connection, reuse your existing VIFs and enable them for dual-stack support. Option A) is correct

zaazanuna Highly Voted 3 years ago

A - correct! The MOST operationally efficient solution that meets the requirements is option A. This option updates the Direct Connect transit VIF to support IPv6 and configures BGP peering with the AWS assigned IPv6 peering address. It also creates a new VPN connection that supports IPv6 connectivity, adds an egress-only internet gateway, and updates any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices. This solution does not require any changes to the current infrastructure and effectively blocks direct access to the instances' new IPv6 addresses from the internet while allowing outbound internet access from the instances.

WMF0187 2 years, 6 months ago

Option A also says "Create a new VPN connection that supports IPv6 connectivity" which goes against "when updating the hybrid network to support IPv6 the network engineer must avoid making any changes to the current infrastructure" so creating a new VPN connection will change current infrastructure vs updating will not. Thoughts??

Joselito79 2 months, 2 weeks ago

Selected Answer: B

B is the most operationally efficient option because: It requires no changes to existing infrastructure beyond IPv6. It upgrades Direct Connect and VPN for IPv6. It adds egress-only IGW to ensure secure internet access. It avoids creating unnecessary new VIFs or NATs.

aramisrocha 4 months, 1 week ago

Selected Answer: C

C is correct

alfon78 4 months, 1 week ago

Selected Answer: C

Transit VIF can not be updated to change IPv4 to IPv6

Kraftzman 6 months ago

Selected Answer: C

C is correct

1a17d1e 6 months, 3 weeks ago

Selected Answer: C

You can't modify the IPv6 peering settings after the Transit VIF is created.

1a17d1e 7 months, 2 weeks ago

Selected Answer: C

Correct me if I'm wrong but the Q doesn't say that a transit VIF already exists(?) I can't assume there's a transit VIF that exists to update.

1a17d1e 7 months ago

once a Direct Connect transit virtual interface (VIF) is created, you cannot retroactively configure BGP peering with AWS-assigned IPv6 addresses. If you didn't enable IPv6 peering during initial setup, you'll need to delete and recreate the transit VIF to include it.

percolate792 1 year ago

Selected Answer: A

Option should be "A" because a Direct Connect connection can only support one transit VIF. and I think this should be the actual decision factor although updating the transit vif to support ipv6 can create minimal disruption but we can not have multiple transit vif.

RavikantKumarRavi 1 year ago

Selected Answer: C

Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address is not possible once it get created . It need to create again

jfedotov 1 year, 2 months ago

Selected Answer: C

C is correct A is wrong, because there is no option to select both ip4 and ipv6 in transit VIF

Jonalb 1 year, 3 months ago

Selected Answer: A

its A https://aws.amazon.com/blogs/networking-and-content-delivery/dual-stack-ipv6-architectures-for-aws-an d-hybrid-networks/

Spaurito 1 year, 4 months ago

C - When looking at the requirements, this makes more sense. You can't update a VPN and adding new keeps the change separate from the existing configurations.

Raphaello 1 year, 11 months ago

Selected Answer: C

Cannot update the Address Family in existing Transit VIF. Will have to create anew Transit VIF, selecting Address Family IPv6. C is correct.

Raphaello 1 year, 11 months ago

I think A might be correct.. Here's AWS documentation says can "reuse [your] existing VIF's and enable [them] for dual-stack support. << AWS Direct Connect enables you to configure private and dedicated connectivity to your on-premises, and natively supports both IPv4 and IPv6 routing. To use your Direct Connect connection for dual-stack traffic, you need to first create one of the following virtual interfaces (VIFs): Private VIF, Public VIF or Transit VIF, or reuse your existing VIFs and enable them for dual-stack support. >> So obviously o need to create a new VIF. A is fine.

surnila 2 years ago

A Site-to-Site VPN connection cannot support both IPv4 and IPv6 traffic and hence option A is correct

surnila 2 years ago

https://docs.aws.amazon.com/vpn/latest/s2svpn/ipv4-ipv6.html

kyuhuck 2 years ago

Selected Answer: B

Given these considerations, Option B is the most operationally efficient solution that meets the stated requirements. It involves updating the existing Direct Connect and VPN connections to support IPv6, adding an egress-only internet

gateway for controlled IPv6 internet access, and updating VPC security groups and route tables accordingly, without necessitating significant changes to the existing infrastructure.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

https://zhangxuetu.online

[202610]

Question #37 Topic 1

A network engineer must provide additional safeguards to protect encrypted data at Application Load Balancers (ALBs) through the use of a unique random session key.
What should the network engineer do to meet this requirement?

A. Change the ALB security policy to a policy that supports TLS 1.2 protocol only

B. Use AWS Key Management Service (AWS KMS) to encrypt session keys

C. Associate an AWS WAF web ACL with the ALBs. and create a security rule to enforce forward secrecy (FS)

D. Change the ALB security policy to a policy that supports forward secrecy (FS) **Most Voted**

Correct Answer: D

Community vote distribution



Comments

study_aws1 **Highly Voted** 3 years ago

Option D) Use ELBSecurityPolicy-FS policies, if you require Forward Secrecy • Provides additional safeguards against the eavesdropping of encrypted data • Using a unique random session key

titi_r **Highly Voted** 2 years, 12 months ago

Selected Answer: D

Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key. This prevents the decoding of captured data, even if the secret long-term key is compromised. https://aws.amazon.com/about-aws/whats-new/2014/02/19/elastic-load-balancing-perfect-forward-secrecy-and-more-new-security-features/ https://aws.amazon.com/about-aws/whats-new/2018/06/application-load-balancer-adds-new-security-policies-including-policy-for-forward-secrecy/

btech24 1 year, 6 months ago

D is the correct answer Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key. This prevents the decoding of captured data, even if the secret long-term key is compromised.

Raphaello 1 year, 11 months ago

Selected Answer: D

Select Security Policy that support FS algorithms. D is the correct answer.

marfee 2 years, 1 month ago

I think that it's correcty answer is D.

ILOVEVODKA 3 years ago

Correct is either C or D, bur prob D. B is for sure wrong.

fojta 3 years ago

To provide additional safeguards to protect encrypted data at Amazon Application Load Balancers (ALBs) through the use of a unique random session key, the network engineer should use AWS Key Management Service (AWS KMS) to encrypt session keys. Therefore, the correct answer is B.

helloworldabc 3 years ago

BBBBBBBBB

zaazanuna 3 years ago

B - correct. The requirement is to provide additional safeguards to protect encrypted data at Application Load Balancers (ALBs) through the use of a unique random session key. To meet this requirement, the network engineer should use AWS Key Management Service (AWS KMS) to encrypt session keys. Therefore, the correct answer is option B.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #38 Topic 1

A company has deployed a software-defined WAN (SD-WAN) solution to interconnect all of its offices. The company is migrating workloads to AWS and needs to extend its SD-WAN solution to support connectivity to these workloads.
A network engineer plans to deploy AWS Transit Gateway Connect and two SD-WAN virtual appliances to provide this connectivity. According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time.
How should the network engineer configure routing to meet these requirements?

A. Add a static default route in the transit gateway route table to point to the secondary SD-WAN virtual appliance. Add routes that are more specific to point to the primary SD-WAN virtual appliance.

B. Configure the BGP community tag 7224:7300 on the primary SD-WAN virtual appliance for BGP routes toward the transit gateway.

C. Configure the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway. Most Voted

D. Disable equal-cost multi-path (ECMP) routing on the transit gateway for Transit Gateway Connect.

Correct Answer: C

Community vote distribution



Comments

dremm Highly Voted 2 years, 11 months ago

A - incorrect , static routes are not possible in TGW B- incorrect, these BGP communities are used for BGP over DX C- correct , AS_PATH prepending is a standard BGP way of influencing return traffic for advertised prefixes and SDWAN supports this. D- incorrect, disabling ECMP will make sure the SDWAN>TGW traffic is not load shared, but the return traffic TGW>SDWAN is not affected and therefore both appliances will process traffic.

secdaddy 1 year, 1 month ago

C - as path prepending prefixes being advertised by the SDWAN device also only influences traffic from TGW towards the SD-WAN appliances D - other way around. Disabling ECMP on the TGW affects traffic TGW to SDWAN. None of the answers addresses traffic from the SD-WAN devices towards AWS.

leotoras 2 years, 2 months ago

static routes are possible in TGW as per the documentation: You can create a static route for a VPC, VPN, or transit gateway peering attachment, or you can create a blackhole route that drops traffic that matches the route.

zaazanuna Highly Voted 2 years, 12 months ago

Option C - focuses specifically on the SD-WAN virtual appliances. By configuring the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway, the network engineer can influence routing preferences, making the primary SD-WAN virtual appliance the preferred path while keeping the secondary appliance as a backup. This approach meets the company's requirement of having only a single SD-WAN virtual appliance handle traffic from AWS workloads at a given time without impacting other connections.

ITgeek 2 years, 11 months ago

The company policy doesn't allow the use of the second SD WAN. In the event of a failure this will violate that company policy. Therefore option D is the closest

Fukat 2 years, 8 months ago

"According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time." This means at a given time on single SD-WAN should be used. This is achieved by Option C. Second SD-WAN will be only used if first SD-WAN fails due to AS PATH prepending. Also option D is not correct. ECMP can be turned on/off for the whole TGW and it is only applicable for VPN attachment. - https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html#create-tgw

Joselito79 2 months, 2 weeks ago

Selected Answer: C

Use C: Configure AS_PATH prepend on the secondary SD-WAN appliance to ensure a single primary handles traffic, and the secondary is only used as a failover.

1a17d1e 7 months, 4 weeks ago

Selected Answer: C

Prepending will ensure that routing will prefer a direction as long as the route is advertised. If the route goes away, the route should disappear from both advertising paths, thus maintaining the "only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time". If you advertise specifics on a primary path and an aggregate on the secondary, you will have some traffic using the secondary when a route advertisement disappears while the others will remain on the primary path.

youonebe 1 year, 1 month ago

Selected Answer: A

The answer is A, Cantrill explained this very well in his `Transit gateway Deep Dive` course

Spaurito 1 year, 4 months ago

Option C is best. Option A says adding a static route and add additional afterwards. Static Routes take preference but the question states only one appliance can handle traffic at a time. Gotta go with C

Jonalb 1 year, 6 months ago

Selected Answer: C

its a C

acloudguru 1 year, 10 months ago

Selected Answer: A

Both B and C are for preference

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. Influence AS_PATH to favour the primary. CONNECT attachments do not support static routes. BGP is a minimum requirement for Transit Gateway Connect.

Raphaello 1 year, 11 months ago

AWS doc explicitly states.. "A Connect peer using the BGP AS-PATH attribute is the preferred route when you have two Connect peers." Additionally, using ECMP (option D) is actually the opposite of what we want to achieve here. ECMP will provide redundancy (load-balancing). Again AWS documentation clearly states ECMP requires SAME AS-PATH ATTRIBUTE on all peered BGP. " you must configure the appliance to advertise the same prefixes to the transit gateway with the same BGP AS-PATH attribute." https://docs.aws.amazon.com/vpc/latest/tgw/tgw-connect.html#tgw-connect-requirements

tromyunpak 2 years ago

Correct Answer is C - A will only influence the traffic from the AWS side B is applicable to Direct Connect C uses prepend to prioritise traffic D only load sharing is disabled routes are still active

meseerie 2 years ago

I have created this scenario in Production using AS_Path prepend. AS_Path It's like basically faking an extra hop/ For BGP AS_Path and local preference will do the job for routing advert. The Goal was to achieve an Active/Standby scenario and avoid asymmetric routing. Option C correct

vikasj1in 2 years, 1 month ago

Selected Answer: A

Adding a static default route in the transit gateway route table to point to the secondary SD-WAN virtual appliance ensures that the secondary appliance is the default route, meaning it will be used only when no more specific route is available. Adding more specific routes to point to the primary SD-WAN virtual appliance allows for traffic from AWS workloads to be directed to the primary appliance, satisfying the company policy that only a single SD-WAN virtual appliance should handle traffic from AWS workloads at a given time. Options B and C involve BGP configurations but may not be as straightforward or aligned with the requirement of having a single SD-WAN virtual appliance handling traffic at a time. Option D is not relevant to this specific scenario and doesn't address the requirement of having a single SD-WAN virtual appliance handle traffic at a given time.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

FayeG 2 years, 4 months ago

Selected Answer: C

As per https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-sd-wan.html SD-Wan connects to TGW using BGP for routing. Therefore no static route, therefore C is the answer.

WMF0187 2 years, 6 months ago

If there are two Connect peers, the preferred route is the Transit Gateway Connect peer that uses the BGP AS-PATH attribute. To use Equal Cost Multipath (ECMP) routing between multiple appliances, you must configure the appliances to advertise the same prefixes to transit gateways using the same BGP AS-PATH attribute. The AS-PATH and autonomous system number (ASN) must match for the transit gateway to select all available ECMP paths. Transit Gateways can use ECMP between Transit Gateway Connect peers on the same Connect attachment or between Connect attachments on the same Transit Gateway. Transit Gateway does not support the use of ECMP between both redundant BGP peer connections established by one peer. Connect attachments propagate routes to the Transit Gateway route table by default. Static routes are not supported.
https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/tgw-connect.html#tgw-connect-requirements

ExamTopix01 2 years, 7 months ago

C A Transit Gateway Connect peer using the BGP AS-PATH attribute is the preferred route when you have two Connect peers. https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/tgw-connect.html#tgw-connect-requirements

sp237 2 years, 8 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/migrating-sd-wan-appliances-to-aws-transit-gateway-connect/ Improved availability: Transit Gateway Connect supports equal-cost multipathing (ECMP) with a 5-tuple hash – protocol number, source IP address, destination IP address, source port number, and destination port number. This allows your traffic to be distributed evenly across multiple appliances, reducing the impact of a single appliance failure compared to the one-appliance-per-AZ approach with VPC attachments.

https://zhangxuetu.online

[202610]

Question #39 Topic 1

A company is planning to deploy many software-defined WAN (SD-WAN) sites. The company is using AWS Transit Gateway and has deployed a transit gateway in the required AWS Region. A network engineer needs to deploy the SD-WAN hub virtual appliance into a VPC that is connected to the transit gateway. The solution must support at least 5 Gbps of throughput from the SD-WAN hub virtual appliance to other VPCs that are attached to the transit gateway.
Which solution will meet these requirements?

A. Create a new VPC for the SD-WAN hub virtual appliance. Create two IPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway. Configure BGP over the IPsec VPN connections

B. Assign a new CIDR block to the transit gateway. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Add a transit gateway Connect attachment. Create a Connect peer and specify the GRE and BGP parameters. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway. Most Voted

C. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Create two IPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway. Configure BGP over the IPsec VPN connections.

D. Assign a new CIDR block to the transit gateway. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Add a transit gateway Connect attachment. Create a Connect peer and specify the VXLAN and BGP parameters. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.

Correct Answer: B

Community vote distribution

B (100%)

Comments

study_aws1 Highly Voted 2 years, 6 months ago

Should be B) A Connect attachment uses an existing VPC or AWS Direct Connect attachment as the underlying transport mechanism. • Supports Generic Routing Encapsulation (GRE) tunnel protocol for high performance, and Border Gateway Protocol (BGP) for dynamic routing.

Raphaello 1 year, 5 months ago

Selected Answer: B

B is the correct answer. TGW Connect attachment over VPC attachment, with GRE and BGP used.

tromyunpak 1 year, 6 months ago

B is the correct answer due to GRE and connect peer which delivers 5GB/s A is wrong due to IPSEC is 1.25/Gb/s per vpn even ECMP configured you get less than 5Gb/s C is wrong same as A D is wrong VXLAN is not supported with TGW

marfee 1 year, 7 months ago

I think that it's correcty answer is B.

FayeG 1 year, 11 months ago

Selected Answer: B

Although SD-WAN devices can use VXLAN only GRE is support on TGW as of this comment's timestamp.

skiingfalcon 1 year, 11 months ago

Selected Answer: B

https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-sd-wan-connectivity-with-aws-transit-gateway-connect/

prajkash 2 years, 2 months ago

Voting for B

symplesims 2 years, 3 months ago

Exactly B https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-sd-wan-connectivity-with-aws-transit-gateway-connect/

albertkr 2 years, 4 months ago

Selected Answer: B

https://aws.amazon.com/blogs/networking-and-content-delivery/integrate-sd-wan-devices-with-aws-transit-gateway-and-aws-direct-connect/

Chinmoy 2 years, 4 months ago

Selected Answer: B

Gre and baby with connect attachment

ITgeek 2 years, 4 months ago

Selected Answer: B

Should b B

silviahdz 2 years, 5 months ago

Selected Answer: B

B is the correct answer, TGW Connect is setup with GRE and BGP no mention of VXLAN: https://aws.amazon.com/transit-gateway/faqs/

Jotoval 2 years, 5 months ago

Sould be B according this document. https://aws.amazon.com/es/blogs/networking-and-content-delivery/simplify-sd-wan-connectivity-with-aws-transit-gateway-connect/

helloworldabc 2 years, 6 months ago

DDDDDDDD

zaazanuna 2 years, 6 months ago

D - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #40 Topic 1

A company is deploying a new application on AWS. The application uses dynamic multicasting. The company has five VPCs that are all attached to a transit gateway Amazon EC2 instances in each VPC need to be able to register dynamically to receive a multicast transmission.
How should a network engineer configure the AWS resources to meet these requirements?

A. Create a static source multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.

B. Create a static source multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.

C. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address. **Most Voted**

D. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway. Associate the VPCs and applicable subnets with the multicast domain. Register the multicast senders' network interface with the multicast domain. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.

Correct Answer: C

Community vote distribution

C (100%)

Comments

ITgeek **Highly Voted** 2 years, 5 months ago

Selected Answer: C

C for UDP not TCP

Raphaello 1 year, 5 months ago

Selected Answer: C

Multicast is a connectionless UDP-based transport, and dynamic group membership is through IGMP. C is the correct answer.

vikasj1in 1 year, 7 months ago

Selected Answer: C

Using IGMP (Internet Group Management Protocol) is a common approach for dynamic multicasting. It allows hosts to report their multicast group memberships to any neighboring multicast routers, which in this case is the transit gateway. Creating an IGMP multicast domain within the transit gateway helps organize and manage the multicast traffic. Associating the VPCs and applicable subnets with the multicast domain ensures that the multicast traffic is properly routed within the transit gateway. Registering the multicast senders' network interface with the multicast domain allows them to dynamically join the multicast group. Adjusting the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address ensures proper communication between multicast senders and receivers.

marfee 1 year, 7 months ago

I think that it's correcty answer is C.

Arad 1 year, 11 months ago

Selected Answer: C

Correct answer is C.

Alabi 2 years ago

Selected Answer: C

C for sure

sdey0008 2 years, 3 months ago

IGMP+UDP

joeyjones 2 years, 4 months ago

https://docs.aws.amazon.com/vpc/latest/tgw/how-multicast-works.html
https://docs.aws.amazon.com/vpc/latest/tgw/working-with-multicast.html#multicast-configurations-igmp

ohcan 2 years, 5 months ago

C. I doubt with A, but as it requires "dynamic" multicast then C is better.

study_aws1 2 years, 6 months ago

Yes C is correct

helloworldabc 2 years, 6 months ago

CCCCCCCC

zaazanuna 2 years, 6 months ago

C - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #41 Topic 1

A company is creating new features for its ecommerce website. These features will use several microservices that are accessed through different paths. The microservices will run on Amazon Elastic Container Service (Amazon ECS). The company requires the use of HTTPS for all of its public websites. The application requires the customer's source IP addresses.
A network engineer must implement a load balancing strategy that meets these requirements.
Which combination of actions should the network engineer take to accomplish this goal? (Choose two.)

A. Use a Network Load Balancer

B. Retrieve client IP addresses by using the X-Forwarded-For header **Most Voted**

C. Use AWS App Mesh load balancing

D. Retrieve client IP addresses by using the X-IP-Source header

E. Use an Application Load Balancer. **Most Voted**

Correct Answer: BE

Community vote distribution

BE (100%)

Comments

zaazanuna **Highly Voted** 2 years, 5 months ago

Using an Application Load Balancer (ALB) is more appropriate in this scenario because it supports path-based routing, which is required for the microservices accessed through different paths. ALB also supports HTTPS, which is a requirement for the company's public websites.

Raphaello 1 year, 5 months ago

Selected Answer: BE

BE are the correct answers.

marfee 1 year, 7 months ago

I think that it's correcty answer is B & E.

halukd 1 year, 8 months ago

B,C AppMesh is the best for microservices with ECS. https://aws.amazon.com/app-mesh/features/

Arad 1 year, 11 months ago

Selected Answer: BE

obviously B & E.

Scunningham99 2 years ago

B & E https://docs.aws.amazon.com/elasticloadbalancing/latest/application/x-forwarded-headers.html

ozan11 2 years, 3 months ago

The application requires the customer’s source IP addresses. NLB does that. ALB don't as far as I know. I'll go with AB.

PTLS 2 years, 5 months ago

Selected Answer: BE

B, E are correct

helloworldabc 2 years, 6 months ago

BBBBBBBEEEEEEEE

zaazanuna 2 years, 6 months ago

B, E - correct.

https://zhangxuetu.online

[202610]

Question #42 Topic 1

A company is migrating its containerized application to AWS. For the architecture the company will have an ingress VPC with a Network Load Balancer (NLB) to distribute the traffic to front-end pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The front end of the application will determine which user is requesting access and will send traffic to 1 of 10 services VPCs. Each services VPC will include an NLB that distributes traffic to the services pods in an EKS cluster.
The company is concerned about overall cost. User traffic will be responsible for more than 10 TB of data transfer from the ingress VPC to services VPCs every month. A network engineer needs to recommend how to design the communication between the VPCs.
Which solution will meet these requirements at the LOWEST cost?

A. Create a transit gateway. Peer each VPC to the transit gateway. Use zonal DNS names for the NLB in the services VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs.

B. Create an AWS PrivateLink endpoint in every Availability Zone in the ingress VPC. Each PrivateLink endpoint will point to the zonal DNS entry of the NLB in the services VPCs.

C. Create a VPC peering connection between the ingress VPC and each of the 10 services VPCs. Use zonal DNS names for the NLB in the services VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs. **Most Voted**

D. Create a transit gateway. Peer each VPC to the transit gateway. Turn off cross-AZ load balancing on the transit gateway. Use Regional DNS names for the NLB in the services VPCs.

Correct Answer: C

Community vote distribution



Comments

titi_r **Highly Voted** 2 years, 12 months ago

Selected Answer: C

C - seems the right one. VPC peering offers the lowest overall cost when compared to other options for inter-VPC connectivity. https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-to-vpc-connectivity.html There is no such thing as "TG peering"; there are VPC peering and TG attachments.

seochan 1 year, 10 months ago

I agree that C is right, but TGW peering exists. https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html

Spaurito 1 year, 4 months ago

C - the scenario states "each services VPC." VPC peering is more appropriate for costs.

Raphaello 1 year, 11 months ago

Selected Answer: C

VPC peering is the lowest cost option, additionally VPC peering is for handling direct connectivity requirements, whereas AWS PrivateLink (service endpoint) is handling API style client-server connectivity. In this scenario option C is the correct answer.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

Vogd 2 years, 2 months ago

C - https://aws.amazon.com/about-aws/whats-new/2021/05/amazon-vpc-announces-pricing-change-for-vpc-peering/ private link used to interconnect hundred to thousand VPC's. Peering is our use case scenario.

cumzle_com 2 years, 3 months ago

Selected Answer: B

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/access-container-applications-privately-on-amazon-eks-using-aws-privatelink-and-a-network-load-balancer.html

Balasmaniam 2 years, 9 months ago

B is correct ans

Training 2 years, 9 months ago

Should be B. https://aws.amazon.com/blogs/networking-and-content-delivery/implement-a-central-ingress-application-load-balancer-supporting-private-amazon-elastic-kubernetes-service-vpcs/

tech4932943240 2 years, 10 months ago

c seems correct

Spike2020 2 years, 11 months ago

B is the least costly

bcx 2 years, 8 months ago

B has PrivateLink processing charges. VPC peering is free as long as you stay within the same AZ.

ITgeek 2 years, 11 months ago

Selected Answer: C

Considering cost C, is the ideal solution

awsguru1998 2 years, 11 months ago

B is correct. TG costs more and no such thing as vpc peer to TG

slackbot 2 years, 11 months ago

mr Guru, VPC endpoints are not free as well. C is cheapest

devopsbro 3 years ago

Though transit gateway solves works here, but it comes with running cost per hours+data transfer costs. In case of VPC peering, it comes with free of cost. Only need to pay the data transfer cost. So I think VPC peering is most cost effective option.

study_aws1 3 years ago

VPC cannot be peered but attached to Transit Gateway (Either it can be VPC peering or Transit Gateway peering). Additionally, Transit Gateway has its own cost including hourly cost of attachment + Data transfer. PrivateLink resolves the cost problem of high volume of data transfer & is a easy way for ingress VPC to route traffic based on Endpoint service exposed. Also, minimize cross-AZ traffic by using zonal DNS names for the NLB is addressed in this scenario. It should be Option B)

zaazanuna 3 years ago

While AWS PrivateLink provides private connectivity between VPCs, it is generally more expensive than VPC peering, especially when dealing with a large amount of data transfer, such as the 10 TB mentioned in the question.

study_aws1 2 years, 12 months ago

After careful review, changed to C) considering cost. With Privatelink Endpoint in each AZ in Ingress VPC, it would turn up to 30 Zonal endpoints with 3 AZ - not effective from cost consideration./

helloworldabc 3 years ago

AAAAAAAAAAA

zaazanuna 3 years ago

A - correct. Option A is the most cost-effective solution because it allows the company to minimize cross-AZ traffic by using zonal DNS names for the NLB in the services VPCs. This will help to reduce data transfer costs. Additionally, by using a transit gateway, the company can easily peer each VPC to the transit gateway and manage the traffic flow between them.

https://zhangxuetu.online

[202610]

Question #43 Topic 1

A company has stateful security appliances that are deployed to multiple Availability Zones in a centralized shared services VPC. The AWS environment includes a transit gateway that is attached to application VPCs and the shared services VPC. The application VPCs have workloads that are deployed in private subnets across multiple Availability Zones. The stateful appliances in the shared services VPC inspect all east west (VPC-to-VPC) traffic.
Users report that inter-VPC traffic to different Availability Zones is dropping. A network engineer verified this claim by issuing Internet Control Message Protocol (ICMP) pings between workloads in different Availability Zones across the application VPCs. The network engineer has ruled out security groups, stateful device configurations and network ACLs as the cause of the dropped traffic.
What is causing the traffic to drop?

A. The stateful appliances and the transit gateway attachments are deployed in a separate subnet in the shared services VPC.

B. Appliance mode is not enabled on the transit gateway attachment to the shared services VPC. Most Voted

C. The stateful appliances and the transit gateway attachments are deployed in the same subnet in the shared services VPC.

D. Appliance mode is not enabled on the transit gateway attachment to the application VPCs.

Correct Answer: B

Community vote distribution

B (100%)

Comments

study_aws1 Highly Voted 2 years, 6 months ago

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html Option B)

devopsbro Highly Voted 2 years, 6 months ago

B - Transit gateway Appliance mode should be enabled for the appliance VPC attachment to avoid dropping of the cross AZ traffics.

kourosh 1 year, 5 months ago

Selected Answer: B

B - Should be enabled under VPC which the appliance is located.

Raphaello 1 year, 5 months ago

Selected Answer: B

B is the correct answer. Appliance mode needs to be enabled on the shared VPC where the stateful inspection appliance resides.

marfee 1 year, 7 months ago

I think that it's correcty answer is B.

Arad 1 year, 11 months ago

Selected Answer: B

For sure B.

ohcan 2 years, 5 months ago

Selected Answer: B

B. Appliance mode needs to be enabled in the appliance VPC

helloworldabc 2 years, 6 months ago

AAAAAAAAAAA

zaazanuna 2 years, 6 months ago

A - correct. Option D suggests that the issue is caused by Appliance Mode not being enabled on the transit gateway attachment to the application VPCs. However, this is unlikely to be the cause of the problem described in the scenario, because Appliance Mode is used to forward all traffic to the next hop, without performing routing table lookups or IP address translations. In this case, the issue is related to inter-VPC traffic between different Availability Zones, and the fact that the stateful security appliances in the shared services VPC are dropping the traffic. Therefore, the root cause of the problem is related to the deployment of the stateful security appliances and the transit gateway attachments in the shared services VPC, as well as the fact that they are not able to handle the inter-Availability Zone traffic from the application VPCs. This is why the correct answer is option A, which suggests that the stateful appliances and the transit gateway attachments are deployed in a separate subnet in the shared services VPC.

Fukat 2 years, 2 months ago

If you read carefully the option says the stateful appliances and the transit gateway attachments are deployed in a "separate subnet". It does not mentions anything about AZ. If you see the diagram following doc, then it is actually required that appliance and TGW attachment ENI should in different subnet, ow routing will not work - https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html So answer B is correct

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #44 Topic 1

A company has hundreds of Amazon EC2 instances that are running in two production VPCs across all Availability Zones in the us-east-1 Region. The production VPCs are named
VPC A and VPC B.
A new security regulation requires all traffic between production VPCs to be inspected before the traffic is routed to its final destination. The company deploys a new shared VPC that contains a stateful firewall appliance and a transit gateway with a VPC attachment across all VPCs to route traffic between VPC A and VPC B through the firewall appliance for inspection. During testing, the company notices that the transit gateway is dropping the traffic whenever the traffic is between two Availability Zones.
What should a network engineer do to fix this issue with the LEAST management overhead?

A. In the shared VPC, replace the VPC attachment with a VPN attachment. Create a VPN tunnel between the transit gateway and the firewall appliance. Configure BGP.

B. Enable transit gateway appliance mode on the VPC attachment in VPC A and VPC B.

C. Enable transit gateway appliance mode on the VPC attachment in the shared VPC. **Most Voted**

D. In the shared VPC, configure one VPC peering connection to VPC A and another VPC peering connection to VPC B.

Correct Answer: C

Community vote distribution

C (95%) B (5%)

Comments

study_aws1 **Highly Voted** 2 years, 6 months ago
It is option C)

devopsbro **Highly Voted** 2 years, 6 months ago
C is correct.

Raphaello 1 year, 5 months ago
Selected Answer: C
C is the correct answer. Appliance mode needs to be enabled on the shared VPC where the stateful inspection appliance resides.

tromyunpak 1 year, 6 months ago
the answer is C - The reason is that the appliance mode will avoid having asymmetric flows. With asymmetric flows the firewall will drop the traffic

vikasj1in 1 year, 7 months ago

Selected Answer: B

Enabling transit gateway appliance mode on the VPC attachment in VPC A and VPC B allows the traffic between the Availability Zones to be processed by the firewall appliance. This mode is specifically designed to handle scenarios where traffic needs to be inspected by a security appliance before being routed to its final destination. It provides a straightforward solution without the need for additional VPNs or VPC peering connections. Option A involves replacing the VPC attachment with a VPN attachment and creating a VPN tunnel, which introduces additional complexity. Option C involves enabling appliance mode only on the shared VPC attachment, which might not address the specific issue related to traffic between Availability Zones. Option D suggests using VPC peering connections, which may not be the most efficient solution for this scenario.

vikasj1in 1 year, 7 months ago

Changing to Option C. the shared VPC is the central point where traffic inspection is required, so configuring it in the shared VPC would be more appropriate.

marfee 1 year, 7 months ago

I think that it's correcty answer is B.

Arad 1 year, 11 months ago

Selected Answer: C

Correct answer is C.

evargasbrz 2 years, 1 month ago

Selected Answer: C

Following this document: https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html the appliance mode must be enabled to keep the traffic in the same firewall appliance, regardless of the AZ where are the source and destination. When appliance mode is not enabled, a transit gateway attempts to keep traffic routed between VPC attachments in the originating Availability Zone until it reaches its destination.

PhilMultiCloud 2 years, 1 month ago

Selected Answer: C

To fix the issue of dropped traffic between two Availability Zones when routing traffic between VPC A and VPC B through the firewall appliance for inspection, the network engineer should enable transit gateway appliance mode on the VPC attachment in the shared VPC (Option C). Enabling transit gateway appliance mode ensures that all traffic passing through the transit gateway is inspected by the stateful firewall appliance. This helps in meeting the security regulation requirements without the need for complex changes such as replacing VPC attachments with VPN attachments or configuring VPC peering connections. Enabling transit gateway appliance mode on the VPC attachment in the shared VPC is the solution that requires the least management overhead and directly addresses the issue of dropped traffic between Availability Zones.

Manh 2 years, 2 months ago

Ans is B: https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html For each VPC attachment, specify a subnet in each Availability Zone. For the shared services VPC, these are the subnets where traffic is routed to the VPC from the transit gateway. In the preceding example, these are subnets A and C. For the VPC attachment for VPC C, enable appliance mode support so that response traffic is routed to the same Availability Zone in VPC C as the source traffic. The Amazon VPC console supports appliance mode. You can also use the Amazon VPC API, an AWS SDK, the AWS CLI to enable appliance mode, or AWS CloudFormation. For example, add --options ApplianceModeSupport=enable to the create-transit-gateway-vpc-attachment or modify-transit-gateway-vpc-attachment command.

zendevloper 1 year, 10 months ago

B is wrong. Appliance mode must be enabled in VPC C (where the appliance is deployed) Quote from docs: > If your VPC attachments span multiple Availability Zones and you require traffic between source and destination hosts to be routed through the same appliance for stateful inspection, enable appliance mode support for the VPC attachment in which the appliance is located.

Wiss7 2 years, 2 months ago

Selected Answer: C

C! Appliance mode is on the attachment towards the 3rd party FW VPC

silviahdz 2 years, 5 months ago

Selected Answer: C

C is the right answer.

ohcan 2 years, 5 months ago

Selected Answer: C

C. Appliance mode always enabled in the "shared" VPC

Mr_Marcus 2 years, 5 months ago

C - https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

helloworldabc 2 years, 6 months ago

BBBBBBBBBB

zaazanuna 2 years, 6 months ago

B - correct. Option B is the correct answer as enabling appliance mode on the VPC attachment in VPC A and VPC B will allow the transit gateway to forward all traffic between Availability Zones to the stateful firewall appliance. This will fulfill the requirement of inspecting all traffic between production VPCs while keeping the management overhead low. The other options are not necessary or will add additional complexity to the network design. Option A suggests using VPNs, which can add additional overhead and complexity compared to transit gateway attachments. Option C suggests enabling appliance mode on the VPC attachment in the shared VPC, which would not address the issue of traffic being dropped between Availability Zones. Option D suggests using VPC peering connections, which would not enable the traffic to be inspected by the stateful firewall appliance.

https://zhangxuetu.online

[202610]

Question #45 Topic 1

A company has deployed a critical application on a fleet of Amazon EC2 instances behind an Application Load Balancer. The application must always be reachable on port 443 from the public internet. The application recently had an outage that resulted from an incorrect change to the EC2 security group.
A network engineer needs to automate a way to verify the network connectivity between the public internet and the EC2 instances whenever a change is made to the security group. The solution also must notify the network engineer when the change affects the connection.
Which solution will meet these requirements?

A. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture REJECT traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for rejected traffic. Create an alarm to notify the network engineer.

B. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture all traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for all traffic. Create an alarm to notify the network engineer

C. Create a VPC Reachability Analyzer path on port 443. Specify the security group as the source. Specify the EC2 instances as the destination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fail Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security group occurs.

D. Create a VPC Reachability Analyzer path on port 443. Specify the internet gateway of the VPC as the source. Specify the EC2 instances as the destination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fail. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security group occurs. Most Voted

Correct Answer: D

Community vote distribution

D (93%) C (7%)

Comments

rhinozD Highly Voted 2 years, 11 months ago

Selected Answer: D

refer this link. https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/

cutedragonster Highly Voted 2 years, 12 months ago

Selected Answer: D

C is not correct because security group is not a valid source

vikasj1in 2 years, 1 month ago

That's right. Reference link here to find out the proper source & destination - https://docs.aws.amazon.com/vpc/latest/reachability/how-reachability-analyzer-works.html#source-and-destination-resources

Spaurito 1 year, 4 months ago

Reviewing the link provided shows the example of the IGW as a source and EC2 and a destination. D is the best choice as a security group is an path component not a Src/Dst resource.

arturogomezb 1 year, 9 months ago

source NAT gateway in VPC reachability no simulates conection EC2 -> Nat gateway , but NAT gateway --> EC2 , then it´s possible to change outbound SG rules and no afect to VPC reachability but afect to EC2 --> NAT gateway. In my opinion the option A is ok.

arturogomezb 1 year, 9 months ago

Sorry, it´s wrong , the option is D, the conexión to check is from internet NAT gateway --> EC2

Raphaello 1 year, 11 months ago

Selected Answer: D

Correct answer is D. IGW and EC2 are valid Reachability Analyzer source/destination.

marfee 2 years, 1 month ago

I think that it's correcty answer is D.

MarcosSantos 2 years, 2 months ago

In this question I would go with letter A. Because with this alarm that we created from Cloudwatch logs, we were able to integrate it with an SNS topic. And that in a simpler way. The link you provided: https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/ Apparently it notifies via SNS and also returns the sg port to the way it was before the rule was removed. But the question focused on just notifying, and not that if any change in the sg occurs, return the port.

Arad 2 years, 4 months ago

Selected Answer: D

D is correct answer.

demoras 2 years, 9 months ago

Selected Answer: D

D- Internet gateway is a valid source

ITgeek 2 years, 11 months ago

Selected Answer: D

D is correct

ohcan 2 years, 11 months ago

Selected Answer: D

D correct. A or B are missing the SNS part. C wrong source

MarcosSantos 2 years, 2 months ago

By creating the Clouwatch alarm, we can integrate it with an sns topic

TicDcNess 2 years, 11 months ago

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html Example section at the end metric filter and alarm for a flow log should be A

ILOVEVODKA 2 years, 12 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/ D - for sure

fojta 2 years, 12 months ago

Selected Answer: C

By using a security group as the source for the Reachability Analyzer path, you can ensure that traffic originating from any IP address within that security group is able to reach the application on the specified port. This allows you to test connectivity from multiple potential sources, rather than just a single IP address.

Jotoval 2 years, 12 months ago

should be D, c is not possible the sources are Instances Internet gateways Network interfaces Transit gateways Transit gateway attachments VPC endpoint services VPC endpoints VPC peering connections VPN gateways

ILOVEVODKA 3 years ago

https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/

study_aws1 3 years ago

It should be option D) The question requires - "automate a way to verify the network connectivity between the public internet and the EC2 instances", not just on failed connections. By implementing automated reachability assessment using Reachability Analyzer, application issues due to connectivity problems are detected quickly. Below post demonstrates an automated method to verify network connectivity between VPC elements after an infrastructure change is made, and alert administrators in the event reachability has been affected. https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/ Application load Balancer is supported as intermediary path in the reachability analyzer It is option D)

https://zhangxuetu.online

[202610]

Question #46 Topic 1

A security team is performing an audit of a company's AWS deployment. The security team is concerned that two applications might be accessing resources that should be blocked by network ACLs and security groups. The applications are deployed across two Amazon Elastic Kubernetes Service (Amazon EKS) clusters that use the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes. The clusters are in separate subnets within the same VPC and have a Cluster Autoscaler configured.
The security team needs to determine which POD IP addresses are communicating with which services throughout the VPC. The security team wants to limit the number of flow logs and wants to examine the traffic from only the two applications.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create VPC flow logs in the default format. Create a filter to gather flow logs only from the EKS nodes. Include the srcaddr field and the dstaddr field in the flow logs.

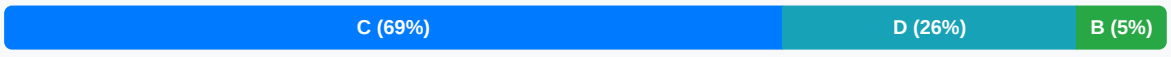
B. Create VPC flow logs in a custom format. Set the EKS nodes as the resource Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.

C. Create VPC flow logs in a custom format. Set the application subnets as resources. Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs. **Most Voted**

D. Create VPC flow logs in a custom format. Create a filter to gather flow logs only from the EKS nodes. Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.

Correct Answer: C

Community vote distribution



Comments

rhinozD Highly Voted 2 years, 11 months ago

Selected Answer: C

You cannot set the EKS nodes as the resource of a VPC flow log. So B is wrong. I think C and D are also correct. But "The security team wants to limit the number of flow logs and wants to examine the traffic from only the two applications", so it is easier to set the resource of the VPC flow logs to the subnets of the two clusters. So answer is C.

johnconnor 2 years, 7 months ago

He is right, you can only use IPs. see > https://aws.amazon.com/blogs/networking-and-content-delivery/using-vpc-flow-logs-to-capture-and-query-eks-network-communications/

Neo00 2 years, 8 months ago

D doesn't say set EKS node as VPC flow log source, it says create a filter based on EKS node, don't be tricked. so Answer is D

ILOVEVODKA Highly Voted 3 years ago

B https://aws.amazon.com/blogs/networking-and-content-delivery/using-vpc-flow-logs-to-capture-and-query-eks-network-communications/

Joselito79 2 months, 2 weeks ago

Selected Answer: D

D Custom format, filter on EKS nodes, pkt-srcaddr/pkt-dstaddr Correct. Captures pod-to-service traffic (required by security audit). Minimizes number of flow logs by filtering on application nodes. Operationally simple: no extra subnets or node tagging needed beyond filtering for EKS nodes.

woorkim 1 year, 5 months ago

C , because node can not be loggged!

Jonalb 1 year, 9 months ago

Selected Answer: C

its corret is C

vikasj1in 2 years, 1 month ago

Selected Answer: D

Creating VPC flow logs in a custom format allows you to specify the fields you want to include in the logs, reducing the volume of data and focusing on the specific information needed. By setting a filter to gather flow logs only from the EKS nodes, you can narrow down the logs to the traffic generated by the EKS nodes. Including the pkt-srcaddr (source IP address) and pkt-dstaddr (destination IP address) fields in the flow logs enables the security team to examine traffic from specific applications running on the EKS nodes. Options A, B, and C involve creating flow logs with different configurations but do not specifically address filtering traffic from only the two applications or minimizing operational overhead as effectively as option D.

Spaurito 1 year, 4 months ago

D - you can only capture from ENI and filter with IP addresses. Subnets are not a resource and can not be monitored. It's a place holder for IP Addresses.

marfee 2 years, 1 month ago

I think that it's correcty answer is D.

jopaca1216 2 years, 4 months ago

With a simple google, i found the correct answer. C is correct.
https://docs.aws.amazon.com/cli/latest/reference/ec2/create-flow-logs.html

Arad 2 years, 4 months ago

Selected Answer: C

I think the right answer is C. we cannot filter VPC flow logs based on EKS worker nodes (so option D is wrong), but we can create VPC flow logs based on subnets as resource, so option C is correct.

neotusca 2 years, 5 months ago

I'm C. You can't setting filter with EKS-node in vpcflowlogs. It's trick. You'll see just all, accept, rejct.

Certified101 2 years, 7 months ago

Selected Answer: C

When you create a VPC Flow Log, you can choose to create it for a specific VPC, Subnet, or Network Interface. Therefore, in the context of AWS VPC flow logs, creating a filter to gather flow logs only from the EKS nodes (as stated in option D) is not feasible. Because the two applications are deployed in separate subnets within the same VPC, the best way to capture only the traffic related to these applications is to create flow logs for those specific subnets where the applications are deployed. Therefore, option C remains the most suitable choice.

AdamWest 2 years, 10 months ago

Selected Answer: C

C The other options are less efficient: Option A doesn't allow to focus on just the application traffic. Option B and D would include the traffic from all applications running on the EKS nodes, not just the two applications of interest. So, the option that fulfills the requirement with the least operational overhead is Option C.

confusedyeti69 2 years, 2 months ago

You assume there are other applications running on the EKS nodes but not the possibility of other resources in the application subnet??

AdamWest 2 years, 10 months ago

Selected Answer: C

C - You cannot set EKS nodes a the resource of a VPC flow log.

Chinmoy 2 years, 10 months ago

Selected Answer: C

Eks Node can’t be specified in VPC log filter

sjoe 2 years, 11 months ago

Option C , is correct . Application Pods can take IPs from both subnets

Kristin01 2 years, 11 months ago

why not B?

dremm 2 years, 11 months ago

Selected Answer: D

I think D) is correct. CNI plug in adds IPs to the PODs which we can then filter in the VPC Flow logs via pkt-srcaddr. "The Amazon VPC CNI plugin for Kubernetes add-on is deployed on each Amazon EC2 node in your Amazon EKS cluster. The add-on creates elastic network interfaces and attaches them to your Amazon EC2 nodes. The add-on also assigns a private IPv4 or IPv6 address from your VPC to each pod and service." - https://docs.aws.amazon.com/eks/latest/userguide/managing-vpc-cni.html

sudipta0007 2 years, 3 months ago

D is not correct as its said in question that cluster autoscaller (not HPA) is configured so EKS cluster can launched new done . So Ip of the node is not static due to scaleout event .

that1guy 2 years, 11 months ago

"EKS nodes" is not a directly supported resource by VPC flow logs. "The clusters are in separate subnets within the same VPC..." easiest is to just enable flow logs for the whole subnet, otherwise you would have to enable it for each ENI individually. See: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

that1guy 2 years, 11 months ago

To clarify, the answer is C

linuxek21 2 years, 11 months ago

To add to the above: The Amazon VPC CNI plugin for Kubernetes add-on is deployed on each Amazon EC2 node in your Amazon EKS cluster. The add-on creates elastic network interfaces and attaches them to your Amazon EC2 nodes. If we select only specific ENIs of the nodes for the VPC flow log, we will need to come back again when there are new ENIs added.

study_aws1 2 years, 11 months ago

Bang on!!! The wording in the question "....have a Cluster Autoscaler configured" itself indicates we cannot consider EKS node as a resource even if we read "EKS nodes" and "EKS nodes ENI" in option B). Option C) looks good.

https://zhangxuetu.online

[202610]

Question #47 Topic 1

A data analytics company has a 100-node high performance computing (HPC) cluster. The HPC cluster is for parallel data processing and is hosted in a VPC in the AWS Cloud. As part of the data processing workflow, the HPC cluster needs to perform several DNS queries to resolve and connect to Amazon RDS databases, Amazon S3 buckets, and on-premises data stores that are accessible through AWS Direct Connect. The HPC cluster can increase in size by five to seven times during the company's peak event at the end of the year.
The company is using two Amazon EC2 instances as primary DNS servers for the VPC. The EC2 instances are configured to forward queries to the default VPC resolver for Amazon Route 53 hosted domains and to the on-premises DNS servers for other on-premises hosted domain names. The company notices job failures and finds that DNS queries from the HPC cluster nodes failed when the nodes tried to resolve RDS and S3 bucket endpoints.
Which architectural change should a network engineer implement to provide the DNS service in the MOST scalable way?

A. Scale out the DNS service by adding two additional EC2 instances in the VPC. Reconfigure half of the HPC cluster nodes to use these new DNS servers. Plan to scale out by adding additional EC2 instance-based DNS servers in the future as the HPC cluster size grows.

B. Scale up the existing EC2 instances that the company is using as DNS servers. Change the instance size to the largest possible instance size to accommodate the current DNS load and the anticipated load in the future.

C. Create Route 53 Resolver outbound endpoints. Create Route 53 Resolver rules to forward queries to on-premises DNS servers for on premises hosted domain names. Reconfigure the HPC cluster nodes to use the default VPC resolver instead of the EC2 instance-based DNS servers. Terminate the EC2 instances. **Most Voted**

D. Create Route 53 Resolver inbound endpoints. Create rules on the on-premises DNS servers to forward queries to the default VPC resolver. Reconfigure the HPC cluster nodes to forward all DNS queries to the on-premises DNS servers. Terminate the EC2 instances.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Raphaello **Highly Voted** 1 year, 11 months ago

Selected Answer: C

Focus on the ask, do not get distracted by trivial inputs. We need to keep queries forwarded to on-prem DNS, all while using "AWSProvidedDNS" (replacing EC2-based DNS with Route 53 resolver)..and to do that we need resolver outbound endpoint. C is the correct answer.

bcx Highly Voted 2 years, 8 months ago

Selected Answer: C

The VPC+2 addresses that those two EC2-based DNS use have a limit of 1024 queries per second. So we must get rid of them. We use the route 53 resolver, and for that we need an outgoing endpoint that can forwards queries to the omp-prem zones.

woorkim 1 year, 5 months ago

c is correct!

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

Arad 2 years, 4 months ago

Selected Answer: C

Definitely C.

ITgeek 2 years, 11 months ago

Selected Answer: C

CCCC is correct

study_aws1 3 years ago

It is C)

helloworldabc 3 years ago

CCCCCCCCC

zaazanuna 3 years ago

C - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #48 Topic 1

A company's network engineer is designing an active-passive connection to AWS from two on-premises data centers. The company has set up AWS Direct Connect connections between the on-premises data centers and AWS. From each location, the company is using a transit VIF that connects to a Direct Connect gateway that is associated with a transit gateway.
The network engineer must ensure that traffic from AWS to the data centers is routed first to the primary data center. The traffic should be routed to the failover data center only in the case of an outage.
Which solution will meet these requirements?

A. Set the BGP community tag for all prefixes from the primary data center to 7224:7100. Set the BGP community tag for all prefixes from the failover data center to 7224:7300

B. Set the BGP community tag for all prefixes from the primary data center to 7224:7300. Set the BGP community tag for all prefixes from the failover data center to 7224:7100 **Most Voted**

C. Set the BGP community tag for all prefixes from the primary data center to 7224:9300. Set the BGP community tag for all prefixes from the failover data center to 7224:9100

D. Set the BGP community tag for all prefixes from the primary data center to 7224:9100. Set the BGP community tag for all prefixes from the failover data center to 7224:9300

Correct Answer: B

Community vote distribution

B (100%)

Comments

zaazanuna Highly Voted 3 years ago

B - correct. Option B is the correct solution. Set the BGP community tag for all prefixes from the primary data center to 7224:7300, and set the BGP community tag for all prefixes from the failover data center to 7224:7100. This way, the primary data center will have a lower BGP local preference, making it the preferred path. If there is an outage in the primary data center, the failover data center will have a higher BGP local preference and will become the preferred path. The other options do not provide the correct community tag values for the primary and failover data centers.

woorkim 1 year, 5 months ago

B to coltrol inbound traffic, LP has to be used!

Raphaello 1 year, 11 months ago

Selected Answer: B

Correct answer is B. TGW + DxGW (transit VIF), so the BGP community tags in use are 7224:7100/7200/7300, with 7300 is the highest priority and takes precedence, therefore to be used with primary DC.

tromyunpak 2 years ago

B is the correct answer 7224:7300 has the highest priority whilst 7224:7100 has the lowest (7224:7X BGP communities are used for private/transit vifs) A is wrong since the priority is wrong whilst the correct tag 7X00 were used C&D are since the 7224:9X BGP communities are used for public vifs

tromyunpak 2 years ago

C&D are wrong

vikasj1in 2 years, 1 month ago

Selected Answer: B

BGP community tags are used to influence routing decisions. In this case, the tags are set differently for the primary and failover data centers. Setting the BGP community tag for all prefixes from the primary data center to 7224:7300 indicates a preference for routing through the primary data center. Setting the BGP community tag for all prefixes from the failover data center to 7224:7100 indicates that this is a failover route and should only be used in the case of an outage. This configuration ensures that traffic is routed to the primary data center by default and only fails over to the secondary data center in case of an outage in the primary data center.

yorkicurke 2 years, 2 months ago

Selected Answer: B

C & D: are using 7224:9XX which are for Public VIFs

Certified101 2 years, 7 months ago

Selected Answer: B

https://repost.aws/knowledge-center/direct-connect-bgp-communities Direct Connect supports local preference BGP community tags to control the route preference of traffic on private and transit virtual interfaces. Direct Connect supports the following local preference BGP communities: 7224:7100 Low preference, 7224:7200 Medium preference, and 7224:7300 High preference1. Direct Connect evaluates local preference BGP community tags from lowest to highest preference. For each prefix that you advertise over a BGP session, you can apply a community tag to indicate the associated path's priority for returning traffic1.

PTLS 2 years, 11 months ago

Selected Answer: B

BBBBBBBB

that1guy 2 years, 11 months ago

See section "Local preference BGP communities" from:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

that1guy 2 years, 11 months ago

To clarify, the answer is B

study_aws1 3 years ago

It is B)

helloworldabc 3 years ago

BBBBBBBBBBB

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #49 Topic 1

A real estate company is building an internal application so that real estate agents can upload photos and videos of various properties. The application will store these photos and videos in an Amazon S3 bucket as objects and will use Amazon DynamoDB to store corresponding metadata. The S3 bucket will be configured to publish all PUT events for new object uploads to an Amazon Simple Queue Service (Amazon SQS) queue.
A compute cluster of Amazon EC2 instances will poll the SQS queue to find out about newly uploaded objects. The cluster will retrieve new objects, perform proprietary image and video recognition and classification update metadata in DynamoDB and replace the objects with new watermarked objects. The company does not want public IP addresses on the EC2 instances.
Which networking design solution will meet these requirements MOST cost-effectively as application usage increases?

A. Place the EC2 instances in a public subnet. Disable the Auto-assign Public IP option while launching the EC2 instances. Create an internet gateway. Attach the internet gateway to the VPC. In the public subnet's route table, add a default route that points to the internet gateway.

B. Place the EC2 instances in a private subnet. Create a NAT gateway in a public subnet in the same Availability Zone. Create an internet gateway. Attach the internet gateway to the VPC. In the public subnet's route table, add a default route that points to the internet gateway

C. Place the EC2 instances in a private subnet. Create an interface VPC endpoint for Amazon SQS. Create gateway VPC endpoints for Amazon S3 and DynamoDB. **Most Voted**

D. Place the EC2 instances in a private subnet. Create a gateway VPC endpoint for Amazon SQS. Create interface VPC endpoints for Amazon S3 and DynamoDB.

Correct Answer: C

Community vote distribution

C (100%)

Comments

woorkim 1 year, 5 months ago

YES, C!!!!!

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer.

tromyunpak 2 years ago

C is the right answer as using gw endpoints for s3 and dynamodb and interface endpoint for sqs and the ec2 are in the private subnet. A is wrong due to the public subnet. B is a good option but not cost effective so the answer is wrong. D is wrong due to the gateway endpoint of sqs (only s3 and dynamodb are gateway endpoints)

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

Arad 2 years, 4 months ago

Selected Answer: C

definitely C.

habros 2 years, 5 months ago

Selected Answer: C

SQS: no choice, only interface endpoint (cost $ but negligible compared to S3/DynamoDB) S3/DynamoDB: Gateway endpoints $0.00 for endpoint use. C all the way

neotusca 2 years, 5 months ago

C : SQS interface endpoint(free), S3 & DynamoDB gateway endpoint D : SQS gateway endpoint, S3 & DynamoDB interface endpoint(free) think about data size of SQS vs data size of S3 & DynamoDB

neotusca 2 years, 5 months ago

The comment above is wrong, I hope it gets deleted.

neotusca 2 years, 5 months ago

Sorry.. The 'free' sign is reversed.

Scunningham99 2 years, 6 months ago

C interface endpoint https://docs.aws.amazon.com/vpc/latest/privatelink/aws-services-privatelink-support.html gateway not supported service https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html

Mishranihal737 2 years, 7 months ago

Answer will be C - > To access S3 , Dynamo DB you need Gateway Endpoints.

ITgeek 2 years, 11 months ago

Selected Answer: C

C is the most Cost effective and less complicated

zaazanuna 2 years, 12 months ago

Actually D. because Gateway Endpoint is free of charge vs Interface Endpoint

ohcan 2 years, 11 months ago

GW endpoint works only with S3 and DynamoDB.

helloworldabc 3 years ago

CCCCCCCCCC

zaazanuna 3 years ago

C - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #50 Topic 1

A company has an AWS Direct Connect connection between its on-premises data center in the United States (US) and workloads in the us-east-1 Region. The connection uses a transit VIF to connect the data center to a transit gateway in us-east-1.
The company is opening a new office in Europe with a new on-premises data center in England. A Direct Connect connection will connect the new data center with some workloads that are running in a single VPC in the eu-west-2 Region. The company needs to connect the US data center and us-east-1 with the Europe data center and eu-west-2. A network engineer must establish full connectivity between the data centers and Regions with the lowest possible latency.
How should the network engineer design the network architecture to meet these requirements?

A. Connect the VPC in eu-west-2 with the Europe data center by using a Direct Connect gateway and a private VIF. Associate the transit gateway in us-east-1 with the same Direct Connect gateway. Enable SiteLink for the transit VIF and the private VIF.

B. Connect the VPC in eu-west-2 to a new transit gateway. Connect the Europe data center to the new transit gateway by using a Direct Connect gateway and a new transit VIF. Associate the transit gateway in us-east-1 with the same Direct Connect gateway. Enable SiteLink for both transit VIFs. Peer the two transit gateways. Most Voted

C. Connect the VPC in eu-west-2 to a new transit gateway. Connect the Europe data center to the new transit gateway by using a Direct Connect gateway and a new transit VIF. Create a new Direct Connect gateway. Associate the transit gateway in us-east-1 with the new Direct Connect gateway. Enable SiteLink for both transit VIFs. Peer the two transit gateways.

D. Connect the VPC in eu-west-2 with the Europe data center by using a Direct Connect gateway and a private VIF. Create a new Direct Connect gateway. Associate the transit gateway in us-east-1 with the new Direct Connect gateway. Enable SiteLink for the transit VIF and the private VIF.

Correct Answer: B

Community vote distribution

B (100%)

Comments

study_aws1 Highly Voted 3 years ago

B) is correct. Below link (Figure 9) explains. https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-direct-connect-sitelink/

AzureDP900 1 year, 2 months ago

Option B is correct Here's why: Connecting the VPC in eu-west-2 to a new transit gateway (Option B) allows the network engineer to create a separate logical connection between the two Regions. This provides better isolation and control over traffic flow. The Europe data center connects to the new transit gateway by using a Direct Connect gateway and a new transit VIF. This establishes a direct, private connection between the data centers, reducing latency and improving performance. Associating the transit gateway in us-east-1 with the same Direct Connect gateway enables SiteLink between the two Regions. This allows traffic to move seamlessly between the data centers, even if they are not directly connected by a VIF. Enabling SiteLink for both transit VIFs ensures that traffic can be routed correctly between the regions. The other options do not provide the same level of isolation and control over traffic flow as Option B.

Spaurito 1 year, 4 months ago

C - looks to be the answer. It states a new Direct connect is being created and you have to associate the DX to the existing, not use the same DX.

1a17d1e 9 months, 2 weeks ago

I agree with this. You want them attached to the same Direct Connect if you want to use SiteLink and says the US already has a Direct Connect. Wouldn't that be "with the same Direct Connect gateway", thus keeping them on its original (thus separate) Direct Connects? C says "with the new Direct Connect gateway" which would be the Direct Connect created for EU, attaching them to the same Direct Connect?

woorkim 1 year, 5 months ago

its B!

6ad97eb 1 year, 9 months ago

Associate the transit gateway in us-east-1 with the same Direct Connect gateway. Enable SiteLink for both transit VIFs This is not even required

Raphaello 1 year, 11 months ago

Selected Answer: B

B is the correct answer. One DxGW can connect to up to 6 TGW in different accounts and regions. SiteLink will enable the on-prem DC's to communicate via DxGW and the underlying DX connection. Peering TGW will ensure VPC's in the 2 AWS regions connect.

tromyunpak 2 years ago

The answer is B - C&D are wrong. Sitelink works if the vifs are using the same DXGW. A caters to the on-premises connectivity but not the VPC connectivity since there is no TGW in eu-west-2

marfee 2 years, 1 month ago

I think that it's correcty answer is B.

Arad 2 years, 4 months ago

Selected Answer: B

B is correct answer.

Mishranihal737 2 years, 7 months ago

Yes B is correct

Certified101 2 years, 7 months ago

Selected Answer: B

Options A, C, and D are not suitable as they do not fully satisfy the requirements, especially regarding achieving the lowest possible latency. For instance, option A does not provide for peering between the two transit gateways, and

options C and D suggest the use of multiple Direct Connect gateways which is not necessary and could potentially introduce more latency and complexity to the setup.

DeathFrmAbv 2 years, 8 months ago

was hard to decide between A and B as both have One direct connect gateway (least hops), in the case of A it was associated with private VIF whereas B is transit VIF. Since transit gateway seems best practice architecture (even through the EU region has 1 VPC only), I go with B.

rhinozD 2 years, 11 months ago

Selected Answer: B

I think C is also doable even the SiteLink part won't help. But the traffic can go around via the Transit Gateway peering. However, C costs you more money and it gets higher latency than B. The answer is B.

study_aws1 2 years, 10 months ago

Option C) & D) will not work as DC connectivity through Sitelink will require the same Direct Connect gateway. The reason transit gateway peering is used is to connect VPCs in 2 regions as per the question. That is why option B), else option A) would have made it.

printfmarcelo 2 years, 11 months ago

Selected Answer: B

i agree with zaazanuna B - correct. This solution creates a new transit gateway in the eu-west-2 Region and connects it to the VPC in that Region.

helloworldabc 3 years ago

BBBBBBBBBBBBBB

zaazanuna 3 years ago

B - correct. This solution creates a new transit gateway in the eu-west-2 Region and connects it to the VPC in that Region. The Europe data center is connected to the new transit gateway using a Direct Connect gateway and a new transit VIF. The transit gateway in us-east-1 is associated with the same Direct Connect gateway, and both transit VIFs are enabled with SiteLink. The two transit gateways are then peered, allowing full connectivity between the data centers and Regions with the lowest possible latency. This solution is cost-effective and efficient as it does not require creating a new Direct Connect gateway.

https://zhangxuetu.online

[202610]

Question #51 Topic 1

A network engineer has deployed an Amazon EC2 instance in a private subnet in a VPC. The VPC has no public subnet. The EC2 instance hosts application code that sends messages to an Amazon Simple Queue Service (Amazon SQS) queue. The subnet has the default network ACL with no modification applied. The EC2 instance has the default security group with no modification applied.
The SQS queue is not receiving messages.
Which of the following are possible causes of this problem? (Choose two.)

A. The EC2 instance is not attached to an IAM role that allows write operations to Amazon SQS. Most Voted

B. The security group is blocking traffic to the IP address range used by Amazon SQS

C. There is no interface VPC endpoint configured for Amazon SQS Most Voted

D. The network ACL is blocking return traffic from Amazon SQS

E. There is no route configured in the subnet route table for the IP address range used by Amazon SQS

Correct Answer: AC

Community vote distribution

AC (100%)

Comments

study_aws1 Highly Voted 3 years ago

It is A) and C) A - EC2 requires IAM role that allows write operations to Amazon SQS C - Being in private subnet, interface endpoint is required to access SQS

Mr_Marcus 2 years, 12 months ago

A - Agreed. See Note at top of page. https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-examples-of-iam-policies.html C - Agreed. https://www.linkedin.com/pulse/aws-interface-endpoint-vs-gateway-alex-chang/

dremm Highly Voted 2 years, 11 months ago

Selected Answer: AC

A and C are correct. C - VPC has no public subnet , therefore VPC interface endpoint is needed to get to SQS A- IAM roles are also needed for write operations B- Incorrect , default SG allows 0.0.0.0/0 on any port for outbound traffic from EC2 D- Incorrect, Network ACL allows 0.0.0.0/0 inbound by default E- Incorrect, Amazon SQS uses interface endpoint (privatelink), so no routes are needed in the routing table unlike Gateway Endpoints.

rhinozD 2 years, 11 months ago

D - Incorrect, By default, Network ACL allows all inbound and OUTBOUND IPv4 traffic, if applicable, IPv6 traffic. I agree with you on the others.

Spaurito 1 year, 4 months ago

Option C and E - These are all on private subnets. NACL's untouched and should allow all in/outbound traffic by default. SQS being a public service, and no IGW, and you have to create the SQS endpoint, then you need to have a route for the connectivity. This makes the most sense.

Spaurito 1 year, 4 months ago

Changing to AC. Even on private subnets should have no impact

woorkim 1 year, 5 months ago

a &c for correct answer!

Raphaello 1 year, 11 months ago

Selected Answer: AC

AC are the correct answers.

Arad 2 years, 4 months ago

Selected Answer: AC

For sure A and C.

Mishranihal737 2 years, 7 months ago

Yes A & C are correct. E is incorrect as Routes are needed for gateway endpoints only.

sp237 2 years, 7 months ago

A and C https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-sending-messages-from-vpc.html

ITgeek 2 years, 11 months ago

Selected Answer: AC

A and C are correct

devopsbro 3 years ago

switching to A and C.

devopsbro 3 years ago

CD - Need VPC interface endpoint to communicate with SQS from private subnet. Default NACL will block all the inbound traffic.

helloworldabc 3 years ago

BBBBBBBEEEEEEE

Mr_Marcus 2 years, 12 months ago

B is wrong. The default security group allows all outbound traffic, until modified. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/default-custom-security-groups.html#default-security-group

zaazanuna 3 years ago

B, E - correct. B. The security group is blocking traffic to the IP address range used by Amazon SQS: By default, Amazon SQS uses the Amazon S3 endpoint for the region. If the default security group applied to the instance is blocking outbound traffic to the Amazon S3 endpoint, then the EC2 instance cannot send messages to the Amazon SQS queue. E. There is no route configured in the subnet route table for the IP address range used by Amazon SQS:

The EC2 instance in the private subnet requires a route to the Amazon SQS endpoint. If there is no route configured in the subnet route table, then the traffic will not be able to reach the Amazon SQS service.

rhinozD 2 years, 11 months ago

Both B and E are wrong. B: No, SG allows all outbound traffic. E: No, Event if you use the SQS Endpoint, it is an interface endpoint and you don't need to modify route table.

Mr_Marcus 2 years, 12 months ago

B is wrong. The default security group allows all outbound traffic, until modified.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/default-custom-security-groups.html#default-security-group

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #52 Topic 1

A network engineer needs to standardize a company's approach to centralizing and managing interface VPC endpoints for private communication with AWS services. The company uses AWS Transit Gateway for inter-VPC connectivity between AWS accounts through a hub-and-spoke model. The company's network services team must manage all Amazon Route 53 zones and interface endpoints within a shared services AWS account. The company wants to use this centralized model to provide AWS resources with access to AWS Key Management Service (AWS KMS) without sending traffic over the public internet.
What should the network engineer do to meet these requirements?

A. In the shared services account, create an interface endpoint for AWS KMS. Modify the interface endpoint by disabling the private DNS name. Create a private hosted zone in the shared services account with an alias record that points to the interface endpoint. Associate the private hosted zone with the spoke VPCs in each AWS account. **Most Voted**

B. In the shared services account, create an interface endpoint for AWS KMS. Modify the interface endpoint by disabling the private DNS name. Create a private hosted zone in each spoke AWS account with an alias record that points to the interface endpoint. Associate each private hosted zone with the shared services AWS account.

C. In each spoke AWS account, create an interface endpoint for AWS KMS. Modify each interface endpoint by disabling the private DNS name. Create a private hosted zone in each spoke AWS account with an alias record that points to each interface endpoint. Associate each private hosted zone with the shared services AWS account.

D. In each spoke AWS account, create an interface endpoint for AWS KMS. Modify each interface endpoint by disabling the private DNS name. Create a private hosted zone in the shared services account with an alias record that points to each interface endpoint. Associate the private hosted zone with the spoke VPCs in each AWS account.

Correct Answer: A

Community vote distribution

A (100%)

Comments

zaazanuna **Highly Voted** 3 years ago

A - correct. Option A is the correct answer because it creates a private hosted zone in the shared services account with an alias record that points to the interface endpoint, and associates the private hosted zone with the spoke VPCs in each AWS account. Disabling the private DNS name of the interface endpoint ensures that DNS resolution of the

endpoint is restricted to the Amazon Route 53 private hosted zone. This option creates a centralized model for managing interface endpoints and Route 53 zones in a shared services AWS account, which simplifies administration and reduces complexity.

AzureDP900 1 year, 2 months ago

Selected Answer: A

Option A creates a private hosted zone in the shared services account with an alias record that points to the interface endpoint. This allows DNS resolution of the endpoint to be restricted to the Amazon Route 53 private hosted zone. By disabling the private DNS name of the interface endpoint, DNS resolution is further restricted to only the private hosted zone, which prevents traffic from leaking out onto the public internet. Associating the private hosted zone with the spoke VPCs in each AWS account ensures that all network traffic destined for the interface endpoint is routed through the shared services account. This centralized model simplifies administration and reduces complexity by allowing a single point of management for all interface endpoints and Route 53 zones in the shared services account.

woorkim 1 year, 5 months ago

A is answer!!!

Raphaello 1 year, 11 months ago

Selected Answer: A

A is the correct answer. Instead of using the service-created private hosted zone that is associated with the endpoint creation, we you need to manually create it to have the flexibility of sharing it with other VPC's. That is done by disabling private dns name for the endpoint.

marfee 2 years, 1 month ago

I think that it's correcty answer is A.

Arad 2 years, 4 months ago

Selected Answer: A

A is the right answer.

rhinozD 2 years, 11 months ago

Selected Answer: A

Yeah, A - no doubt.

silviahdz 2 years, 11 months ago

Selected Answer: A

+ A is correct.

ITgeek 2 years, 11 months ago

Selected Answer: A

A is correct because it centralizes in the shared service and VPC

study_aws1 3 years ago

A - correct

helloworldabc 3 years ago

AAAAAAAAAAA

https://zhangxuetu.online

[202610]

Question #53 Topic 1

A development team is building a new web application in the AWS Cloud. The main company domain, example.com, is currently hosted in an Amazon Route 53 public hosted zone in one of the company's production AWS accounts.
The developers want to test the web application in the company's staging AWS account by using publicly resolvable subdomains under the example.com domain with the ability to create and delete DNS records as needed. Developers have full access to Route 53 hosted zones within the staging account, but they are prohibited from accessing resources in any of the production AWS accounts.
Which combination of steps should a network engineer take to allow the developers to create records under the example com domain? (Choose two.)

A. Create a public hosted zone for example com in the staging account

B. Create a staging example.com NS record in the example.com domain. Populate the value with the name servers from the staging.example.com domain. Set the routing policy type to simple routing. Most Voted

C. Create a private hosted zone for staging example com in the staging account.

D. Create an example com NS record in the staging example.com domain. Populate the value with the name servers from the example.com domain. Set the routing policy type to simple routing.

E. Create a public hosted zone for staging.example.com in the staging account. Most Voted

Correct Answer: BE

Community vote distribution



Comments

that1guy Highly Voted 2 years, 11 months ago

Selected Answer: BE

When a client queries a DNS server for a domain name, the DNS server typically starts by looking for NS records to determine which name servers are authoritative for the domain. The DNS server then queries the authoritative name servers to obtain the information about the domain that the client requested. For example, suppose you own the domain example.com, but you want to delegate control of the subdomain sub.example.com to a different set of name servers. You would create NS records in the example.com zone file that point to the name servers for sub.example.com. This tells DNS servers that the name servers for sub.example.com are authoritative for that subdomain, and they should query those name servers for any requests related to sub.example.com.

study_aws1 Highly Voted 3 years ago

It is a case of sub-domain delegation, not split DNS. Hence, option B) and E) are correct

deepakno 8 months, 3 weeks ago

Selected Answer: DE

Developers are prohibited from accessing resources in any of the production AWS accounts. So how B is possible?

woorkim 1 year, 5 months ago

B &E The other options are incorrect because: A: Creating a public hosted zone for example.com in the staging account would conflict with the existing zone in the production account. C: A private hosted zone would not be publicly resolvable, which is a requirement. D: Creating an NS record for example.com in the staging zone would be incorrect as the staging zone should not control the parent domain.

vikasj1in 2 years, 1 month ago

Selected Answer: AE

Option A creates a public hosted zone for the main example.com domain in the staging account, giving developers the ability to create records under the example.com domain. Option E creates a separate public hosted zone for staging.example.com in the staging account, providing a dedicated space for developers to create and manage subdomains for testing. Options B, C, and D are not necessary for achieving the goal of allowing developers to create records under the example.com domain in the staging account while being isolated from production AWS accounts.

Spaurito 1 year, 4 months ago

The public hosted zone is already created in a production account so this would cause a conflict.

marfee 2 years, 1 month ago

I think that it's correcty answer is BE.

Certified101 2 years, 7 months ago

Selected Answer: BE

Options A, C, and D are not correct because they either conflict with the existing Route 53 setup (A), involve creating a private zone which wouldn't be publicly resolvable (C), or reverse the direction of the NS record delegation (D).

titi_r 2 years, 12 months ago

Selected Answer: BE

B and E - correct. A - incorrect, the Devs must be able to modify the sub-domains of example.com, but not the root domain itself.

ILOVEVODKA 3 years ago

Yea, B and E. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingNewSubdomain.html

ILOVEVODKA 2 years, 12 months ago

I will swap to AB

helloworldabc 3 years ago

AAAAAAAABBBBBBB

zaazanuna 3 years ago

A, B - correct. Explanation: Creating a public hosted zone for example.com in the staging account will allow the developers to create DNS records under the example.com domain for testing purposes without impacting the production environment. Creating a staging.example.com NS record in the example.com domain and populating it with the name servers from the staging.example.com domain will delegate authority for the staging.example.com subdomain to the staging account, allowing the developers to create and delete DNS records for that subdomain as needed. The routing policy should be set to simple routing to return the results of the DNS query based on the values in the resource record sets.

rhinozD 2 years, 11 months ago

No, A is wrong. If you want a public sub-domain in the staging account. You have to create that sub-domain public hosted zone in the staging account, NOT recreate the domain in the product account(example.com.)

Spaurito 1 year, 4 months ago

I agree. My point was you can't have in the Staging and production Acct's simultaniously

Spaurito 1 year, 4 months ago

Option A will create a conflict with the Production Account. Option B would be done after Option E is done to allow for the requirement.

https://zhangxuetu.online

[202610]

Question #54 Topic 1

A company plans to deploy a two-tier web application to a new VPC in a single AWS Region. The company has configured the VPC with an internet gateway and four subnets. Two of the subnets are public and have default routes that point to the internet gateway. Two of the subnets are private and share a route table that does not have a default route.
The application will run on a set of Amazon EC2 instances that will be deployed behind an external Application Load Balancer. The EC2 instances must not be directly accessible from the internet. The application will use an Amazon S3 bucket in the same Region to store data. The application will invoke S3 GET API operations and S3 PUT API operations from the EC2 instances. A network engineer must design a VPC architecture that minimizes data transfer cost.
Which solution will meet these requirements?

A. Deploy the EC2 instances in the public subnets. Create an S3 interface endpoint in the VPC. Modify the application configuration to use the S3 endpoint-specific DNS hostname.

B. Deploy the EC2 instances in the private subnets. Create a NAT gateway in the VPC. Create default routes in the private subnets to the NAT gateway. Connect to Amazon S3 by using the NAT gateway.

C. Deploy the EC2 instances in the private subnets. Create an S3 gateway endpoint in the VPSpecify die route table of the private subnets during endpoint creation to create routes to Amazon S3. Most Voted

D. Deploy the EC2 instances in the private subnets. Create an S3 interface endpoint in the VPC. Modify the application configuration to use the S3 endpoint-specific DNS hostname.

Correct Answer: C

Community vote distribution



Comments

attal Highly Voted 2 years, 10 months ago

Selected Answer: C

C is correct. Recurring questions about gateway VPC endpoints (https://repost.aws/knowledge-center/vpc-reduce-nat-gateway-transfer-costs)

ShinLi 2 years, 5 months ago

Cost: Gateway endpoints for S3 are offered at no cost and the routes are managed through route tables. Interface endpoints are priced at $0.01/per AZ/per hour. Cost depends on the Region, check current pricing. Data transferred through the interface endpoint is charged at $0.01/per GB (depending on Region).

zaazanuna Highly Voted 3 years ago

C - correct. Option C is the optimal solution as it involves deploying the EC2 instances in the private subnets, which provides additional security benefits. Additionally, creating an S3 gateway endpoint in the VPC will enable the EC2 instances to communicate with Amazon S3 directly, without incurring data transfer costs. This is because the S3 gateway endpoint uses Amazon's private network to transfer data between the VPC and S3, which is not charged for data transfer. Furthermore, specifying the route table of the private subnets during endpoint creation will create routes to Amazon S3, which is required for the EC2 instances to communicate with S3.

woorkim 1 year, 5 months ago

its c!

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. EC2 in private subnet, accessing S3 via gateway endpoint that has no additional cost.

jinu 2 years ago

if go for D. Reason being that you need your EC2 instances to remain in a private subnet and based on https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html, the feature for interface endpoint is that it Uses private IP addresses from your VPC to access Amazon S3

1a17d1e 9 months, 2 weeks ago

Reading the link jinu provided I have to agree and choose D. MY original answer was C specifically because I thought you needed a GW endpoint S3 but the link says otherwise.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

marfee 2 years, 1 month ago

I think that it's correcty answer is C.

Arad 2 years, 4 months ago

Selected Answer: C

C is the right answer.

Manh 2 years, 7 months ago

Selected Answer: B

The solution that minimizes data transfer cost is to deploy the EC2 instances in the private subnets and create an S3 interface endpoint in the VPC. The S3 interface endpoint will allow the EC2 instances to access Amazon S3 without having to go through the internet gateway, which will minimize data transfer cost. The application configuration will need to be modified to use the S3 endpoint-specific DNS hostname.

takecoffe 2 years, 9 months ago

Selected Answer: C

C is the correct. s3 gateway endpoint

tcp22 2 years, 10 months ago

C for sure

rhinozD 2 years, 11 months ago

Selected Answer: A

C - no doubt.

study_aws1 3 years ago

C - Correct

helloworldabc 3 years ago

CCCCCCCCCCCCCCC

https://zhangxuetu.online

[202610]

Question #55 Topic 1

A company has two AWS accounts one for Production and one for Connectivity. A network engineer needs to connect the Production account VPC to a transit gateway in the Connectivity account. The feature to auto accept shared attachments is not enabled on the transit gateway.
Which set of steps should the network engineer follow in each AWS account to meet these requirements?

A. 1. In the Production account: Create a resource share in AWS Resource Access Manager for the transit gateway. Provide the Connectivity account ID. Enable the feature to allow external accounts
2. In the Connectivity account: Accept the resource.
3. In the Connectivity account: Create an attachment to the VPC subnets.
4. In the Production account: Accept the attachment. Associate a route table with the attachment.

B. 1. In the Production account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Connectivity account ID. Enable the feature to allow external accounts.
2. In the Connectivity account: Accept the resource.
3. In the Production account: Create an attachment on the transit gateway to the VPC subnets.
4. In the Connectivity account: Accept the attachment. Associate a route table with the attachment.

C. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Production account ID. Enable the feature to allow external accounts.
2. In the Production account: Accept the resource.
3. In the Connectivity account: Create an attachment on the transit gateway to the VPC subnets.
4. In the Production account: Accept the attachment. Associate a route table with the attachment.

D. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the transit gateway. Provide the Production account ID Enable the feature to allow external accounts.
2. In the Production account: Accept the resource.
3. In the Production account: Create an attachment to the VPC subnets.
4. In the Connectivity account: Accept the attachment. Associate a route table with the attachment. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

awsguru1998 **Highly Voted** 2 years, 11 months ago

D, although zaazanuna has got this dump from somewhere they are posting all ChatGPT hallucination responses

study_aws1 Highly Voted 3 years ago

It is D). The transit gateway is owned by Connectivity account, and it is the production account who will create a VPC attachmennt to the TGW post resource share by Connectivity account through AWS RAM.

Spaurito 1 year, 4 months ago

D, The Connectivity Acct owns the transit gateway and needs to create the create the share.

woorkim 1 year, 5 months ago

its D!

Raphaello 1 year, 11 months ago

Selected Answer: D

D is the correct answer. The logical answer.

vikasj1in 2 years, 1 month ago

Selected Answer: D

In option D, the resource share is created in the Connectivity account for the transit gateway, and the Production account ID is provided. This allows the Production account to accept the shared transit gateway resource. In step 3, the attachment is created in the Production account for the VPC subnets. The Connectivity account then accepts the attachment, and a route table is associated with the attachment to manage the routing. Options A, B, and C have the steps in a different order or involve sharing VPC subnets directly, which is not the typical approach for connecting a VPC to a transit gateway in another account.

marfee 2 years, 1 month ago

I think that it's correct answer is D.

Arad 2 years, 4 months ago

Selected Answer: D

definitely D.

tcp22 2 years, 10 months ago

D for sure.

awser7 2 years, 11 months ago

Selected Answer: D

D is correct

dremm 2 years, 11 months ago

Selected Answer: D

D is correct, the first step is to share the TGW From the Connectivity account to the Production account, making all the other options incorrect.

ILOVEVODKA 2 years, 12 months ago

D for sure: https://repost.aws/knowledge-center/transit-gateway-sharing

helloworldabc 3 years ago

A Correct

zaazanuna 3 years ago

A - correct. Step 1: In the Production account, create a resource share in AWS Resource Access Manager for the transit gateway and provide the Connectivity account ID. Enabling the feature to allow external accounts is also required to share resources between accounts. Step 2: In the Connectivity account, accept the shared resource. This action will allow the Production account to use the transit gateway in the Connectivity account. Step 3: In the Connectivity account, create an attachment to the VPC subnets. This attachment will enable communication between the VPC in the Production account and the transit gateway in the Connectivity account. Step 4: In the Production account, accept the attachment and associate a route table with the attachment. This will enable the VPC to route traffic through the transit gateway to other resources in the Connectivity account.

https://zhangxuetu.online

[202610]

Question #56 Topic 1

A company is running multiple workloads on Amazon EC2 instances in public subnets. In a recent incident, an attacker exploited an application vulnerability on one of the EC2 instances to gain access to the instance. The company fixed the application and launched a replacement EC2 instance that contains the updated application. The attacker used the compromised application to spread malware over the internet. The company became aware of the compromise through a notification from AWS. The company needs the ability to identify when an application that is deployed on an EC2 instance is spreading malware.
Which solution will meet this requirement with the LEAST operational effort?

A. Use Amazon GuardDuty to analyze traffic patterns by inspecting DNS requests and VPC flow logs. **Most Voted**

B. Use Amazon GuardDuty to deploy AWS managed decoy systems that are equipped with the most recent malware signatures.

C. Set up a Gateway Load Balancer. Run an intrusion detection system (IDS) appliance from AWS Marketplace on Amazon EC2 for traffic inspection.

D. Configure Amazon Inspector to perform deep packet inspection of outgoing traffic.

Correct Answer: A

Community vote distribution



Comments

ITgeek **Highly Voted** 2 years, 11 months ago

Selected Answer: A

the emphasis is on the efforts to stand out a solution, that is where guarduty can help in identify

zaazanuna **Highly Voted** 3 years ago

A - correct. This solution involves using Amazon GuardDuty to monitor network traffic and analyze DNS requests and VPC flow logs for suspicious activity. This will allow the company to identify when an application is spreading malware by monitoring the network traffic patterns associated with the instance. GuardDuty is a fully managed threat detection service that continuously monitors for malicious activity and unauthorized behavior in your AWS accounts and workloads. It requires minimal setup and configuration and can be integrated with other AWS services for automated remediation. This solution requires the least operational effort compared to the other options

AzureDP900 1 year, 2 months ago

Selected Answer: A

Amazon GuardDuty is a service that analyzes network traffic patterns and detects malicious activity in real-time. It can be configured to inspect DNS requests and VPC flow logs, which would provide the necessary visibility into applications running on EC2 instances. By using Amazon GuardDuty, the company can identify potential malware-related activity without having to implement additional infrastructure or configuration changes. This solution requires minimal operational effort as it leverages an existing AWS service.

woorkim 1 year, 5 months ago

A B. AWS managed decoy systems (honeypots) are not the most appropriate or least effort solution for identifying malware spread from EC2 instances. C. Gateway Load Balancer with an IDS appliance from AWS Marketplace is a more complex setup, requiring manual configuration, management, and scaling. D. Amazon Inspector is primarily focused on vulnerability assessments rather than inspecting outgoing traffic for malware.

Raphaello 1 year, 11 months ago

Selected Answer: A

GuardDuty is AWS intelligent threat detection, which I think the answer to the ask in this scenario. However, option C (GWLB + IDS) is not entirely wrong, apart from "operational effort" part.

patanjali 2 years ago

Selected Answer: A

LEAST operational effort is only using GuardDuty. GWLB option is another way to do this too but that involve lots of operational overhead and lots of config/routing change.

marfee 2 years, 1 month ago

I think that it's correct answer is A.

JoseCC 2 years, 7 months ago

A - correct https://aws.amazon.com/blogs/aws/new-for-amazon-guardduty-malware-detection-for-amazon-ebs-volumes/

Mishranihal737 2 years, 7 months ago

Yes correct answer is A

silviahdz 2 years, 11 months ago

Selected Answer: A

A is the right choice as it requires less effort.

dremm 2 years, 11 months ago

Selected Answer: C

C is correct. Although GuardDuty can detect malware infected machines, it cannot prevent spreading. This options requires Malware Protection to be enabled on GuardDuty which is not mentioned in the answers. DNS queries and VPC flow logs will not help in detecting malware spread. C is the most logical answer here.

that1guy 2 years, 11 months ago

> "Although GuardDuty can detect malware infected machines, it cannot prevent spreading." This isn't an requirement from the question: "The company needs the ability to *identify* when an application that is deployed on an EC2 instance is spreading malware."

dremm 2 years, 11 months ago

You are right, switching to A)

helloworldabc 3 years ago

AAAAAAAAAAA

https://zhangxuetu.online

[202610]

Question #57 Topic 1

A company deploys a new web application on Amazon EC2 instances. The application runs in private subnets in three Availability Zones behind an Application Load Balancer (ALB). Security auditors require encryption of all connections. The company uses Amazon Route 53 for DNS and uses AWS Certificate Manager (ACM) to automate SSL/TLS certificate provisioning. SSL/TLS connections are terminated on the ALB.
The company tests the application with a single EC2 instance and does not observe any problems. However, after production deployment, users report that they can log in but that they cannot use the application. Every new web request restarts the login process.
What should a network engineer do to resolve this issue?

A. Modify the ALB listener configuration. Edit the rule that forwards traffic to the target group. Change the rule to enable group-level stickiness. Set the duration to the maximum application session length.

B. Replace the ALB with a Network Load Balancer. Create a TLS listener. Create a new target group with the protocol type set to TLS Register the EC2 instances. Modify the target group configuration by enabling the stickiness attribute.

C. Modify the ALB target group configuration by enabling the stickiness attribute. Use an application-based cookie. Set the duration to the maximum application session length. Most Voted

D. Remove the ALB. Create an Amazon Route 53 rule with a failover routing policy for the application name. Configure ACM to issue certificates for each EC2 instance.

Correct Answer: C

Community vote distribution

C (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: C

To resolve this issue, the network engineer needs to enable session persistence in the Application Load Balancer (ALB) so that subsequent requests from the same client IP address are directed to the same target instance. This is known as "sticky sessions" or "session persistence." By enabling sticky sessions and using an application-based cookie, the ALB can direct all subsequent HTTP requests from a client with a specific IP address to the same EC2 instance that handled the initial request. This ensures that the user remains logged in without requiring them to re-enter their credentials for every new request.

woorkim 1 year, 5 months ago

C is correct!

vikasj1in 2 years, 1 month ago

Selected Answer: C

Enabling stickiness at the target group level helps maintain session affinity for clients, directing them consistently to the same target within the target group. Using an application-based cookie for stickiness ensures that the session information is maintained based on the application's session management mechanism. Setting the duration to the maximum application session length ensures that the stickiness persists for the entire session. Option A suggests group-level stickiness, but it doesn't mention the use of application-based cookies, which are crucial for maintaining session information. Option B recommends replacing the ALB with a Network Load Balancer, which might not be necessary to address the session management issue. Option D suggests removing the ALB, which is not a viable solution for providing load balancing and SSL termination for web applications.

marfee 2 years, 1 month ago

I think that It's correct answer is C.

marfee 2 years, 1 month ago

I think that It's correct answer is C.

yorkicurke 2 years, 2 months ago

Selected Answer: C

Application-based Cookies * Custom cookie • Generated by the target • Can include any custom attributes required by the application * Application cookie • Generated by the load balancer • Cookie name is AWSALBAPP ; Should be used if you need sticky sessions across all layers Duration-based Cookies • Cookie generated by the load balancer • Cookie name is AWSALB for ALB, AWSELB for CLB

kaikin 2 years, 4 months ago

Answer is C

Cheam 2 years, 6 months ago

Selected Answer: C

Sticky sessions via the ALB is done via cookies. The source of the cookies can come from: 1) The application itself 2) Or the ALB Ref: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html All the best.

qsergii 2 years, 8 months ago

Why should use an application-based cookie?

ExamTopix01 2 years, 7 months ago

Option C is incorrect because it describes duration-based cookies.
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html

ExamTopix01 2 years, 7 months ago

The question statement does not mention cookies, so the answer is option A.

ITgeek 2 years, 11 months ago

Selected Answer: C

C for Cookie Stickiness

titi_r 2 years, 12 months ago

Selected Answer: C

C. https://aws.amazon.com/about-aws/whats-new/2021/02/application-load-balancer-supports-application-cookie-stickiness/

helloworldabc 3 years ago

CCCCCCC

zaazanuna 3 years ago

C - correct

https://zhangxuetu.online

[202610]

Question #58 Topic 1

A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway for internet access. After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses. The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue?

A. Configure the NAT gateway timeout to allow connections for up to 600 seconds.

B. Enable enhanced networking on the client EC2 instances.

C. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds. Most Voted

D. Close idle TCP connections through the NAT gateway.

Correct Answer: C

Community vote distribution

C (100%)

Comments

study_aws1 Highly Voted 2 years, 6 months ago

https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-troubleshooting.html#nat- gateway- troubleshooting-timeout It is Option C)

tcp22 Highly Voted 2 years, 4 months ago

C Problem Your instances can access the internet, but the connection drops after 350 seconds. Cause If a connection that's using a NAT gateway is idle for 350 seconds or more, the connection times out. When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet). Solution To prevent the connection from being dropped, you can initiate more traffic over the connection. Alternatively, you can enable TCP keepalive on the instance with a value less than 350 seconds.

8e0b117 1 year, 1 month ago

Selected Answer: C

you cant modify the nat gateway idle timeout

AzureDP900 1 year, 2 months ago

Selected Answer: C

This will help prevent the NAT gateway from dropping the connection too early, allowing the long-running queries to complete and return any necessary response data.

marfee 1 year, 7 months ago

I think that It's correct answer is C.

that1guy 2 years, 5 months ago

Selected Answer: C

See section "Internet connection drops after 350 seconds" from https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-troubleshooting.html

ITgeek 2 years, 5 months ago

Selected Answer: C

C is correct

helloworldabc 2 years, 6 months ago

CCCCCCCCC

zaazanuna 2 years, 6 months ago

C - correct. When a TCP connection is idle for a long time, it may be terminated by network devices, including the NAT gateway. By enabling TCP keepalive, the client EC2 instances can periodically send packets to the third-party database to indicate that the connection is still active, preventing it from being terminated prematurely.

https://zhangxuetu.online

[202610]

Question #59 Topic 1

A company uses AWS Direct Connect to connect its corporate network to multiple VPCs in the same AWS account and the same AWS Region. Each VPC uses its own private VIF and its own virtual LAN on the Direct Connect connection. The company has grown and will soon surpass the limit of VPCs and private VIFs for each connection.
What is the MOST scalable way to add VPCs with on-premises connectivity?

A. Provision a new Direct Connect connection to handle the additional VPCs. Use the new connection to connect additional VPCs.

B. Create virtual private gateways for each VPC that is over the service quota. Use AWS Site-to-Site VPN to connect the virtual private gateways to the corporate network.

C. Create a Direct Connect gateway, and add virtual private gateway associations to the VPCs. Configure a private VIF to connect to the corporate network.

D. Create a transit gateway, and attach the VPCs. Create a Direct Connect gateway, and associate it with the transit gateway. Create a transit VIF to the Direct Connect gateway. Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Comments

tcp22 Highly Voted 2 years, 10 months ago

D for sure using DXGW with TGW allow you to also be flexible in case of expanding to new regions with more TGW in those regions.

woorkim 1 year, 5 months ago

D is only answer!

mousomgogoi 1 year, 8 months ago

why so many and are wrong, or getting contradictory

Raphaello 1 year, 11 months ago

Selected Answer: D

Correct answer is D. 1 DxGW can connect to up to 6 TGW. Each TGW can connect to thousands of VPCs (5000 attachments).

marfee 2 years, 1 month ago

I think that It's correct answer is D.

marfee 2 years, 1 month ago

I think that it's correct answer is D.

Arad 2 years, 4 months ago

Selected Answer: D

For sure D.

DeathFrmAbv 2 years, 8 months ago

D no brainer

silviahdz 2 years, 11 months ago

Selected Answer: D

D is the more scalable.

ITgeek 2 years, 11 months ago

Selected Answer: D

D transit GW

ohcan 2 years, 11 months ago

Selected Answer: D

D is much scalable

dremm 2 years, 11 months ago

D is correct. TGW and DXG provide the most scaling.

helloworldabc 3 years ago

DDDDDDDDDDD

zaazanuna 3 years ago

D - correct. When a company requires connectivity to multiple VPCs over AWS Direct Connect, a scalable solution is to use a transit gateway. A transit gateway is a hub that can interconnect multiple VPCs and VPN connections. The VPCs can communicate with each other over the transit gateway, and on-premises networks can communicate with the VPCs through the Direct Connect gateway. This solution provides a central point of management and simplifies the configuration of network routing. By associating the Direct Connect gateway with the transit gateway, traffic between the VPCs and the on-premises network can be routed through the Direct Connect connection.

https://zhangxuetu.online

[202610]

Question #60 Topic 1

A network engineer is designing a hybrid architecture that uses a 1 Gbps AWS Direct Connect connection between the company's data center and two AWS Regions: us-east-1 and eu-west-1. The VPCs in us-east-1 are connected by a transit gateway and need to access several on-premises databases. According to company policy, only one VPC in eu-west-1 can be connected to one on-premises server. The on-premises network segments the traffic between the databases and the server.
How should the network engineer set up the Direct Connect connection to meet these requirements?

A. Create one hosted connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use one Direct. Connect gateway for both VIFs to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

B. Create one hosted connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use two Direct Connect gateways, one for each VIF, to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

C. Create one dedicated connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use one Direct Connect gateway for both VIFs to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

D. Create one dedicated connection. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use two Direct Connect gateways, one for each VIF, to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

that1guy **Highly Voted** 2 years, 11 months ago

Selected Answer: D

A and B are wrong, Direct Connect *hosted* connections only support 1 VIF per connection, see: https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html C is wrong, see: https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-gateways.html > "You cannot attach a Direct Connect gateway to a transit gateway when the Direct Connect gateway is already associated with a virtual private gateway or is attached to a private virtual interface."

Mishranihal737 2 years, 7 months ago

But we can do the other way round, connect to tgw first and then to vgw ?

Tofu13 2 years, 6 months ago

As Mishranihal737 pointed out, the other way round should be possible, so imo the above explanation for why C is wrong is misleading, while still providing the right answer (D). Beyond statements are the key to solve the problem: 1. "VPCs in us-east-1 are connected by a transit gateway and need to access several on-premises databases" 2. "only one VPC in eu-west-1 can be connected to one on-premises server" Hence, the VPCs in us-east-1 are not allowed to access the server. Using only one DX gateway would break with the requirement described in 2. and break with the segmentation of DB and server, because: "A Direct Connect gateway is a globally available resource. You can connect to any Region globally using a Direct Connect gateway." https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

Raphaello 1 year, 11 months ago

Well put.

titi_r Highly Voted 2 years, 12 months ago

Selected Answer: D

A and B - wrong: a hosted connection supports a single VIF only. C - wrong: you cannot attach both a private VIF and a transit VIF to the same transit GW. D - correct.

Mr_Marcus 2 years, 12 months ago

Supporting A&B being wrong. https://help.mulesoft.com/s/article/Can-t-Create-More-Than-1-Virtual-Interface-VIF-In-A-Direct-Connect

AzureDP900 1 year, 2 months ago

Selected Answer: D

This setup meets the requirements as follows: The dedicated connection allows for a more direct and secure connection between the on-premises network and the AWS Regions. Using two separate Direct Connect gateways, one for each VIF, ensures that traffic is routed to the corresponding AWS Region along the path with the lowest latency. This setup also allows for better isolation and security of the on-premises networks, as each connection is dedicated to a specific region.

woorkim 1 year, 5 months ago

D is correct!

Raphaello 1 year, 11 months ago

Selected Answer: D

D is the correct answer. You cannot attach a Direct Connect gateway to a transit gateway when the Direct Connect gateway is already associated with a virtual private gateway or is attached to a private virtual interface.

marfee 2 years, 1 month ago

I think that It's correct answer is D.

Arad 2 years, 4 months ago

Selected Answer: D

D is the right answer.

DeathFrmAbv 2 years, 8 months ago

D is the answer, but ideally in real life I would just use a transit gateway in the EU region as well and connect them to the same direct connect gateway instead of having to use two direct connect gateways due to mixing up private VIFS

with transit VIFS

study_aws1 3 years ago

One Hosted connection only supports a single VIF, not two VIFs. Option D) is the answer.

helloworldabc 3 years ago

BBBBBBBBBB

zaazanuna 3 years ago

B - correct. This solution meets the requirements of the company by using a single Direct Connect connection with two VIFs, one connected to the transit gateway in us-east-1 and the other connected to the VPC in eu-west-1. Two Direct Connect gateways are used, one for each VIF, to route traffic from the Direct Connect location to the corresponding AWS Region along the path that has the lowest latency. This setup ensures that traffic between the VPCs in us-east-1 and on-premises databases is routed through the transit gateway, while traffic between the VPC in eu-west-1 and the on-premises server is routed directly through the private VIF.

Spaurito 1 year, 4 months ago

B is correct. This meets the requirements.

Spaurito 1 year, 4 months ago

D - have to change. As per that1guy said, hosted connection only supports 1 VIF

https://zhangxuetu.online

[202610]

Question #61 Topic 1

A company has deployed an application in a VPC that uses a NAT gateway for outbound traffic to the internet. A network engineer notices a large quantity of suspicious network traffic that is traveling from the VPC over the internet to IP addresses that are included on a deny list. The network engineer must implement a solution to determine which AWS resources are generating the suspicious traffic. The solution must minimize cost and administrative overhead.
Which solution will meet these requirements?

A. Launch an Amazon EC2 instance in the VPC. Use Traffic Mirroring by specifying the NAT gateway as the source and the EC2 instance as the destination. Analyze the captured traffic by using open-source tools to identify the AWS resources that are generating the suspicious traffic.

B. Use VPC flow logs. Launch a security information and event management (SIEM) solution in the VPC. Configure the SIEM solution to ingest the VPC flow logs. Run queries on the SIEM solution to identify the AWS resources that are generating the suspicious traffic.

C. Use VPC flow logs. Publish the flow logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the flow logs to identify the AWS resources that are generating the suspicious traffic. Most Voted

D. Configure the VPC to stream the network traffic directly to an Amazon Kinesis data stream. Send the data from the Kinesis data stream to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Athena to query the data to identify the AWS resources that are generating the suspicious traffic.

Correct Answer: C

Community vote distribution

C (100%)

Comments

study_aws1 Highly Voted 2 years, 6 months ago

C) ensures - The solution must minimize cost and administrative overhead

vikasj1in Highly Voted 1 year, 7 months ago

Selected Answer: C

VPC flow logs capture information about the IP traffic going to and from network interfaces in a VPC. They provide details such as source and destination IP addresses, ports, and protocols. Publishing the VPC flow logs to a log group in Amazon CloudWatch Logs (Option C) allows for centralized and easy access to the flow log data. CloudWatch Logs Insights can be used to query the flow logs efficiently and identify the AWS resources that are generating the

suspicious traffic. This solution minimizes cost by leveraging existing AWS services (CloudWatch Logs) and has lower administrative overhead compared to setting up custom streaming solutions (such as Amazon Kinesis) or deploying additional instances (as in Option A). Options A, B, and D introduce additional complexity and may have higher associated costs or administrative overhead compared to using CloudWatch Logs Insights for analyzing VPC flow logs.

Raphaello 1 year, 5 months ago

Selected Answer: C

C is the correct answer. VPC flow logs (with custom format to have "pkt-srcaddr" & "pkt-dstaddr" since it goes via NAT GW). Direct it to CloudWatch Logs, and use CW Logs Insights for querying and visualization.

Arad 1 year, 11 months ago

Selected Answer: C

C is the correct answer.

bcx 2 years, 2 months ago

Selected Answer: C

No doubt it is C, it is simple to implement (even temporarily) and is affordable.

Wiss7 2 years, 2 months ago

Selected Answer: C

Lowest cost

ITgeek 2 years, 5 months ago

Selected Answer: C

C is the simples

ohcan 2 years, 5 months ago

Selected Answer: C

C. " The solution must minimize cost and administrative overhead."

helloworldabc 2 years, 6 months ago

CCCCCCCCC

zaazanuna 2 years, 6 months ago

C - correct.

https://zhangxuetu.online

[202610]

Question #62 Topic 1

A company has its production VPC (VPC-A) in the eu-west-1 Region in Account 1. VPC-A is attached to a transit gateway (TGW-A) that is connected to an on-premises data center in Dublin, Ireland, by an AWS Direct Connect transit VIF that is configured for an AWS Direct Connect gateway. The company also has a staging VPC (VPC-B) that is attached to another transit gateway (TGW-B) in the eu-west-2 Region in Account 2.
A network engineer must implement connectivity between VPC-B and the on-premises data center in Dublin.
Which solutions will meet these requirements? (Choose two.)

A. Configure inter-Region VPC peering between VPC-A and VPC-B. Add the required VPC peering routes. Add the VPC-B CIDR block in the allowed prefixes on the Direct Connect gateway association.

B. Associate TGW-B with the Direct Connect gateway. Advertise the VPC-B CIDR block under the allowed prefixes. Most Voted

C. Configure another transit VIF on the Direct Connect connection and associate TGW-B. Advertise the VPC-B CIDR block under the allowed prefixes.

D. Configure inter-Region transit gateway peering between TGW-A and TGW-B. Add the peering routes in the transit gateway route tables. Add both the VPC-A and the VPC-B CIDR block under the allowed prefix list in the Direct Connect gateway association. Most Voted

E. Configure an AWS Site-to-Site VPN connection over the transit VIF to TGW-B as a VPN attachment.

Correct Answer: BD

Community vote distribution



Comments

study_aws1 Highly Voted 3 years ago

Only one Transit VIF is possible with one Direct connection. With DX gateway, 3 Transit Gateways (same or different regions) can be added. Option B) and D) are correct, though B) itself fulfils the requirement in the question.

JoseCC 2 years, 7 months ago

Regarding option D) the documentation states that you can use up to 6 TGW per DX gateway. AWS Direct Connect quotas.

leotoras 2 years, 2 months ago

The number of transit virtual interfaces allowed is now four (4) and is counted against the maximum of 51 virtual interfaces per dedicated connection. This limit cannot be increased. This limit cannot be increased. Contact your Solutions Architect (SA) or Technical Account Manager (TAM) for further assistance.

zaazanuna Highly Voted 3 years ago

B, C - correct. B. Associate TGW-B with the Direct Connect gateway. Advertise the VPC-B CIDR block under the allowed prefixes. This will allow traffic from VPC-B to be sent over the Direct Connect connection to the on-premises data center via TGW-B. C. Configure another transit VIF on the Direct Connect connection and associate TGW-B. Advertise the VPC-B CIDR block under the allowed prefixes. This will enable the use of the Direct Connect connection for VPC-B's traffic by connecting TGW-B to the Direct Connect gateway.

ChinkSantana 2 years, 2 months ago

C did not mention Direct Connect Gateway which is an important component for C to work so C is out of the debate.

Joselito79 2 months, 2 weeks ago

Selected Answer: BD

B: Direct association of TGW-B with Direct Connect gateway → direct, simplest path. D: Inter-region peering → allows traffic to flow via TGW-A if needed (additional path, supports multi-account, cross-region). Note: Option B is simpler operationally if Direct Connect gateway supports multiple TGWs in the same region/account scope; Option D adds inter-region resilience.

Geetar 1 year ago

Selected Answer: AD

TGW is a regional resource therefore without a direct connect gateway you can't attach/associate the TGW to the transit vif. Hence the janky the peering being the way.

dspd 1 year, 2 months ago

Selected Answer: B

only B is require. Why even need D as question does not ask connectivity between both the VPCs

dspd 1 year, 2 months ago

Selected Answer: A

Only A is require. Why even need D as question does not ask connectivity between both the VPCs

dspd 1 year, 2 months ago

sorry only B is require. Why even need D as question does not ask connectivity between both the VPCs

AzureDP900 1 year, 2 months ago

Selected Answer: BD

The correct reasons why options B and D are the correct answers: B. Associate TGW-B with the Direct Connect gateway. Advertise the VPC-B CIDR block under the allowed prefixes. This solution provides a direct connection between VPC-B and the on-premises data center in Dublin via the existing Direct Connect gateway. D. Configure inter-Region transit gateway peering between TGW-A and TGW-B. Add the peering routes in the transit gateway route tables. Add both the VPC-A and the VPC-B CIDR block under the allowed prefix list in the Direct Connect gateway association. This solution provides a connection between the two transit gateways, allowing for connectivity between VPC-A and VPC-B, which can then be extended to the on-premises data center in Dublin via the Direct Connect gateway.

woorkim 1 year, 5 months ago

Valid Solutions: The two correct solutions are: B: Associate TGW-B with Direct Connect gateway because: Direct Connect gateway supports multiple transit gateway associations Works across regions Simple and direct path D: Configure inter-Region transit gateway peering because: Allows communication between transit gateways Can route traffic through existing Direct Connect setup Provides flexibility for future expansion

rltk8029 1 year, 11 months ago

They testing your English here, C looks fine but missing *gateway** -- instead it says Direct Connect *connection**. if it would say "gateway", then C would be more optimal -- each TGW connected to DXGW.

Raphaello 1 year, 11 months ago

Selected Answer: BD

BD are the correct answers. 2 TGW's (each in its own region, with peering between them) + 1 DxGW (with transit VIF) + DX connection (to the company's DC)

marfee 2 years, 1 month ago

I think that it's correct answer is BD.

MarcosSantos 2 years, 2 months ago

The question seems poorly formatted to me: It should contain only one answer, as it only asks for communication between the TGW-B and the On-Premises, and not the connectivity between the vpcs. "A network engineer must implement connectivity between VPC-B and the on-premises data center in Dublin. Which solutions will meet these requirements?" For me the letter B is correct

kaush4u 2 years, 1 month ago

IT should be BE , B is correct .There is no requirement to connect VPCs in Question, Also E is also a possible solution

dremm 2 years, 11 months ago

Selected Answer: BD

B) D) It's not an option of which 2 steps are required to achieve the connectivity, but which 2 solutions can achieve the same result, thus B,D

silviahdz 2 years, 11 months ago

Selected Answer: BD

B & D Correct, implementing either will work.

Jotoval 2 years, 12 months ago

i think B and D considering 1 direct connect connection only can have 1 Transit VIF

helloworldabc 3 years ago

BBBBBBCCCCCCC

https://zhangxuetu.online

[202610]

Question #63 Topic 1

A company's network engineer is designing a hybrid DNS solution for an AWS Cloud workload. Individual teams want to manage their own DNS hostnames for their applications in their development environment. The solution must integrate the application-specific hostnames with the centrally managed DNS hostnames from the on-premises network and must provide bidirectional name resolution. The solution also must minimize management overhead.

Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Use an Amazon Route 53 Resolver inbound endpoint. Most Voted

B. Modify the DHCP options set by setting a custom DNS server value.

C. Use an Amazon Route 53 Resolver outbound endpoint. Most Voted

D. Create DNS proxy servers.

E. Create Amazon Route 53 private hosted zones. Most Voted

F. Set up a zone transfer between Amazon Route 53 and the on-premises DNS.

Correct Answer: ACE

Community vote distribution

ACE (100%)

Comments

study_aws1 Highly Voted 2 years, 6 months ago

For bidirectional name resolution, both Route 53 Resolver inbound & outbound endpoint is required. It is A), C), E)

silviahdz Highly Voted 2 years, 5 months ago

Selected Answer: ACE

Second study_aws1

Raphaello 1 year, 5 months ago

Selected Answer: ACE

ACE are the correct answers. To ensure bidirectional name resolution, both resolver inbound and outbound endpoints are required, and private hosted zone for individual team to be able to manage their DNS records. +forwarding rules.

marfee 1 year, 7 months ago

I think that it's correct answer is ACE.

Arad 1 year, 11 months ago

Selected Answer: ACE

For sure ACE.

ITgeek 2 years, 5 months ago

Selected Answer: ACE

ACE are correct

ILOVEVODKA 2 years, 6 months ago

ACE https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/

helloworldabc 2 years, 6 months ago

AAAABBBBEEEE

zaazanuna 2 years, 6 months ago

A, B, E - correct.

https://zhangxuetu.online

[202610]

Question #64 Topic 1

A company hosts a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin in an Amazon CloudFront distribution. The company wants to implement a custom authentication system that will provide a token for its authenticated customers.
The web application must ensure that the GET/POST requests come from authenticated customers before it delivers the content. A network engineer must design a solution that gives the web application the ability to identify authorized customers.
What is the MOST operationally efficient solution that meets these requirements?

A. Use the ALB to inspect the authorized token inside the GET/POST request payload. Use an AWS Lambda function to insert a customized header to inform the web application of an authenticated customer request.

B. Integrate AWS WAF with the ALB to inspect the authorized token inside the GET/POST request payload. Configure the ALB listener to insert a customized header to inform the web application of an authenticated customer request.

C. Use an AWS Lambda@Edge function to inspect the authorized token inside the GET/POST request payload. Use the Lambda@Edge function also to insert a customized header to inform the web application of an authenticated customer request. **Most Voted**

D. Set up an EC2 instance that has a third-party packet inspection tool to inspect the authorized token inside the GET/POST request payload. Configure the tool to insert a customized header to inform the web application of an authenticated customer request.

Correct Answer: C

Community vote distribution

C (100%)

Comments

titi_r Highly Voted 2 years, 12 months ago

Selected Answer: C

C) is correct. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions.html

woorkim 1 year, 5 months ago

only c is correct! Use when you need some of the capabilities of Lambda@Edge that aren't available with CloudFront Functions (e.g., longer execution time, network access, …)

Raphaello 1 year, 11 months ago

Selected Answer: C

C it the correct answer. Lambda@Edge (after viewer request/before origin request) can inspect cookies/authentication token, and perform function logic and redirection (to login page when needed).

marfee 2 years, 1 month ago

I think that It's correct answer is C.

Arad 2 years, 4 months ago

Selected Answer: C

C is correct answer.

Mishranihal737 2 years, 7 months ago

Yes c is correct

bala2021 2 years, 10 months ago

CUse an AWS Lambda@Edge function to inspect the authorized token inside the GET/POST request payload. Use the Lambda@Edge function also to insert a customized header to inform the web application of an authenticated customer request. C : Ans

ITgeek 2 years, 11 months ago

Selected Answer: C

C for the use of custom Lambdas

fojta 2 years, 12 months ago

AAAAAAAAAAAA

helloworldabc 3 years ago

CCCCCCCCCC

zaazanuna 3 years ago

C - correct.

https://zhangxuetu.online

[202610]

Question #65 Topic 1

A company has created three VPCs: a production VPC, a nonproduction VPC, and a shared services VPC. The production VPC and the nonproduction VPC must each have communication with the shared services VPC. There must be no communication between the production VPC and the nonproduction VPC. A transit gateway is deployed to facilitate communication between VPCs.
Which route table configurations on the transit gateway will meet these requirements?

A. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for only the shared services VPC. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs. **Most Voted**

B. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for each VPC. Create an additional route table with only the shared services VPC attachment associated with propagated routes from each VPC.

C. Configure a route table with all the VPC attachments associated with propagated routes for only the shared services VPCreate an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

D. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes disabled. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

Correct Answer: A

Community vote distribution



Comments

silviahdz **Highly Voted** 2 years, 11 months ago

Selected Answer: A

A, RT1 associated to spokes propagate Hub. RT2 associate to Hub and propagate spokes.

woorkim 1 year, 5 months ago

A is correct!

Raphaello 1 year, 11 months ago

Selected Answer: A

A is the correct answer. Instead of the TGW default route table, we now need to create 3 separate route tables. 1. prod with its route(s) propagated into it (via prod VPC attachment) 2. non-prod with its route(s) propagated into it (via non-prod VPC attachment) 3. shared with prod and non-prod route(s) propagated into it each via its respective attachment.

marfee 2 years, 1 month ago

I think that it's answer is A.

ITgeek 2 years, 11 months ago

Selected Answer: A

A is correct

study_aws1 3 years ago

A - correct

helloworldabc 3 years ago

AAAAAAAAAAAAAAA

zaazanuna 3 years ago

A - correct.

https://zhangxuetu.online

[202610]

Question #66 Topic 1

A company is using an AWS Site-to-Site VPN connection from the company's on-premises data center to a virtual private gateway in the AWS Cloud Because of congestion, the company is experiencing availability and performance issues as traffic travels across the internet before the traffic reaches AWS. A network engineer must reduce these issues for the connection as quickly as possible with minimum administration effort.
Which solution will meet these requirements?

A. Edit the existing Site-to-Site VPN connection by enabling acceleration. Stop and start the VPN service on the customer gateway for the new setting to take effect.

B. Configure a transit gateway in the same AWS Region as the existing virtual private gateway. Create a new accelerated Site-to-Site VPN connection. Connect the new connection to the transit gateway by using a VPN attachment. Update the customer gateway device to use the new Site to Site VPN connection. Delete the existing Site-to-Site VPN connection **Most Voted**

C. Create a new accelerated Site-to-Site VPN connection. Connect the new Site-to-Site VPN connection to the existing virtual private gateway. Update the customer gateway device to use the new Site-to-Site VPN connection. Delete the existing Site-to-Site VPN connection.

D. Create a new AWS Direct Connect connection with a private VIF between the on-premises data center and the AWS Cloud. Update the customer gateway device to use the new Direct Connect connection. Delete the existing Site-to-Site VPN connection.

Correct Answer: B

Community vote distribution



Comments

study_aws1 Highly Voted 3 years ago

B - correct Acceleration is only supported for Site-to-Site VPN connections that are attached to a transit gateway. Virtual private gateways do not support accelerated VPN connections.
https://docs.aws.amazon.com/vpn/latest/s2svpn/accelerated-vpn.html

woorkim 1 year, 5 months ago

B is correct TGW is required!

hedglin 1 year, 6 months ago

I was wrong. Correct answer is B Not C.

hedglin 1 year, 8 months ago

The correct answer is C. Option B is incorrect because it involves unnecessary steps of creating a transit gateway and using a VPN attachment. The question does not mention any requirement for a transit gateway.

hogtrough 1 year, 7 months ago

Correct answer is B. The transit gateway is required because acceleration is only allowed on S2S VPN through a Transit Gateway.

Raphaello 1 year, 11 months ago

Selected Answer: B

B is the correct answer. Accelerated site-to-site VPN is the usage of AWS Global Accelerator as an entry point to route traffic from your on-prem to AWS edge location that is closest to customer GW to avoid any congestions on the Internet. It only works with TGW.

JoellaLi 2 years ago

You cannot turn on or turn off acceleration for an existing Site-to-Site VPN connection. Instead, you can create a new Site-to-Site VPN connection with acceleration on or off as needed. Then, configure your customer gateway device to use the new Site-to-Site VPN connection and delete the old Site-to-Site VPN connection.

marfee 2 years, 1 month ago

I thin that It's correct answer is B.

skiingfalcon 2 years, 5 months ago

Selected Answer: B

Acceleration is only supported for Site-to-Site VPN connections that are attached to a transit gateway. Virtual private gateways do not support accelerated VPN connections. An Accelerated Site-to-Site VPN connection cannot be used with an AWS Direct Connect public virtual interface.

qsergii 2 years, 8 months ago

Selected Answer: B

B, others longer or not possible

DeathFrmAbv 2 years, 8 months ago

Its says congestion, performance issue. So why not D ?

DeathFrmAbv 2 years, 8 months ago

Sorry my bad, it says minimum administration effort as well

ITgeek 2 years, 11 months ago

Selected Answer: B

TCW plus VPN accelerated

ohcan 2 years, 11 months ago

Selected Answer: B

B. Accelerated VPN requires transit GW

helloworldabc 3 years ago

BBBBBBBBBBB

zaazanuna 3 years ago

B - correct.

https://zhangxuetu.online

[202610]

Question #67 Topic 1

An Australian ecommerce company hosts all of its services in the AWS Cloud and wants to expand its customer base to the United States (US). The company is targeting the western US for the expansion.
The company's existing AWS architecture consists of four AWS accounts with multiple VPCs deployed in the ap-southeast-2 Region. All VPCs are attached to a transit gateway in ap-southeast-2. There are dedicated VPCs for each application service. The company also has VPCs for centralized security features such as proxies, firewalls, and logging.
The company plans to duplicate the infrastructure from ap-southeast-2 to the us-west-1 Region. A network engineer must establish connectivity between the various applications in the two Regions. The solution must maximize bandwidth, minimize latency and minimize operational overhead.
Which solution will meet these requirements?

A. Create VPN attachments between the two transit gateways. Configure the VPN attachments to use BGP routing between the two transit gateways.

B. Peer the transit gateways in each Region. Configure routing between the two transit gateways for each Region's IP addresses. Most Voted

C. Create a VPN server in a VPC in each Region. Update the routing to point to the VPN servers for the IP addresses in alternate Regions.

D. Attach the VPCs in us-west-1 to the transit gateway in ap-southeast-2.

Correct Answer: B

Community vote distribution

B (100%)

Comments

woorkim 1 year, 5 months ago

B is correct!

Raphaello 1 year, 11 months ago

Selected Answer: B

B is the correct answer. TGW peering.

marfee 2 years, 1 month ago

I think that it's correct answer is B.

Arad 2 years, 4 months ago

Selected Answer: B

B, no brainer!

silviahdz 2 years, 11 months ago

Selected Answer: B

TGW peering with static routes.

ITgeek 2 years, 11 months ago

Selected Answer: B

TGW peering

study_aws1 3 years ago

B - correct. Only possible solution here is TGW peering and adding static routes for peering connection.

helloworldabc 3 years ago

BBBBBBBBBBBBBB

zaazanuna 3 years ago

B - seems to be more appropriate. Option B could be a possible solution, but it depends on the specific requirements and constraints of the company. Peering the transit gateways in each region would establish a private network connection between the two regions, allowing the company to route traffic between the VPCs in different regions without going over the public internet. This would help minimize latency and maximize bandwidth while reducing the operational overhead of managing multiple VPN connections.

https://zhangxuetu.online

[202610]

Question #68 Topic 1

An IoT company sells hardware sensor modules that periodically send out temperature, humidity, pressure, and location data through the MQTT messaging protocol. The hardware sensor modules send this data to the company's on-premises MQTT brokers that run on Linux servers behind a load balancer. The hardware sensor modules have been hardcoded with public IP addresses to reach the brokers.
The company is growing and is acquiring customers across the world. The existing solution can no longer scale and is introducing additional latency because of the company's global presence. As a result, the company decides to migrate its entire infrastructure from on premises to the AWS Cloud. The company needs to migrate without reconfiguring the hardware sensor modules that are already deployed across the world. The solution also must minimize latency.
The company migrates the MQTT brokers to run on Amazon EC2 instances.
What should the company do next to meet these requirements?

A. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listeners. Use Bring Your Own IP (BYOIP) from the on-premises network with the NLB.

B. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listeners. Create an AWS Global Accelerator accelerator in front of the NLUse Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator. Most Voted

C. Place the EC2 instances behind an Application Load Balancer (ALB). Configure TCP listeners. Create an AWS Global Accelerator accelerator in front of the ALB. Use Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator

D. Place the EC2 instances behind an Amazon CloudFront distribution. Use Bring Your Own IP (BYOIP) from the on-premises network with CloudFront.

Correct Answer: B

Community vote distribution

B (100%)

Comments

acloudguru Highly Voted 1 year, 10 months ago
I just met this question in yesterday's exam,.

woorkim 1 year, 5 months ago
it has to be B

Raphaello 1 year, 11 months ago
Selected Answer: B

B is the correct answer. AGA with BYOIP + NLB

vikasj1in 2 years, 1 month ago

Selected Answer: B

Using a Network Load Balancer (NLB) with TCP listeners allows the company to maintain compatibility with the existing hardware sensor modules that are already configured to send data via the MQTT protocol using public IP addresses. Creating an AWS Global Accelerator accelerator in front of the NLB provides a global anycast IP address, which can help minimize latency for the global user base. Using Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator allows the company to retain the public IP addresses hardcoded in the existing hardware sensor modules, eliminating the need for reconfiguration. Options A, C, and D do not provide the same level of compatibility with existing hardware sensor modules or may introduce unnecessary complexity.

marfee 2 years, 1 month ago

I think that it's correct answer is B.

Arad 2 years, 4 months ago

Selected Answer: B

B is correct answer.

MohamedSherif1 2 years, 7 months ago

Selected Answer: B

B. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listeners. Create an AWS Global Accelerator accelerator in front of the NLUse Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator.

JoseCC 2 years, 7 months ago

B) Global acelerador + NLB https://aws.amazon.com/blogs/iot/creating-static-ip-addresses-and-custom-domains-for-aws-iot-core-endpoints/

rhinozD 2 years, 10 months ago

Selected Answer: B

Refer this: https://www.hivemq.com/blog/running-hivemq-cluster-aws-auto-discovery/

silviahdz 2 years, 11 months ago

Selected Answer: B

B, we need global accelerator and there's no need for ALB.

awskiller007 2 years, 8 months ago

For my understanding - can you please explain why not C.

oldsport 2 years, 4 months ago

ALB. only has listeners on HTTP and HTTPS not TCP.

qsergii 2 years, 8 months ago

ALB is not necessary

ITgeek 2 years, 11 months ago

Selected Answer: B

Global accelerator

study_aws1 3 years ago

B - correct

helloworldabc 3 years ago

BBBBBBBBBB

zaazanuna 3 years ago

B - correct.

https://zhangxuetu.online

[202610]

Question #69 Topic 1

A company has deployed a web application on AWS. The web application uses an Application Load Balancer (ALB) across multiple Availability Zones. The targets of the ALB are AWS Lambda functions. The web application also uses Amazon CloudWatch metrics for monitoring.
Users report that parts of the web application are not loading properly. A network engineer needs to troubleshoot the problem. The network engineer enables access logging for the ALB.
What should the network engineer do next to determine which errors the ALB is receiving?

A. Send the logs to Amazon CloudWatch Logs. Review the ALB logs in CloudWatch Insights to determine which error messages the ALB is receiving.

B. Configure the Amazon S3 bucket destination. Use Amazon Athena to determine which error messages the ALB is receiving. **Most Voted**

C. Configure the Amazon S3 bucket destination. After Amazon CloudWatch Logs pulls the ALB logs from the S3 bucket automatically, review the logs in CloudWatch Logs to determine which error messages the ALB is receiving.

D. Send the logs to Amazon CloudWatch Logs. Use the Amazon Athena CloudWatch Connector to determine which error messages the ALB is receiving.

Correct Answer: B

Community vote distribution

B (100%)

Comments

devopsbro Highly Voted 2 years, 6 months ago

ELB doesn't have direct integration with CloudWatch. ELB can drop the logs in S3 bucket and Athena can be used to analyse the logs. Ans - B

study_aws1 Highly Voted 2 years, 6 months ago

Option B) is correct Access logs is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logs for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logs at any time.
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

AzureDP900 1 year, 2 months ago

Selected Answer: B

This solution meets the requirements of the network engineer as follows: Configuring an S3 bucket destination for log data allows the network engineer to capture and analyze log data from the ELB. Using Amazon Athena to query the

logs enables the network engineer to quickly identify error messages and troubleshoot issues.

Raphaello 1 year, 5 months ago

Selected Answer: B

ELB can only send access logs to S3; from there use Athena for querying. B is correct.

marfee 1 year, 7 months ago

I think that it's correct answer is B.

qsergii 2 years, 1 month ago

Selected Answer: B

Cloud watch impossible, only one option - B

tcp22 2 years, 4 months ago

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html B

rhinozD 2 years, 4 months ago

Selected Answer: B

B - for sure. As the others explained.

ITgeek 2 years, 5 months ago

Selected Answer: B

ELB stores the logs directly into S3

awsguru1998 2 years, 5 months ago

B is correct. ALB access logs can only be stored in an S3 bucket and cannot be sent directly to CloudWatch Logs. Therefore, option A is not a valid solution for determining which error messages the ALB is receiving

ILOVEVODKA 2 years, 6 months ago

B - for sure

helloworldabc 2 years, 6 months ago

AAAAAAAAAAAA

zaazanuna 2 years, 6 months ago

A - correct.

https://zhangxuetu.online

[202610]

Question #70 Topic 1

A company is planning to use Amazon S3 to archive financial data. The data is currently stored in an on-premises data center. The company uses AWS Direct Connect with a Direct Connect gateway and a transit gateway to connect to the on-premises data center. The data cannot be transported over the public internet and must be encrypted in transit.
Which solution will meet these requirements?

A. Create a Direct Connect public VIF. Set up an IPsec VPN connection over the public VIF to access Amazon S3. Use HTTPS for communication.

B. Create an IPsec VPN connection over the transit VIF. Create a VPC and attach the VPC to the transit gateway. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS for communication. **Most Voted**

C. Create a VPC and attach the VPC to the transit gateway. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS for communication.

D. Create a Direct Connect public VIF. Set up an IPsec VPN connection over the public VIF to the transit gateway. Create an attachment for Amazon S3. Use HTTPS for communication.

Correct Answer: B

Community vote distribution



Comments

that1guy **Highly Voted** 2 years, 11 months ago

Selected Answer: B

Technically both B and C are possible, but with B encryption is enforced. You can prevent unencrypted S3 actions via bucket policies, but not mentioned in the question, see: https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-HTTP-HTTPS In this case interface vpc endpoint for S3 is also correct, see: https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html > "You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints (by using AWS PrivateLink). A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on premises, or from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway." But in this context I would go for B:

Spike2020 2 years, 11 months ago

But you cannot create a vpn over a trasit VIF

rhinozD 2 years, 10 months ago

I think you can create an IPSec VPN over a transit VIF if there is a Direct Connect Gateway. https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway-vpn.html

fojta Highly Voted 2 years, 12 months ago

Selected Answer: B

both B and C are correct. Option B involves double encryption which is more secure but it's not explicitly defined in requirement that it would be required.

woorkim 1 year, 4 months ago

B is correct due to e2e encryption!

AlirezaNetWorld 1 year, 6 months ago

C is the best answer for this question to meet all the company's requirements.

Ravan 1 year, 6 months ago

Selected Answer: C

Option B (IPsec VPN over Transit VIF): Although this option includes a VPN, it adds unnecessary complexity. A direct interface VPC endpoint for S3, as in Option C, is a more straightforward and secure solution that avoids public internet use and encryption concerns.

hcong 1 year, 7 months ago

Selected Answer: C

Because it introduces an additional VPN connection, which is unnecessary if you already have Direct Connect

YogiB1 1 year, 10 months ago

Both B and C meet the required objective. B provides double encryption BUT it is not end to end, before Customer Gateway (on-prem server to on-prem router) and After TGW (TGW to VPC S3 Endpoint), the data is being carried as HTTPS. So VPN is just adding double encryption for partial route not end to end. In that case it is not much better than C.

seochan 1 year, 10 months ago

Selected Answer: B

Both B and C are possible solution, but C is not mentioning about routing configuration on TGW or etc. and you can make IPsec VPN over transit VIF https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway-vpn.html

seochan 1 year, 10 months ago

C is not possible since S3 itself cannot terminate TLS (HTTPS) connection

Raphaello 1 year, 11 months ago

Selected Answer: C

The request is to avoid transporting data over the Internet (DX would ensure that), and use in-transit encryption (HTTPS will do that). That being said, I see no point to create IPSEC VPN over DX connection, as long as Amazon S3 supports both interface endpoints (along with gateway endpoints ofc), and can reach S3 interface endpoint through DX connection and configure it (via IAM policy) to only used HTTPS. Option C is correct. Fulfilling, and without IPSEC VPN config. Had option C worded "S3 gateway endpoint" instead of "S3 interface endpoint", it would be wrong. As it is, it is just fine.

FayeG 2 years, 4 months ago

Selected Answer: C

Using HTTPS allows us to fulfil the end to end encryption without needing a VPN. Using Interface endpoints to S3 allows us an HTTPS API to S3 that stays in AWS private network. Thus we didn't need a VPN thus the correct answer is C.

passtest100 2 years, 5 months ago

C is enough, even VPN can established over transit VIF. End-end encryption is guaranteed by https, double encryption is not required, and site-site vpn is not end-to-end encryption of data in transit.

Cheam 2 years, 6 months ago

For those wondering how answer B will look like, please refer to the URL below. Ref: https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/traffic-encryption-options-direct-connect-ra.pdf All the best.

Chika22 2 years, 11 months ago

Selected Answer: A

I think (A) is the correct answer. Public VIF doesn't mean the traffic will flow through the public Internet. It'll reach AWS services through Public IP.

rhinozD 2 years, 10 months ago

How do you do this: "Set up an IPsec VPN connection over the public VIF to access Amazon S3"?

study_aws1 2 years, 11 months ago

Agree B) will be the most suitable option here. Just for knowledge & clarity purposes, was curious to understand why Option A) got ruled out here.

silviahdz 2 years, 11 months ago

"The data cannot be transported over the public internet"

ITgeek 2 years, 11 months ago

Selected Answer: B

create vpc endpoint and use IPSec VPN

AWSDEvops 2 years, 10 months ago

B and C - there is no interface EP for S3 - it's Gateway EP.

Josh1217 2 years, 8 months ago

Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, transit gateway, or AWS Direct Connect connection in your VPC cannot use a gateway endpoint to communicate with Amazon S3. Hence Interface EP.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html

gpt_test 2 years, 11 months ago

Selected Answer: B

Explanation: To meet the requirements of encrypting the data in transit and avoiding public internet, you can create an IPsec VPN connection over the transit VIF. Then, create a VPC and attach it to the transit gateway. Inside the VPC, you can provision an interface VPC endpoint (also known as a PrivateLink) for Amazon S3, which allows secure communication to Amazon S3 over the AWS network. Using HTTPS for communication ensures that the data remains encrypted in transit.

https://zhangxuetu.online

[202610]

Question #71 Topic 1

A company is using Amazon Route 53 Resolver DNS Firewall in a VPC to block all domains except domains that are on an approved list. The company is concerned that if DNS Firewall is unresponsive, resources in the VPC might be affected if the network cannot resolve any DNS queries. To maintain application service level agreements, the company needs DNS queries to continue to resolve even if Route 53 Resolver does not receive a response from DNS Firewall.
Which change should a network engineer implement to meet these requirements?

A. Update the DNS Firewall VPC configuration to disable fail open for the VPC.

B. Update the DNS Firewall VPC configuration to enable fail open for the VPC. **Most Voted**

C. Create a new DHCP options set with parameter dns_firewall_fail_open=false. Associate the new DHCP options set with the VPC.

D. Create a new DHCP options set with parameter dns_firewall_fail_open=true. Associate the new DHCP options set with the VPC.

Correct Answer: B

Community vote distribution

B (100%)

Comments

gpt_test **Highly Voted** 2 years, 11 months ago

Selected Answer: B

Explanation: Enabling the "fail open" feature in the Route 53 Resolver DNS Firewall VPC configuration ensures that if DNS Firewall becomes unresponsive, DNS queries will still be resolved. This helps maintain application service level agreements by allowing resources in the VPC to continue operating even if Route 53 Resolver does not receive a response from DNS Firewall.

woorkim 1 year, 4 months ago

B is correct! Fail-close vs Fail-Open (DNS Firewall Configuration): • Fail-close: Resolver blocks query if no response from DNS Firewall (security over availability) • Fail-open: Resolver allows query if no response from DNS firewall (availability over security)

Raphaello 1 year, 11 months ago

Selected Answer: B

B is the correct answer. The definition of fail open, fellow engineers!

PhilMultiCloud 2 years, 6 months ago

Selected Answer: B

To meet the requirement of maintaining DNS query resolution even if Route 53 Resolver DNS Firewall is unresponsive, the network engineer should implement option B: B. Update the DNS Firewall VPC configuration to enable fail open for the VPC. When you enable "fail open" mode for a VPC's DNS Firewall configuration, it means that if the DNS Firewall service becomes unresponsive or unavailable, the DNS queries will be allowed to pass through without being blocked. This ensures that the application's service level agreements are maintained even if the DNS Firewall service experiences issues. By enabling fail open, you ensure that DNS queries can still be resolved even if DNS Firewall is not functioning correctly. This can prevent disruption to your applications and services due to DNS resolution failures.

evargasbrz 2 years, 7 months ago

Selected Answer: B

B is correct.

JoseCC 2 years, 7 months ago

B) https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-dns-firewall-vpc-configuration.html

ITgeek 2 years, 11 months ago

Selected Answer: B

B, as in BUENO Good luck everyone! Has anyone made it this far taken the test with these questions??

awsguru1998 2 years, 11 months ago

B is correct D is wrong as enabling fail open for the VPC would mean that DNS queries would bypass DNS Firewall and proceed to the default DNS resolver. This might be a security risk as it would allow unapproved domains to be resolved, potentially exposing the company's resources to security threats.

study_aws1 3 years ago

B - coorect

helloworldabc 3 years ago

BBBBBBBBBB

zaazanuna 3 years ago

B - correct.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #72 Topic 1

A company is migrating an existing application to a new AWS account. The company will deploy the application in a single AWS Region by using one VPC and multiple Availability Zones. The application will run on Amazon EC2 instances. Each Availability Zone will have several EC2 instances. The EC2 instances will be deployed in private subnets.

The company's clients will connect to the application by using a web browser with the HTTPS protocol. Inbound connections must be distributed across the Availability Zones and EC2 instances. All connections from the same client session must be connected to the same EC2 instance. The company must provide end-to-end encryption for all connections between the clients and the application by using the application SSL certificate.

Which solution will meet these requirements?

A. Create a Network Load Balancer. Create a target group. Set the protocol to TCP and the port to 443 for the target group. Turn on session affinity (sticky sessions). Register the EC2 instances as targets. Create a listener. Set the protocol to TCP and the port to 443 for the listener. Deploy SSL certificates to the EC2 instances. **Most Voted**

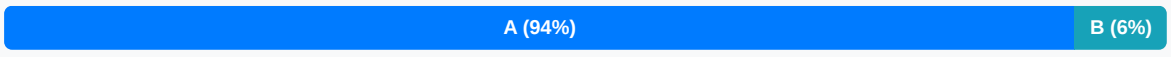
B. Create an Application Load Balancer. Create a target group. Set the protocol to HTTP and the port to 80 for the target group. Turn on session affinity (sticky sessions) with an application-based cookie policy. Register the EC2 instances as targets. Create an HTTPS listener. Set the default action to forward to the target group. Use AWS Certificate Manager (ACM) to create a certificate for the listener.

C. Create a Network Load Balancer. Create a target group. Set the protocol to TLS and the port to 443 for the target group. Turn on session affinity (sticky sessions). Register the EC2 instances as targets. Create a listener. Set the protocol to TLS and the port to 443 for the listener. Use AWS Certificate Manager (ACM) to create a certificate for the application.

D. Create an Application Load Balancer. Create a target group. Set the protocol to HTTPS and the port to 443 for the target group. Turn on session affinity (sticky sessions) with an application-based cookie policy. Register the EC2 instances as targets. Create an HTTP listener. Set the port to 443 for the listener. Set the default action to forward to the target group.

Correct Answer: A

Community vote distribution



Comments

TicDcNess Highly Voted 2 years, 11 months ago

If you need to pass encrypted traffic to targets without the load balancer decrypting it, you can create a Network Load Balancer or Classic Load Balancer with a TCP listener on port 443. Should be A

rhinozD 2 years, 10 months ago

Yeah. That's right. With NLB, sticky sessions are not supported for TLS listeners that use TLS target groups.

mic8 1 year, 4 months ago

Option C is close but doesn't meet the end-to-end encryption requirement in the way described because it terminates SSL at the Network Load Balancer instead of the EC2 instances

Spaurito 1 year, 4 months ago

A - You can do this for this scenario. You shouldn't need an ALB. Don't let the certificate get in the way. If you have a cert on the instance (which the application is using), regardless of the ELB, and a TCP listener for port 443, you got it covered. The certificate is passing through the NLB on port 443.

Ravan 1 year, 6 months ago

Selected Answer: B

ALB with HTTPS Listener: The Application Load Balancer (ALB) is designed for handling HTTP/HTTPS traffic and supports features like SSL termination, sticky sessions, and application-based routing. HTTPS End-to-End: Using HTTPS for the listener and registering the EC2 instances with HTTP or HTTPS will allow end-to-end encryption and efficient load balancing. AWS Certificate Manager (ACM): Using ACM for SSL certificates simplifies management and deployment.

cerifyme85 1 year, 11 months ago

Selected Answer: A

Architectural restirctions with NLB + TLS + Sticky sessions
https://repost.aws/questions/QUKVeULln7Q9asBlZz_bkOgA/nlb-sticky-sessions-and-ssl-encryption#:~:text=When%20you%20are,is%20enabled%20on

Raphaello 1 year, 11 months ago

Selected Answer: A

A is the correct answer. End-to-end encryption, the NLB with TCP listener would do.

marfee 2 years, 1 month ago

I'm from Japan.As a result my inverstigation,I think that the correct answer is A.

MarcosSantos 2 years, 2 months ago

I think it's C. Because using the tls listener on 443 we can use the ACM certificate, I will have to do a lab with tests to see what the applicable answer is. Chat GPT responds that the correct answer would be the letter D, and this is the same answer that I considered to be correct. reading it at this link: https://docs.aws.amazon.com/pt_br/elasticloadbalancing/latest/network/load-balancer-listeners.html It says that using TCP at 443, NLB transmits encrypted traffic to the destination without decrypting it. Therefore, alternative A seems to be very applicable.

Arad 2 years, 4 months ago

Selected Answer: A

Correct answer is A.

habros 2 years, 5 months ago

Selected Answer: A

A. Why? Because TLS no sticky session + ACM does not work in EC2.

daemon101 2 years ago

https://repost.aws/knowledge-center/configure-acm-certificates-ec2

Mishranihal737 2 years, 7 months ago

Yes A is correct

qsergii 2 years, 8 months ago

Selected Answer: A

Only one option - A

takecoffe 2 years, 9 months ago

Selected Answer: A

Ec2 instances need to have certificate .

printfmarcelo 2 years, 11 months ago

Selected Answer: A

Should be A To pass encrypted traffic, ==> Network Load Balancer + TCP.

symplesims 2 years, 11 months ago

In case of Option A, Although it uses TCP and port 443, SSL certificates must be deployed to the EC2 instances, rather than using a certificate from AWS Certificate Manager (ACM). In addition, Network Load Balancers (NLB) are better suited for handling TCP traffic, but its not support session affinity using cookies. So Option B is better.

Kristin01 2 years, 11 months ago

"The company's clients will connect to the application by using a web browser with the HTTPS protocol. "

rhinozD 2 years, 10 months ago

"The company must provide end-to-end encryption for all connections between the clients and the application by using the application SSL certificate." ACM Certificate can be able to deploy to EC2. NLB supports sticky session. -> A

Spike2020 2 years, 11 months ago

A) I also agree its A

https://zhangxuetu.online

[202610]

Question #73 Topic 1

A company is developing an application in which IoT devices will report measurements to the AWS Cloud. The application will have millions of end users. The company observes that the IoT devices cannot support DNS resolution. The company needs to implement an Amazon EC2 Auto Scaling solution so that the IoT devices can connect to an application endpoint without using DNS.

Which solution will meet these requirements MOST cost-effectively?

A. Use an Application Load Balancer (ALB)-type target group for a Network Load Balancer (NLB). Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the ALB. Set up the IoT devices to connect to the IP addresses of the NLB.

B. Use an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoint. Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the ALSet up the IoT devices to connect to the IP addresses of the accelerator.

C. Use a Network Load Balancer (NLB). Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the NLB. Set up the IoT devices to connect to the IP addresses of the NLB. **Most Voted**

D. Use an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoint. Create an EC2 Auto Scaling group. Attach the Auto Scaling group to the NLB. Set up the IoT devices to connect to the IP addresses of the accelerator.

Correct Answer: C

Community vote distribution



Comments

FayeG **Highly Voted** 2 years, 4 months ago

Selected Answer: D

The answer requires one to provide the IoT a single IP address. If you use NLB it gives you only one static (or EIP) per AZ. Thus resulting in multiple IP addreses. However a GA can provide a single front end IP to all the static (or EIP) addresses used by the NLB. Thus using an NLB alone is rulled out. Therefore the GA is the correct option. If the Q had stated that the applications where all in the same subnet then C would be correct. but it doesn't so this can't be assumed. See https://aws.amazon.com/elasticloadbalancing/network-load-balancer/

Spaurito 1 year, 4 months ago

D - agree, because they can't use DNS resolution, this solution fits the requirements.

rhinozD **Highly Voted** 2 years, 10 months ago

Selected Answer: C

B, C, and D are also doable. Let's think about the cost. AWS Global Accelerator is definitely the best option. but it costs more money. NLB is enough. -> C.

Spaurito 1 year, 4 months ago

does not mention cost only latency and a single IP address for connectivity

Spaurito 1 year, 4 months ago

scratch that

Joselito79 2 months, 3 weeks ago

Selected Answer: C

MOST cost-effectively is the difference between C and D , D is most expensive. The correct answer is C

eff3 7 months, 4 weeks ago

Selected Answer: D

specific mentioning 'millions'

8be7437 11 months, 1 week ago

Selected Answer: D

There is also "millions" of end users... got to be global accelerator...

dspd 1 year, 1 month ago

Selected Answer: C

cost effective

46f094c 1 year, 2 months ago

Selected Answer: D

Agree with FayeG. Plus I can't image deploying a million users App with autoscaling in only 1 AZ

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the valid solution and most cost-efficient.

patanjali 2 years ago

Selected Answer: C

GA and NLB both provide static IPs. NLB can handle millions of connection request per second. GA is more for global connectivity which is not asked here. Hence, C is correct answer.

Josh1217 2 years, 8 months ago

Selected Answer: C

A - Not valid B, D - Do not need Global Accelerator C - Best cost effective solution.

Moee 2 years, 8 months ago

WHY a NOT VALID?

tcp22 2 years, 9 months ago

D is very close but since it's not mentioning the users location hence C is correct

NeeG 2 years, 10 months ago

Also for users across region, how would NLB Work? I believe GA will solve that problem

printfmarcelo 2 years, 11 months ago

Selected Answer: C

I agree with Spike2020, Millions of users is NLB.

Kristin01 2 years, 11 months ago

Selected Answer: C

C, cost effective and also "The NLB automatically provides a static IP address for an AZ" so we can use them

Spike2020 2 years, 11 months ago

Answer D C is valid but with millions of users, I side with D

Neo00 2 years, 8 months ago

Network Load Balancer is capable of handling millions of requests per second while maintaining ultra-low latencies.

ITgeek 2 years, 11 months ago

Selected Answer: C

C is the most cost effective

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #74 Topic 1

A company has deployed a new web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Amazon EC2 Auto Scaling group. Enterprise customers from around the world will use the application. Employees of these enterprise customers will connect to the application over HTTPS from office locations.

The company must configure firewalls to allow outbound traffic to only approved IP addresses. The employees of the enterprise customers must be able to access the application with the least amount of latency.

Which change should a network engineer make in the infrastructure to meet these requirements?

A. Create a new Network Load Balancer (NLB). Add the ALB as a target of the NLB.

B. Create a new Amazon CloudFront distribution. Set the ALB as the distribution's origin.

C. Create a new accelerator in AWS Global Accelerator. Add the ALB as an accelerator endpoint. **Most Voted**

D. Create a new Amazon Route 53 hosted zone. Create a new record to route traffic to the ALB.

Correct Answer: C

Community vote distribution

C (100%)

Comments

printfmarcelo **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C, global accelerator Global static IP - Simplify allowlisting in enterprise firewalling and IoT use cases https://aws.amazon.com/global-accelerator/

study_aws1 **Highly Voted** 2 years, 11 months ago

Statement to be noted - "The company must configure firewalls to allow outbound traffic to only approved IP addresses. The employees of the enterprise customers must be able to access the application with the least amount of latency." While Cloudfront can provide low latency, given that the traffic will be routed to specified IPs, the scenario in this question leads to Global Accelerator - C)

woorkim 1 year, 4 months ago

C is right! C. Global Accelerator + ALB Provides 2 static anycast IP addresses Optimizes network path using AWS global network Perfect for dynamic content Reduces latency through edge networking Makes firewall rules simple (only 2 IPs to whitelist) Best solution

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. AGA provides 2 static IP's, and an entry point to route the flow through AWS backbone network, thus least lantency.

marfee 2 years, 1 month ago

I'm from Japan.As the result of my investigate, I guess that it's answer C.

Josh1217 2 years, 8 months ago

Selected Answer: C

Global Accelerator best for accessing application, CloudFront best for delivering content to customers.

ITgeek 2 years, 11 months ago

Selected Answer: C

C, global accelerator

PTLS 2 years, 11 months ago

AWS Global Accelerator: Global traffic manager Use traffic dials to route traffic to the nearest Region or achieve fast failover across Regions. API acceleration Accelerate API workloads by up to 60%, leveraging TCP termination at the edge. Global static IP Simplify allowlisting in enterprise firewalling and IoT use cases. Low-latency gaming and media workloads Use custom routing to deterministically route traffic to a fleet of EC2 instances. Answer is C

Spike2020 2 years, 11 months ago

B) Around the world with least latency, then you use cloudfront.

Spike2020 2 years, 11 months ago

I change to C. While there is an ip prefix list for cloudfront that you can monitor for changes with API. It sounds too cumbersome for this solution.

SAPALL 2 years, 11 months ago

B for me

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #75 Topic 1

A company has hundreds of VPCs on AWS. All the VPCs access the public endpoints of Amazon S3 and AWS Systems Manager through NAT gateways. All the traffic from the VPCs to Amazon S3 and Systems Manager travels through the NAT gateways. The company's network engineer must centralize access to these services and must eliminate the need to use public endpoints.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a central egress VPC that has private NAT gateways. Connect all the VPCs to the central egress VPC by using AWS Transit Gateway. Use the private NAT gateways to connect to Amazon S3 and Systems Manager by using private IP addresses.

B. Create a central shared services VPC. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access. Ensure that private DNS is turned off. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway. Create an Amazon Route 53 forwarding rule for each interface VPC endpoint. Associate the forwarding rules with all the VPCs. Forward DNS queries to the interface VPC endpoints in the shared services VPC.

C. Create a central shared services VPIn the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access. Ensure that private DNS is turned off. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway. Create an Amazon Route 53 private hosted zone with a full service endpoint name for Amazon S3 and Systems Manager. Associate the private hosted zones with all the VPCs. Create an alias record in each private hosted zone with the full AWS service endpoint pointing to the interface VPC endpoint in the shared services VPC. **Most Voted**

D. Create a central shared services VPC. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway. Ensure that private DNS is turned on for the interface VPC endpoints and that the transit gateway is created with DNS support turned on.

Correct Answer: C

Community vote distribution

C (56%) D (44%)

Comments

grc1979 Highly Voted 2 years, 10 months ago

Selected Answer: C

https://aws.amazon.com/es/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/ see Sharing PrivateLink endpoints between VPCs point

evargasbrz Highly Voted 2 years, 7 months ago

Selected Answer: C

When you create a VPC endpoint to an AWS service, you can enable private DNS. When enabled, the setting creates an AWS managed Route 53 private hosted zone (PHZ) which enables the resolution of public AWS service endpoint to the private IP of the interface endpoint. The managed PHZ only works within the VPC with the interface endpoint. In our setup, when we want spoke VPCs to be able to resolve VPC endpoint DNS hosted in a centralized VPC, the managed PHZ won't work. To overcome this, disable the option that automatically creates the private DNS when an interface endpoint is created. Next, manually create a Route 53 PHZ and add an Alias record with the full AWS service endpoint name pointing to the interface endpoint, as shown in the following figure.

steli0 6 months, 1 week ago

Selected Answer: C

D is not correct because the private DNS disablement mentioned in C is about the Interface Endpoints, not the VPC itself or the TGW. Without disabling the Private DNS names for the endpoint (as mentioned in grc1979 documentation) the endpoint will create a private hosted zone by it's own assigned only to the the shared VPC.

valerioagui 8 months ago

Selected Answer: D

Interface VPC endpoints allow private connectivity to AWS services without using public IPs or NAT gateways. Private DNS enabled ensures that service domain names (like s3.amazonaws.com) resolve to the private IPs of the endpoints. TGW with DNS support allows DNS queries to resolve correctly across VPCs. This setup eliminates the need for NAT gateways and centralizes access with minimal operational overhead.

dspd 1 year, 1 month ago

Selected Answer: C

all four are wrong... why to use interface endpoint for s3... it should be gateway as its free..

46f094c 1 year, 2 months ago

Selected Answer: D

for me creating hundreds of zone associations to the VPC is the definition of operational overhead

VerRi 1 year, 6 months ago

Selected Answer: D

C and D should work, and D has the least operational overhead. There is no reason to turn off private DNS unless the question requires more control.

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. Shared, central VPC + interface endpoint for the required services Disable private DNS, create private hosted zone and associated it with all VPC's Connect all VPC through TGW.

stream3652 2 years ago

https://aws.amazon.com/jp/blogs/news/introducing-private-dns-support-for-amazon-s3-with-aws-privatelink/

KobDragoon 2 years ago

Selected Answer: D

I would also vote for C at first, but is there anything wrong with D as the answer with less operational overhead?

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

vikasj1in 2 years, 1 month ago

Selected Answer: C

This option uses interface VPC endpoints to centralize access to Amazon S3 and Systems Manager in a shared services VPC, eliminating the need for public endpoints. Private DNS is turned off to ensure that the fully qualified domain names (FQDNs) of the services are resolved to their public IP addresses. The use of Amazon Route 53 private hosted zones provides a centralized and scalable DNS solution, and alias records are created to point to the interface VPC endpoints in the shared services VPC. AWS Transit Gateway is used to connect all the VPCs to the central shared services VPC, reducing the operational overhead of managing direct VPC-to-VPC connections. Options A, B, and D either have higher operational overhead or do not provide an optimal solution for centralizing access to Amazon S3 and Systems Manager.

Vogd 2 years, 2 months ago

Selected Answer: D

Check Amazon Feature interoperability for TGW DNS support On https://aws.amazon.com/transit-gateway/features/ Check https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html For DNS support, select this option if you need the VPC to resolve public IPv4 DNS host names to private IPv4 addresses when queried from instances in another VPC attached to the transit gateway. Check https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support If you use custom DNS domain names defined in a private hosted zone in Amazon Route 53, or use private DNS with interface VPC endpoints (AWS PrivateLink), you must set both the enableDnsHostnames and enableDnsSupport attributes to true.

Vinsmoke 2 years, 6 months ago

Selected Answer: C

Not D. "When you create a VPC endpoint to an AWS service or AWS PrivateLink SaaS, you can enable Private DNS. When enabled, the setting creates an AWS managed Route 53 private hosted zone (PHZ) for you. The managed PHZ works great for resolving the DNS name within a VPC however, it does not work outside of the VPC. This is where PHZ sharing and Route 53 Resolver come into play to help us get unified name resolution for shared VPC endpoints" https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/

Neo00 2 years, 8 months ago

Selected Answer: D

Enable private DNS option is ok. In this case, the DNS queries for S3 originating will be resolved to the private IPs of S3 interface endpoints I vote D

johnconnor 2 years, 8 months ago

Why not B? What's the main difference for you to Choose C over B?

Josh1217 2 years, 8 months ago

Selected Answer: C

Private DNS needs to be turned off. Hence, D cannot be the answer.

https://zhangxuetu.online

[202610]

Question #76 Topic 1

A company manages resources across VPCs in multiple AWS Regions. The company needs to connect to the resources by using its internal domain name. A network engineer needs to apply the aws.example.com DNS suffix to all resources.

What must the network engineer do to meet this requirement?

A. Create an Amazon Route 53 private hosted zone for aws.example.com in each Region that has resources. Associate the private hosted zone with that Region's VPC. In the appropriate private hosted zone, create DNS records for the resources in each Region.

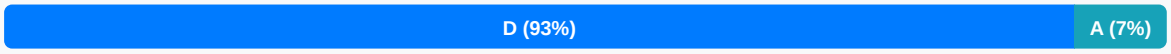
B. Create one Amazon Route 53 private hosted zone for aws.example.com. Configure the private hosted zone to allow zone transfers with every VPC.

C. Create one Amazon Route 53 private hosted zone for example.com. Create a single resource record for aws.example.com in the private hosted zone. Apply a multivalue answer routing policy to the record. Add all VPC resources as separate values in the routing policy.

D. Create one Amazon Route 53 private hosted zone for aws.example.com. Associate the private hosted zone with every VPC that has resources. In the private hosted zone, create DNS records for all resources. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

rhinozD **Highly Voted** 2 years, 10 months ago

Selected Answer: D

Single PHZ can be associated with VPCs across regions. D is correct.

study_aws1 **Highly Voted** 2 years, 11 months ago

This blog is for multi-account DNS architecture, not region. Single PHZ can be associated with multiple VPCs across regions. Option D) is correct

woorkim 1 year, 4 months ago

D is right! Route 53 private hosted zones do not support zone transfers

Raphaello 1 year, 11 months ago

Selected Answer: D

D is the correct answer.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is A according to SPOTO products.

vikasj1in 2 years, 1 month ago

Selected Answer: D

Option D is the most appropriate because it involves creating a single private hosted zone for aws.example.com and associating it with every VPC that has resources. This ensures a centralized management approach. With this approach, you can create DNS records for all resources within the private hosted zone, allowing for a consistent DNS suffix across VPCs and regions. Options A, B, and C do not provide a centralized solution or are not suitable for achieving the desired outcome in a multi-VPC, multi-region environment.

Arad 2 years, 4 months ago

Selected Answer: D

D is the correct answer.

PhilMultiCloud 2 years, 6 months ago

Selected Answer: D

Here are the reasons why Option D is the correct answer: It creates a single private hosted zone for aws.example.com. This ensures that all resources in all VPCs can be accessed using the same domain name. It associates the private hosted zone with every VPC that has resources. This ensures that the DNS records for all resources are replicated to all VPCs. It creates DNS records for all resources in the private hosted zone. This ensures that all resources can be resolved by DNS. Option A is not a valid solution because it would create separate private hosted zones for each Region. This would make it difficult to manage DNS records and would not ensure that all resources are resolved under the same domain name. Option B is not a valid solution because it does not apply the aws.example.com DNS suffix to all resources. Option C is not a valid solution because it does not explicitly associate resources in different VPCs across multiple Regions with the aws.example.com domain name.

Mishranihal737 2 years, 7 months ago

Yes D is Correct ,Route 53 is a global resource.

printfmarcelo 2 years, 11 months ago

Selected Answer: D

Option D) is correct

ITgeek 2 years, 11 months ago

Selected Answer: A

https://aws.amazon.com/blogs/architecture/using-route-53-private-hosted-zones-for-cross-account-multi-region-architectures/

Spike2020 2 years, 11 months ago

The blog you posted supports D

PTLS 2 years, 11 months ago

Selected Answer: D

Looks like D, no need to create resources DNS name in all regions/VPCs

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #77 Topic 1

An insurance company is planning the migration of workloads from its on-premises data center to the AWS Cloud. The company requires end-to-end domain name resolution. Bi-directional DNS resolution between AWS and the existing on-premises environments must be established. The workloads will be migrated into multiple VPCs. The workloads also have dependencies on each other, and not all the workloads will be migrated at the same time.

Which solution meets these requirements?

A. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPC, and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints. Most Voted

B. Configure a public hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPC. and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.

C. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPDefine Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPand share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 outbound endpoints.

D. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver. Associate the Route 53 outbound rules with the application VPCs, and share the private hosted zones with the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.

Correct Answer: A

Community vote distribution

A (100%)

Comments

study_aws1 Highly Voted 2 years, 11 months ago

It is A). PHZ cannot be shared, Route 53 resolver rules can be shared uusing AWS RAM.

secdaddy 1 year, 2 months ago

The use of 'egress zone' bothers me as it *could* indicate Internet which means public zone (B) instead of private zone (A).

zanhsieh 1 year ago

Selected Answer: A

A. B: No. Public zones are for internet-facing domains, not internal VPC resolution. VPCs need private zones for internal DNS. C: No. Forwarding to outbound endpoints is incorrect. Outbound endpoints send queries from AWS, not receive them. Inbound endpoints are needed. D: No. Resolver rules need VPC association, but “associate outbound rules with VPCs” is unclear—rules are typically associated via outbound endpoints in the egress VPC. Associating rules directly with application VPCs contradicts the egress VPC model (rules should stay centralized).

woorkim 1 year, 4 months ago

A is right * associate the private hosted zones with the egress VPC, allowing centralized DNS management, while sharing the rules through RAM for consistency

Raphaello 1 year, 11 months ago

Selected Answer: A

Associate private hosted zoneS with egress VPC, and share forwarding rules (to on-prem DNS) with application VPC's via RAM. Pay attention to the details and wording. A is the correct answer.

shinzor 2 years, 4 months ago

A and C are the same answer. C has some typo's

[Removed] 2 years, 4 months ago

effffff

Arad 2 years, 4 months ago

Selected Answer: A

A is the right answer.

MohamedSherif1 2 years, 7 months ago

Selected Answer: A

A. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPC, and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.

ISSDoksim 2 years, 7 months ago

agreed A -

rhinozD 2 years, 10 months ago

Selected Answer: A

A is correct.

Spike2020 2 years, 11 months ago

D is the correct answer

rhinozD 2 years, 10 months ago

"Associate the Route 53 outbound rules with the application VPCs" -> wrong.

https://zhangxuetu.online

[202610]

Question #78 Topic 1

A global company runs business applications in the us-east-1 Region inside a VPC. One of the company's regional offices in London uses a virtual private gateway for an AWS Site-to-Site VPN connection tom the VPC. The company has configured a transit gateway and has set up peering between the VPC and other VPCs that various departments in the company use.

Employees at the London office are experiencing latency issues when they connect to the business applications.

What should a network engineer do to reduce this latency?

A. Create a new Site-to-Site VPN connection. Set the transit gateway as the target gateway. Enable acceleration on the new Site-to-Site VPN connection. Update the VPN device in the London office with the new connection details. **Most Voted**

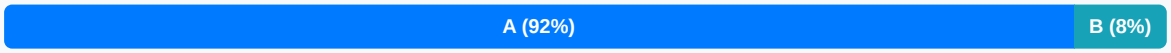
B. Modify the existing Site-to-Site VPN connection by setting the transit gateway as the target gateway. Enable acceleration on the existing Site-to-Site VPN connection.

C. Create a new transit gateway in the eu-west-2 (London) Region. Peer the new transit gateway with the existing transit gateway. Modify the existing Site-to-Site VPN connection by setting the new transit gateway as the target gateway.

D. Create a new AWS Global Accelerator standard accelerator that has an endpoint of the Site-to-Site VPN connection. Update the VPN device in the London office with the new connection details.

Correct Answer: A

Community vote distribution



Comments

ITgeek **Highly Voted** 2 years, 11 months ago

Selected Answer: A

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

rhinozD 2 years, 10 months ago

agree. A is correct.

woorkim 1 year, 4 months ago

A is answer! to increase BW wo interrupt!

Raphaello 1 year, 11 months ago

Selected Answer: A

A is the correct answer. Accelerated site-to-site VPN is available only with TGW VPN attachment, where you can enable it, but you do not manage or even view the accelerators.

Arad 2 years, 4 months ago

Selected Answer: A

Correct answer is A.

FayeG 2 years, 4 months ago

Selected Answer: A

Acceleration drops the VPN into the nearest GA so the connection goes over the Atlantic on fast, private AWS links, not congested public ones. Both TGW peering and VPNs use encryption. So you gain nothing (in terms of latency) by using peered TGWs even though a VPN is between 10% and 20% more latency impaired than an unencrypted network. Bandwidth considerations are out of scope.

qsergii 2 years, 8 months ago

Selected Answer: B

Modification possible and is easiest way

Tofu13 2 years, 6 months ago

Modification is not possible. -> B wrong, A right. https://docs.aws.amazon.com/vpn/latest/s2svpn/accelerated-vpn.html You cannot turn on or turn off acceleration for an existing Site-to-Site VPN connection. Instead, you can create a new Site-to-Site VPN connection with acceleration on or off as needed. Then, configure your customer gateway device to use the new Site-to-Site VPN connection and delete the old Site-to-Site VPN connection.

albertkr 2 years, 9 months ago

Option C involves creating a new transit gateway in the eu-west-2 (London) Region and peering it with the existing transit gateway. The existing Site-to-Site VPN connection would then be modified to use the new transit gateway as the target gateway. This approach could help reduce latency by providing a more direct route for traffic between the London office and the VPC hosting the business applications. Although unsure whether this is the most cost effective or efficient way, however cost and efficiency factors are not asked in this question.

tcp22 2 years, 10 months ago

The company workload is only in us-east-1, and they don't use any other region, hence no point of creating a new TGW in eu-west-2 and peer with TGW in us-east-1, Answer is A

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #79 Topic 1

A company has a hybrid cloud environment. The company's data center is connected to the AWS Cloud by an AWS Direct Connect connection. The AWS environment includes VPCs that are connected together in a hub-and-spoke model by a transit gateway. The AWS environment has a transit VIF with a Direct Connect gateway for on-premises connectivity.

The company has a hybrid DNS model. The company has configured Amazon Route 53 Resolver endpoints in the hub VPC to allow bidirectional DNS traffic flow. The company is running a backend application in one of the VPCs.

The company uses a message-oriented architecture and employs Amazon Simple Queue Service (Amazon SQS) to receive messages from other applications over a private network. A network engineer wants to use an interface VPC endpoint for Amazon SQS for this architecture. Client services must be able to access the endpoint service from on premises and from multiple VPCs within the company's AWS infrastructure.

Which combination of steps should the network engineer take to ensure that the client applications can resolve DNS for the interface endpoint? (Choose three.)

A. Create the interface endpoint for Amazon SQS with the option for private DNS names turned on.

B. Create the interface endpoint for Amazon SQS with the option for private DNS names turned off. Most Voted

C. Manually create a private hosted zone for sqs.us-east-1.amazonaws.com. Add necessary records that point to the interface endpoint. Associate the private hosted zones with other VPCs. Most Voted

D. Use the automatically created private hosted zone for sqs.us-east-1.amazonaws.com with previously created necessary records that point to the interface endpoint. Associate the private hosted zones with other VPCs.

E. Access the SQS endpoint by using the public DNS name sqs.us-east-1 amazonaws.com in VPCs and on premises. Most Voted

F. Access the SQS endpoint by using the private DNS name of the interface endpoint .sqs.us-east-1.vpce.amazonaws.com in VPCs and on premises.

Correct Answer: BCE

Community vote distribution



Comments

Fati_2022 Highly Voted 2 years, 10 months ago

Selected Answer: BCF

Its internal and the access should be private ,which makes F correct

trap 2 years, 9 months ago

That's correct aws.amazon.com/blogs/networking-and-content-delivery/centralize-access-using-vpc-interface-endpoints/

6e5b127 1 year, 8 months ago

BCE public DNS name will be resolve to interface endpoint private IP finally Also, options B and F are indeed in conflict: If we turn off private DNS names (option B), the interface endpoint won't have a private DNS name to use, making option F impossible.

jhon648274 1 year, 7 months ago

B turns off private dns meaning that the automatic private hosted zone that resolves the public name to the private ip won't be created.

study_aws1 Highly Voted 2 years, 11 months ago

To access interface endpoints through other VPCs, we need to - 1. Disable private DNS for VPC endpoints 2. Create PHZ e.g. sqs.us-east-1.amazonaws.com 3. Create Alias record pointing to VPC endpoint DNS 4. Associate PHZ with all the spoke VPCs Hence, answer is B), C) & E)

MarcosSantos 2 years, 2 months ago

Hello, does the letter E speak about public DNS? But in this case wouldn't it be correct to use private DNS? So the letter F instead of E?

Ohnet 3 months, 3 weeks ago

Selected Answer: BCE

https://aws.amazon.com/es/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/

Ohnet 3 months, 4 weeks ago

Selected Answer: BCE

BCE.....

unknownXXX 5 months, 2 weeks ago

Selected Answer: ACE

ACE, The question asks about combination of step so what is the point of manually create private hosted zone if you don't use the record.

a0e6696 7 months ago

Selected Answer: BCF

with the Private DNS enabled, private hosted will be created automatically but it will not be visible nor associated with other vpcs. Even with the DNS enabled, from the on-premises side we have to write DNS forwarder rule to forward domain to sqs.us-east-1.amazonaws.com to AWS VPC .2 IP address or IP address if any inbound rules in route53. I will be with the BCF

valerioagui 8 months ago

Selected Answer: ADF

A enables private DNS resolution, allowing clients to use the standard service name (sqs.us-east-1.amazonaws.com) and have it resolve to the private IP of the interface endpoint. D leverages the automatically created private hosted zone, reducing operational overhead and ensuring consistency. F confirms that clients can use the private DNS name for direct access, which is necessary for hybrid environments with DNS forwarding.

dcantos 9 months, 1 week ago

Selected Answer: ADF

I think....

AWSLoverLoverLoverLoverLover 11 months, 3 weeks ago

Selected Answer: BCF

B, C & F Public DNS Name (sqs.us-east-1.amazonaws.com) This is the standard public AWS SQS endpoint. It routes traffic over the public internet. It can be accessed from anywhere, including VPCs and on-premises networks, but requires internet access or AWS PrivateLink. Private DNS Name (.sqs.us-east-1.vpce.amazonaws.com) This is the private endpoint for SQS, which is available when you create an AWS PrivateLink interface endpoint for SQS. It allows access to SQS entirely within the AWS network (without going over the public internet). Only accessible from within the VPC or from on-premises via a VPN or Direct Connect to AWS.

Hubabi 1 year, 1 month ago

Selected Answer: BCE

BCE With C) you create the private hosted zone for sqs.us-east-1.amazonaws.com that is basically the PUBLIC DNS name of SQS service, and associate the VPCs with this private zone. Then, you MUST use that public name, because that's the one that you have created in your private zone! You didn't create a zone for sqs.us-east-1.vpce.amazonaws.com! Thus it's E and not F.

dspd 1 year, 1 month ago

Selected Answer: BCF

E: Using the public DNS name would not leverage the private interface endpoint and could potentially route traffic over the public internet, which is not desired in this private network setup.

rodrigoMD 1 year, 1 month ago

Selected Answer: BCE

BCE https://aws.amazon.com/blogs/networking-and-content-delivery/centralize-access-using-vpc-interface-endpoints/ If you want to resolve the AWS service endpoint natively from within spoke VPCs, then you must perform these additional steps: Disable the Private DNS for an interface VPC endpoint in the hub VPC (if it’s enabled). Create a Private Hosted Zone with same name as AWS service endpoint (for example, sqs.us-east-1.amazonaws.com) and create an A record (alias) to point to an interface VPC endpoint DNS.

secdaddy 1 year, 2 months ago

Selected Answer: ADF

There's direct connect so no need for public DNS. There are resolver endpoints for onprem bidir DNS. D associates the auto created zone with the other vpcs. F is thus possible.

AzureDP900 1 year, 2 months ago

Selected Answer: BCF

These options complement each other and provide a complete solution for resolving DNS for the interface endpoint: Option B disables private DNS names, which would prevent client applications from accessing the SQS endpoint. This option is not recommended. Option C manually creates a private hosted zone and associates it with other VPCs or uses the automatically created one provided by Amazon SQS. This ensures that client applications can resolve DNS

for the interface endpoint. Option F provides the correct format for using the private DNS name of the interface endpoint (in this case, .sqs.us-east-1.vpce.amazonaws.com).

woorkim 1 year, 4 months ago

B,C,E!

qomtodie 1 year, 6 months ago

Selected Answer: BCE

We created the PRIVATE hosted zone.

qomtodie 1 year, 6 months ago

Sorry, I chose wrong. BCF is right.

qomtodie 1 year, 7 months ago

BCF It's so obvious. Why you choose E?

https://zhangxuetu.online

[202610]

Question #80 Topic 1

A company's network engineer builds and tests network designs for VPCs in a development account. The company needs to monitor the changes that are made to network resources and must ensure strict compliance with network security policies. The company also needs access to the historical configurations of network resources.

Which solution will meet these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with a custom pattern to monitor the account for changes. Configure the rule to invoke an AWS Lambda function to identify noncompliant resources. Update an Amazon DynamoDB table with the changes that are identified.

B. Create custom metrics from Amazon CloudWatch logs. Use the metrics to invoke an AWS Lambda function to identify noncompliant resources. Update an Amazon DynamoDB table with the changes that are identified.

C. Record the current state of network resources by using AWS Config. Create rules that reflect the desired configuration settings. Set remediation for noncompliant resources. **Most Voted**

D. Record the current state of network resources by using AWS Systems Manager Inventory. Use Systems Manager State Manager to enforce the desired configuration settings and to carry out remediation for noncompliant resources.

Correct Answer: C

Community vote distribution

C (100%)

Comments

ITgeek **Highly Voted** 2 years, 5 months ago

Selected Answer: C

AWS Config

Raphaello 1 year, 5 months ago

Selected Answer: C

AWS Config to record configuration changes, API timelines, and compliance timelines. C is the correct answer.

Certified101 2 years, 1 month ago

Selected Answer: C

AWS Config = Compliance

https://zhangxuetu.online

[202610]

Question #81 Topic 1

A company is migrating an application from on premises to AWS. The company will host the application on Amazon EC2 instances that are deployed in a single VPC. During the migration period, DNS queries from the EC2 instances must be able to resolve names of on-premises servers. The migration is expected to take 3 months After the 3-month migration period, the resolution of on-premises servers will no longer be needed.

What should a network engineer do to meet these requirements with the LEAST amount of configuration?

A. Set up an AWS Site-to-Site VPN connection between on premises and AWS. Deploy an Amazon Route 53 Resolver outbound endpoint in the Region that is hosting the VPC. Most Voted

B. Set up an AWS Direct Connect connection with a private VIF. Deploy an Amazon Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint in the Region that is hosting the VPC.

C. Set up an AWS Client VPN connection between on premises and AWS. Deploy an Amazon Route 53 Resolver inbound endpoint in the VPC.

D. Set up an AWS Direct Connect connection with a public VIF. Deploy an Amazon Route 53 Resolver inbound endpoint in the Region that is hosting the VPC. Use the IP address that is assigned to the endpoint for connectivity to the on-premises DNS servers.

Correct Answer: A

Community vote distribution

A (100%)

Comments

takecoffe Highly Voted 2 years, 9 months ago

Selected Answer: A

Setting up an AWS Site-to-Site VPN connection between on premises and AWS would enable a secure and encrypted connection over the public internet1. Deploying an Amazon Route 53 Resolver outbound endpoint in the Region that is hosting the VPC would enable forwarding of DNS queries for on-premises servers to the on-premises DNS servers2. This would allow EC2 instances in the VPC to resolve names of on-premises servers during the migration period. After the migration period, the Route 53 Resolver outbound endpoint can be deleted with minimal configuration changes.

woorkim 1 year, 4 months ago

A is correct. DX require 3 MONTH!

hogtrough 1 year, 9 months ago

Selected Answer: A

DX typically takes a few months just to get set up so that removes B and D Client VPN isn't really an option here. That's for end users, not for connectivity between locations.

Raphaello 1 year, 11 months ago

Selected Answer: A

Temporary solution for 3 months, then DX is not an appropriate option. Client VPN is definitely wrong. That leaves site-to-site VPN option, with is A..without even fully reading it.

Arad 2 years, 4 months ago

Selected Answer: A

Definitely A.

tom_cat 2 years, 11 months ago

Selected Answer: A

S2S VPN & outbound resolver

ITgeek 2 years, 11 months ago

Selected Answer: A

Site to Site VPN

https://zhangxuetu.online

[202610]

Question #82 Topic 1

A company is hosting an application on Amazon EC2 instances behind an Application Load Balancer. The instances are in an Amazon EC2 Auto Scaling group. Because of a recent change to a security group, external users cannot access the application.

A network engineer needs to prevent this downtime from happening again. The network engineer must implement a solution that remediates noncompliant changes to security groups.

Which solution will meet these requirements?

A. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

B. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

C. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

D. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

TicDcNess **Highly Voted** 2 years, 11 months ago

Based on the following link I should say D https://aws.amazon.com/blogs/mt/remediate-noncompliant-aws-config-rules-with-aws-systems-manager-automation-runbooks/

woorkim 1 year, 4 months ago

D is only answer!!!

Raphaello 1 year, 11 months ago

Selected Answer: D

Detecting configuration changes that's what AWS Config does best. Then SSM Automation can facilitate remediation. D is the correct answer.

takecoffe 2 years, 9 months ago

Selected Answer: D

Without doubt D

printfmarcelo 2 years, 11 months ago

Selected Answer: D

Answer is D

ITgeek 2 years, 11 months ago

Selected Answer: D

AWS config + System Manager

Spike2020 2 years, 11 months ago

Answer is D

https://zhangxuetu.online

[202610]

Question #83 Topic 1

A company is deploying third-party firewall appliances for traffic inspection and NAT capabilities in its VPC. The VPC is configured with private subnets and public subnets. The company needs to deploy the firewall appliances behind a load balancer.

Which architecture will meet these requirements MOST cost-effectively?

A. Deploy a Gateway Load Balancer with the firewall appliances as targets. Configure the firewall appliances with a single network interface in a private subnet. Use a NAT gateway to send the traffic to the internet after inspection.

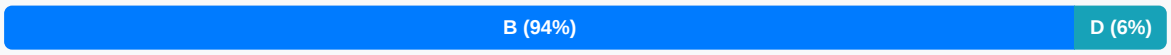
B. Deploy a Gateway Load Balancer with the firewall appliances as targets. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection. Most Voted

C. Deploy a Network Load Balancer with the firewall appliances as targets. Configure the firewall appliances with a single network interface in a private subnet. Use a NAT gateway to send the traffic to the internet after inspection.

D. Deploy a Network Load Balancer with the firewall appliances as targets. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.

Correct Answer: B

Community vote distribution



Comments

devilman222 Highly Voted 2 years, 9 months ago

The answer is obviously B. 100% of the people voted for B. Why does this show the correct solution as D? Why are more than half of the "correct solution", the wrong one?

study_aws1 Highly Voted 2 years, 11 months ago

Two-arm mode: As shown in figure 5b below, the firewall is deployed in two-arm mode and performs both inspection as well as NAT. Some AWS partners provide firewall with NAT functionality. GWLB integrates seamlessly in such deployment mode. You don’t need to do any additional configuration changes in the GWLB. However, the firewall networking differs – one network interface is on the private subnet and the other is on public subnet. This mode

requires software support from the firewall partner. Some of the GWLB partners (Palo Alto Networks, Valtix) support this feature, however consult with an AWS partner of your choice before using this mode. Based on the above, can we blindly choose two-arm or NAT functionality within the firewall for all third party vendor appliances. Also, the cost of implementing firewall in two-arm mode for each appliance vs. cost of a single NAT gateway needs to be evaluated.

AzureDP900 1 year, 2 months ago

Selected Answer: B

This solution meets the requirements most cost-effectively because: It uses a Gateway Load Balancer, which is free of charge for AWS services (it's just an instance of a free service provided by AWS). The firewall appliances are configured with two network interfaces: one in a private subnet and another in a public subnet. This allows the firewall appliances to inspect traffic coming from both the internet and the VPC without requiring additional NAT configurations. By using the NAT functionality on the firewall appliances, you can send traffic to the internet after inspection, meeting the requirements for both third-party firewall appliances and the need to deploy them behind a load balancer.

woorkim 1 year, 4 months ago

B is correct for applliances!

cerifyme85 1 year, 11 months ago

Selected Answer: B

Firewall for "Traffic inspection" and "Nat capablities" ==> Two arm mode

acloudguru 1 year, 11 months ago

Selected Answer: D

NLB is cheaper than GLW, so D is most cost-effectively

Raphaello 1 year, 11 months ago

Selected Answer: B

Both A & B can be correct. Ref: https://aws.amazon.com/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer You can either rely on NAT GW to handle the NATing, while your 3rd FW behind GWLB handle the security policy and inspection (one-arm mode) Or, you can create the FW a dual-homed appliance (two-arm mode), and let it handle both the security inspection and NATing. Both are correct, however the request is to apply the MOST cost-effective solution..then B would be the answer, since that solution will save on NAT GW costs..which are quite high. Pay attention the requirements.

Spaurito 1 year, 4 months ago

Good catch. The NAT GW is expensive. Since you already have the appliances, using the NAT features on them would be the most cost effective.

cerifyme85 1 year, 11 months ago

No not cost.. More a discussion of where u want the NAT to be done from, also one mode changes the port and source addresses

cerifyme85 1 year, 11 months ago

Yea.. true.. my bad.. if u used the nAt functionality on firewall u pay less

Marfee400704 2 years, 1 month ago

I think that it's correct answer is A according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: B

B is the most cost-effective solution as asked in the question.

takecoffe 2 years, 9 months ago

Selected Answer: B

B is the right answer

rhinozD 2 years, 10 months ago

Selected Answer: B

As study_aws1 explained. B is correct.

study_aws1 2 years, 11 months ago

Also, similar from below link - https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-nat-gateway-and-gwlb-with-ec2.html Some third-party appliances can support SNAT and overlay routing (two-arm mode) therefore eliminating the need to create NAT gateways for saving costs. However, consult with an AWS partner of your choice before using this mode as this is dependent on vendor support and implementation. Given the above link, is it advisable to choose an option which does not fall into Best Practices but may have some lower cost, not established with all vendors.

study_aws1 2 years, 11 months ago

GWLB supports two different models of firewall deployment (see figures 5a and 5b below) – one-arm with or two-arm where the firewall can also perform NAT. One-arm mode: As shown in figure 5a below, the firewall is deployed in one-arm mode just for traffic inspection whereas NAT Gateway performs translation. This is the most common deployment method, and eliminates dependency on firewall supporting NAT functionality. Also, it increases performance of the firewall by offloading NAT to NAT Gateway.

study_aws1 2 years, 11 months ago

Please refer the below link and the extract given in the last part - https://aws.amazon.com/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer/

ITgeek 2 years, 11 months ago

Selected Answer: B

Gateway Load balancer, use the built in NAT functionality of the firewall to save money and two network interfaces to inspect both private and public subnets

PTLS 2 years, 11 months ago

Selected Answer: B

use NAT functionality within firewall appliances.

study_aws1 2 years, 11 months ago

Do not think we can rely on NAT functionality in multiple third party firewall appliances individually, we do not know what that will cost & whether all appliances will support NAT functionality. Option A) looks technically more appropriate

https://zhangxuetu.online

[202610]

Question #84 Topic 1

A company's AWS architecture consists of several VPCs. The VPCs include a shared services VPC and several application VPCs. The company has established network connectivity from all VPCs to the on-premises DNS servers.

Applications that are deployed in the application VPCs must be able to resolve DNS for internally hosted domains on premises. The applications also must be able to resolve local VPC domain names and domains that are hosted in Amazon Route 53 private hosted zones.

What should a network engineer do to meet these requirements?

A. Create a new Route 53 Resolver inbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC. Update each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

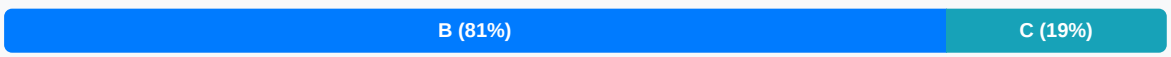
B. Create a new Route 53 Resolver outbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC. Most Voted

C. Create a new Route 53 Resolver outbound endpoint in the shared services VPCreate forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPUpdate each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

D. Create a new Route 53 Resolver inbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC.

Correct Answer: B

Community vote distribution



Comments

study_aws1 Highly Voted 2 years, 5 months ago

Yes it is B). Should have been completed with DHCP Option set as AmazonProvidedDNS for resolving local VPC domain names.

johnconnor 2 years, 1 month ago

Isn't that the answer for C? C Is B plus the DHCP?

Jordarlu 1 year, 4 months ago

https://docs.aws.amazon.com/vpc/latest/userguide/DHCPOptionSet.html#ChangingDHCPOptionsofaVPC Note After you create a DHCP option set, you can't modify it. To update the DHCP options for your VPC, you must create a new DHCP option set and then associate it with your VPC. hence, C is incorrect

steli0 6 months, 1 week ago

Selected Answer: B

B is correct cause outbound is needed and DHCP shouldn't change the default DNS (.2 or link-local) because intra VPC DNS resolution should keep functioning.

6008af2 7 months, 2 weeks ago

Selected Answer: B

Instances should keep using the VPC's AmazonProvidedDNS (.2), so they can still resolve local VPC names and Route 53 private hosted zones—no DHCP change needed.

6008af2 7 months, 2 weeks ago

Selected Answer: C

You need to connect other internal VPCs and not only shared VPCs

deepakno 8 months, 2 weeks ago

Selected Answer: C

How local VPC domain names and domains that are hosted in Amazon Route 53 private hosted zones will be resolved if it is B?

AzureDP900 1 year, 2 months ago

C is right This solution meets the requirements because: It creates a new Route 53 Resolver outbound endpoint, which enables the applications in the shared services VPC to resolve DNS for on-premises hosted domains. It associates forwarding rules with this new Resolver endpoint and each application VPC, ensuring that the applications can resolve local VPC domain names and domains hosted in Amazon Route 53 private hosted zones. It updates each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint, allowing the applications to continue resolving both on-premises and internal AWS domains without any disruptions.

Raphaello 1 year, 5 months ago

Selected Answer: B

B is the correct answer.

Arad 1 year, 10 months ago

Selected Answer: B

B is the correct answer.

neotusca 2 years ago

Absolutely B. I don't know why suggested answer is A.

evargasbrz 2 years, 1 month ago

Selected Answer: B

Definitely option B. Outbound resolver + forwarding rule

Pratap 2 years, 3 months ago

B, VPC DHCP option set need should be AmazonProvided DNS (Default)

ITgeek 2 years, 5 months ago

Selected Answer: B

Outbound resolver + forwarding rule

Spike2020 2 years, 5 months ago

Answer is B you need an outboud R53 resolver to resolve on premise domains.

https://zhangxuetu.online

[202610]

Question #85 Topic 1

A company has been using an outdated application layer protocol for communication among applications. The company decides not to use this protocol anymore and must migrate all applications to support a new protocol. The old protocol and the new protocol are TCP-based, but the protocols use different port numbers.

After several months of work, the company has migrated dozens of applications that run on Amazon EC2 instances and in containers. The company believes that all the applications have been migrated, but the company wants to verify this belief. A network engineer needs to verify that no application is still using the old protocol.

Which solution will meet these requirements without causing any downtime?

A. Use Amazon Inspector and its Network Reachability rules package. Wait until the analysis has finished running to find out which EC2 instances are still listening to the old port.

B. Enable Amazon GuardDuty. Use the graphical visualizations to filter for traffic that uses the port of the old protocol. Exclude all internet traffic to filter out occasions when the same port is used as an ephemeral port.

C. Configure VPC flow logs to be delivered into an Amazon S3 bucket. Use Amazon Athena to query the data and to filter for the port number that is used by the old protocol. **Most Voted**

D. Inspect all security groups that are assigned to the EC2 instances that host the applications. Remove the port of the old protocol if that port is in the list of allowed ports. Verify that the applications are operating properly after the port is removed from the security groups.

Correct Answer: C

Community vote distribution



Comments

Wiss7 **Highly Voted** 2 years, 8 months ago

Selected Answer: C

simplest / no agents /

woorkim 1 year, 4 months ago

C is correct!

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the most logical answer.

WherecanIstart 2 years, 1 month ago

Correct answer is C

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: C

Correct answer is C.

ITgeek 2 years, 10 months ago

Selected Answer: C

Its the simplest C

rhinozD 2 years, 10 months ago

Selected Answer: C

I think C is enough to confirm.

symplesims 2 years, 11 months ago

For AWS Inspector, an agent is required on the EC2 instances, and it accesses them for security assessments, which can impact the workload. Therefore, wouldn't it be more appropriate to analyze VPC Flow Logs in this situation?

Kristin01 2 years, 11 months ago

Selected Answer: C

i think C

SAPALL 2 years, 11 months ago

Selected Answer: A

I'll go with a

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #86 Topic 1

A company has deployed its AWS environment in a single AWS Region. The environment consists of a few hundred application VPCs, a shared services VPC, and a VPN connection to the company's on-premises environment. A network engineer needs to implement a transit gateway with the following requirements:

• Application VPCs must be isolated from each other.
• Bidirectional communication must be allowed between the application VPCs and the on-premises network.
• Bidirectional communication must be allowed between the application VPCs and the shared services VPC.

The network engineer creates the transit gateway with options disabled for default route table association and default route table propagation. The network engineer also creates the VPN attachment for the on-premises network and creates the VPC attachments for the application VPCs and the shared services VPC.

The network engineer must meet all the requirements for the transit gateway by designing a solution that needs the least number of transit gateway route tables.

Which combination of actions should the network engineer perform to accomplish this goal? (Choose two.)

A. Configure a separate transit gateway route table for on premises. Associate the VPN attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

B. Configure a separate transit gateway route table for each application VPC. Associate each application VPC attachment with its respective transit gateway route table. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.

C. Configure a separate transit gateway route table for all application VPCs. Associate all application VPCs with this transit gateway route table. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table. Most Voted

D. Configure a separate transit gateway route table for the shared services VPC. Associate the shared services VPC attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

E. Configure a separate transit gateway route table for on premises and the shared services VPC. Associate the VPN attachment and the shared services VPC attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table. Most Voted

Correct Answer: CE

Community vote distribution



Comments

Kristin01 Highly Voted 2 years, 11 months ago

Selected Answer: CE

CE is correct

netgeek1991 Highly Voted 2 years, 10 months ago

BE is correct. Option C is wrong because if we C. Configure a separate transit gateway route table for all application VPCs. Associate all application VPCs with this transit gateway route table. Then all the Application VPCs will be able to talk to each-other which breaks the requirement of isolating the communication between Application VPCs

netgeek1991 2 years, 10 months ago

Its C and E.

albertkr 2 years, 9 months ago

yeah, won't putting all application VPCs under the same routing table will enable the communication among the VPCs? I can't understand why people voted for B.

cerifyme85 1 year, 11 months ago

It wont.. the question says "Least amount of TGW RT".. so all in the same RT. Connectivity only happens when the routes are propagated to each other. APP vpcs ==> Assocaited to one table App VPCs ==> Propagated to shared VPn + Shared VPCs ==> Associated to Their RTs VPN + Shared VPC ==> Propagated to only AP VPCs

cerifyme85 1 year, 11 months ago

It wont.. the question says "Least amount of TGW RT".. so all in the same RT. Connectivity only happens when the routes are propagated to each other. APP vpcs ==> Assocaited to one table (1RT) App VPCs ==> Propagated to shared + VPN RT VPn + Shared VPCs ==> Associated to Their RT (1 RT) VPN + Shared VPC ==> Propagated to only APP VPCs

dspd 1 year, 1 month ago

Selected Answer: CE

best possible but E is still not correct, because In E, we propagate all application VPC attachments. will it not allow app VPC communication internally ?

woorkim 1 year, 4 months ago

C &E is correct!

AlohaEva 1 year, 7 months ago

Options B and E are correct Based on information here: https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html Example: Isolated VPCs or Isolated VPCs with shared services "Attachments associated with one isolated router can route packets to each other, but cannot route packets to or receive packets from the attachments for another isolated router" - it means that one route table for all attachments will allow communication between each other (which violates requirements) (Option B) In order to provide isolated application VPCs with Transit Gateway (Option E) In order to provide bidirectional communication between on-premises and shared-services VPC and bidirectional communication between application VPCs and the shared services VPC, option E is correct

Blitz1 1 year, 8 months ago

Selected Answer: CE

CE. BE is an option but with too many routing tables. And it seems that not all the ppl understood attachment vs propagation. In a transit gateway route table the routes(actual field in aws console) are coming from the propagation and not from attachment. The simple fact that you create association in the routing table with a transit gateway attachment(vpc) doesn't mean that you have you have transitivity (unless you add also the propagation)

Raphaello 1 year, 11 months ago

Selected Answer: CE

Think of it a 2 separate routing domains (VRF). Application VPCs routing table >> VPN & shared-services VPC routes VPN & Shared-services VPC routing table >> App VPCs routes C & E are the correct answers.

JoellaLi 1 year, 11 months ago

Selected Answer: BE

Each VPC has a route table, and the transit gateway has two route tables—one for the VPCs and one for the VPN connection and shared services VPC.

JoellaLi 1 year, 11 months ago

change to CE. If we configure a separate transit gateway route table for each application VPC and there are 3 application VPCs, then there will be 3 transit gateway route tables in total—one for each application VPC.

mrt261 2 years ago

Selected Answer: BE

Option B allows for isolating each application VPC by creating a separate transit gateway route table for each one. This ensures that communication between application VPCs is isolated. The shared services VPC attachment and the VPN attachment are propagated to each application VPC's transit gateway route table, allowing bidirectional communication with both. Option E creates a separate transit gateway route table for on-premises and the shared services VPC. This allows for efficient routing and isolation. All application VPC attachments are propagated to this transit gateway route table, ensuring bidirectional communication with both the on-premises network and the shared services VPC.

vikasj1in 2 years, 1 month ago

Selected Answer: CE

C) - Create a transit gateway route table specifically for all the application VPCs. - Associate all the application VPC attachments with this transit gateway route table. - Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table. E) - Create another transit gateway route table for on-premises and the shared services VPC. - Associate the VPN attachment and the shared services VPC attachment with this transit gateway route table. - Propagate all application VPC attachments to this transit gateway route table. This way, you can achieve the required isolation between application VPCs, allow bidirectional communication between application VPCs and the on-premises network, and enable communication between application VPCs and the shared services VPC. Using two separate transit gateway route tables helps organize the routing requirements efficiently.

mrt261 2 years ago

With option C, all application VPCs would share the same transit gateway route table, which means they would not be isolated from each other. This violates the requirement that application VPCs must be isolated from each other. Therefore, option C is not suitable for meeting the specified requirements.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is AE according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: CE

CE is the right answer.

az2022 2 years, 5 months ago

DE is correct

Tofu13 2 years, 6 months ago

Selected Answer: CE

C: Allows traffic to flow from App VPCs to Shared-Service VPC and to on-premise. E: Allows traffic to flow from Shared-Service VPC and on-premise to App VPCs. https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated-shared.html

alejo232425 2 years, 4 months ago

the link shared says what someone said above: "The first entry is the default entry for local routing in the VPC" you dont want that. so if you include all all of them will be reachable.

Certified101 2 years, 7 months ago

Selected Answer: CE

By implementing the steps in option C, you're providing the necessary isolation between the application VPCs while allowing for communication with the shared services VPC and the on-premises network. Option E then allows bidirectional communication between the on-premises network, the shared services VPC, and all application VPCs. This is achieved by creating a separate transit gateway route table for the shared services VPC and on-premises network, and propagating the routes of all application VPCs to this route table.

Neo00 2 years, 8 months ago

B,E is correct. C will make all application VPCs talks each other

Neo00 2 years, 8 months ago

I was wrong, should be CE.

JoellaLi 1 year, 11 months ago

Why change to CE?

Spaurito 1 year, 4 months ago

B is not defined in the requirements.

[Removed] 2 years, 8 months ago

Selected Answer: BD

Consider this that the application VPCs must be isolated from each other...

Spaurito 1 year, 4 months ago

B does provided that option but not defined in the requirements.

https://zhangxuetu.online

[202610]

Question #87 Topic 1

A company has an AWS Site-to-Site VPN connection between its existing VPC and on-premises network. The default DHCP options set is associated with the VPC. The company has an application that is running on an Amazon Linux 2 Amazon EC2 instance in the VPC. The application must retrieve an Amazon RDS database secret that is stored in AWS Secrets Manager through a private VPC endpoint. An on-premises application provides internal RESTful API service that can be reached by URL (https://api.example.internal). Two on-premises Windows DNS servers provide internal DNS resolution.

The application on the EC2 instance needs to call the internal API service that is deployed in the on-premises environment. When the application on the EC2 instance attempts to call the internal API service by referring to the hostname that is assigned to the service, the call fails. When a network engineer tests the API service call from the same EC2 instance by using the API service's IP address, the call is successful.

What should the network engineer do to resolve this issue and prevent the same problem from affecting other resources in the VPC?

A. Create a new DHCP options set that specifies the on-premises Windows DNS servers. Associate the new DHCP options set with the existing VPC. Reboot the Amazon Linux 2 EC2 instance.

B. Create an Amazon Route 53 Resolver rule. Associate the rule with the VPC. Configure the rule to forward DNS queries to the on-premises Windows DNS servers if the domain name matches example.internal. Most Voted

C. Modify the local host file in the Amazon Linux 2 EC2 instance in the VPMap the service domain name (api.example.internal) to the IP address of the internal API service.

D. Modify the local /etc/resolv.conf file in the Amazon Linux 2 EC2 instance in the VPC. Change the IP addresses of the name servers in the file to the IP addresses of the company's on-premises Windows DNS servers.

Correct Answer: B

Community vote distribution

B (94%) C (6%)

Comments

deepakno 8 months, 2 weeks ago

Selected Answer: B

Not A since change DHCP will impact entire VPC and the connection to secret manager

Gafa255 10 months, 1 week ago

Selected Answer: B

A is incorrect because if you change the DHCP options, this change applies to all VPCs.

woorkim 1 year, 4 months ago

B is right!

AlirezaNetWorld 1 year, 6 months ago

Why not A? I think it has all, we need to do to solve this issue for now and for the future

Gafa255 10 months, 1 week ago

Because you need to resolve RDS dns internally into VPC.

Raphaello 1 year, 11 months ago

Selected Answer: B

B is the correct answer, but it feels it could be better worded.

Arad 2 years, 4 months ago

Selected Answer: B

I think B is the correct answer.

ISSDoksim 2 years, 7 months ago

B - agreed

albertkr 2 years, 9 months ago

Selected Answer: B

voted for B

rhinozD 2 years, 10 months ago

Selected Answer: C

I just wonder why option C does not mention anything about the outbound endpoint. Can we direct do that without an outbound endpoint? I think C is doable.

tom_cat 2 years, 10 months ago

Yes, it will work but requirement is "prevent the same problem from affecting other resources in the VPC" and modifying file inside single instance won't do it.

Kristin01 2 years, 11 months ago

Selected Answer: B

B is correct

tom_cat 2 years, 11 months ago

Selected Answer: B

Should be B.

https://zhangxuetu.online

[202610]

Question #88 Topic 1

A company has several production applications across different accounts in the AWS Cloud. The company operates from the us-east-1 Region only. Only certain partner companies can access the applications. The applications are running on Amazon EC2 instances that are in an Auto Scaling group behind an Application Load Balancer (ALB). The EC2 instances are in private subnets and allow traffic only from the ALB. The ALB is in a public subnet and allows inbound traffic only from partner network IP address ranges over port 80.

When the company adds a new partner, the company must allow the IP address range of the partner network in the security group that is associated with the ALB in each account. A network engineer must implement a solution to centrally manage the partner network IP address ranges.

Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create an Amazon DynamoDB table to maintain all IP address ranges and security groups that need to be updated. Update the DynamoDB table with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges and security groups from the DynamoDB table to update the security groups. Deploy this solution in all accounts.

B. Create a new prefix list. Add all allowed IP address ranges to the prefix list. Use Amazon EventBridge (Amazon CloudWatch Events) rules to invoke an AWS Lambda function to update security groups whenever a new IP address range is added to the prefix list. Deploy this solution in all accounts.

C. Create a new prefix list. Add all allowed IP address ranges to the prefix list. Share the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM). Update security groups to use the prefix list instead of the partner IP address range. Update the prefix list with the new IP address range when the company adds a new partner. **Most Voted**

D. Create an Amazon S3 bucket to maintain all IP address ranges and security groups that need to be updated. Update the S3 bucket with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges and security groups from the S3 bucket to update the security groups. Deploy this solution in all accounts.

Correct Answer: C

Community vote distribution

C (100%)

Comments

tom_cat **Highly Voted** 2 years, 11 months ago

Selected Answer: C

C - prefix list.

woorkim 1 year, 4 months ago

c is correct. lambda has operation burdern!

Raphaello 1 year, 11 months ago

Selected Answer: C

C is the correct answer. Customer-managed prefix list.

mrt261 2 years ago

Selected Answer: C

Option C leverages AWS RAM to centrally manage the allowed IP address ranges using a prefix list. This approach eliminates the need to manually update security groups in each account when adding a new partner. By updating the prefix list, the changes are automatically propagated to all accounts sharing the prefix list, streamlining the management process. Options A, B, and D involve using AWS Lambda functions to read and update IP address ranges and security groups, which introduces additional complexity compared to leveraging AWS RAM for centralized management. Therefore, Option C is the most operationally efficient solution.

vikasj1in 2 years, 1 month ago

Selected Answer: C

- Create a new prefix list and add all allowed partner network IP address ranges to this prefix list.This prefix list acts as a centralized repository for managing the allowed IP address ranges. - Use AWS Resource Access Manager (AWS RAM) to share the prefix list across different AWS accounts. - Update the security groups associated with the ALB in each account to reference the shared prefix list instead of specifying individual partner IP address ranges. - When adding a new partner, simply update the shared prefix list with the new IP address range. All associated security groups automatically reflect this change. This solution ensures central management, reduces manual updates, and enhances scalability when adding new partners, making it operationally efficient for the given requirements.

Marfee400704 2 years, 1 month ago

I think that it' correct answer is C according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: C

C, no brainer!

tcp22 2 years, 10 months ago

C https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #89 Topic 1

A company uses a 1 Gbps AWS Direct Connect connection to connect its AWS environment to its on-premises data center. The connection provides employees with access to an application VPC that is hosted on AWS. Many remote employees use a company-provided VPN to connect to the data center. These employees are reporting slowness when they access the application during business hours. On-premises users have started to report similar slowness while they are in the office.

The company plans to build an additional application on AWS. On-site and remote employees will use the additional application. After the deployment of this additional application, the company will need 20% more bandwidth than the company currently uses. With the increased usage, the company wants to add resiliency to the AWS connectivity. A network engineer must review the current implementation and must make improvements within a limited budget.

What should the network engineer do to meet these requirements MOST cost-effectively?

A. Set up a new 1 Gbps Direct Connect dedicated connection to accommodate the additional traffic load from remote employees and the additional application. Create a link aggregation group (LAG).

B. Deploy an AWS Site-to-Site VPN connection to the application VPC. Configure the on-premises routing for the remote employees to connect to the Site-to-Site VPN connection. **Most Voted**

C. Deploy Amazon Workspaces into the application VPInstruct the remote employees to connect to Workspaces.

D. Replace the existing 1 Gbps Direct Connect connection with two new 2 Gbps Direct Connect hosted connections. Create an AWS Client VPN endpoint in the application VPC. Instruct the remote employees to connect to the Client VPN endpoint.

Correct Answer: B

Community vote distribution



Comments

tom_cat **Highly Voted** 2 years, 10 months ago

Selected Answer: D

A) If current 1 Gbps Direct Connect is not enough for on-premises users adding another 1 Gbps Direct Connect will not add resiliency. In case of one Direct Connect link failure there will be not enough bandwidth. Especially with new app and increased by 20% usage. B) No resiliency. In case of VPN S2S failure 1 Gbps Direct connect won't be sufficient for on-premises and remote users. C) Very expensive D) Should work. In case of one link failure single 2

Gbps Direct Connect hosted connection will be sufficient to handle all the traffic for on-premises users. Remote users will connect by AWS client VPN directly to VPC.

ChinkSantana 2 years, 2 months ago

With the increased usage, the company wants to add resiliency to the AWS connectivity. A network engineer must review the current implementation and must make improvements within a limited budget. Based on this requirement... B should be the answer

takecoffe Highly Voted 2 years, 10 months ago

Selected Answer: B

deploying an AWS Site-to-Site VPN connection and configuring on-premises routing for remote employees would be the most cost-effective solution while meeting the company's requirements for increased bandwidth and resiliency.

steli0 6 months ago

Selected Answer: B

I think the key is "the MOST cost effective" because both B and E will provide bad experience for remote users (maybe B even more since they will have an additional VPN hop). So B should be the right one having cost in mind because with E you also have the additional cost of AWS Client VPN.

Nouwara 10 months, 2 weeks ago

Selected Answer: B

split users: remote employees uses s2s et on-prem thru direct connect

8be7437 11 months ago

Selected Answer: A

D cannot be, 1 to 4Gb is way more than 20%... C is way to expensive, B doesn't add more BW. Cost effective is A. CostEffective means you pay what you get. and you got the 20% doubling with the LAG.

TechAwesome 1 year ago

Selected Answer: A

Obviously, correct answer is A. Although, option B has low cost, but it won't solve your slow issue, since VPN connection can reach 1.25Gbps maximum. Your company need more than 1.2Gbps in this case.

dspd 1 year, 1 month ago

Selected Answer: B

Not A for sure - AWS Direct Connect LACP (Link Aggregation Control Protocol) does not work on 1 Gbps dedicated connections Even B is not good from resiliency... so ideally not all the answers are correct.... B is closest

46f094c 1 year, 2 months ago

Selected Answer: A

D is the most expensive... 4Gb BW plus VPN-client service In B there is no resiliency, it only says to re-route remote users through the S2S, not on-prem users too. C out So has to be A

AzureDP900 1 year, 2 months ago

The most cost-effective solution would be: Option B . Deploying an AWS Site-to-Site VPN connection to the application VPC. Configuring on-premises routing for remote employees to connect to the Site-to-Site VPN connection. This option provides a more cost-effective solution by leveraging the existing 1 Gbps Direct Connect connection and using the same infrastructure. Adding a new connection would be too expensive, whereas deploying an AWS Site-to-Site VPN connection is a more efficient use of resources. The other options are not correct because: Option A involves setting up a new direct connect link which will increase the cost. Option C introduces Amazon Workspaces which may add an additional layer of complexity and also incur costs.

Spaurito 1 year, 4 months ago

A - This is the better and most cost effective solution. You're not changing the architecture just increasing performance. You can use multiple connections to increase available bandwidth. A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection. LAGs streamline configuration because the LAG configuration applies to all connections in the group. https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html

VerRi 1 year, 6 months ago

Selected Answer: B

A) The bandwidth of DX is 1Gbps, which is also a bottleneck, creating a LAG can speed up On-premises to Global Acceleration Location only, it won't help to provide better performance. B) correct. C) ??? D) It provides more bandwidth but is expensive

AlirezaNetWorld 1 year, 6 months ago

A is the best answer

seochan 1 year, 9 months ago

Selected Answer: A

I don't understand why B should be the answer. The company is already using DX connection; there is no benefit even if you no longer use the existing DX connection. Just adding one more DX connection and aggregating via LAG would solve this problem cost-effectively. I know establishing an S2S connection has a lower initial cost, but it only makes sense when you use both of the connections (DX and S2S).

Marfee400704 2 years, 1 month ago

I think that it's correct answer is A according to SPOTO products.

GaryQian 2 years, 1 month ago

Selected Answer: B

Vote for B. The vpn is cheap compared with other options

michele_scar 2 years, 1 month ago

Selected Answer: B

Is the more cost-effectively solution. You already have a DX for user who needs AWS App; with the Site-to-site ONLY for the newest application you can use 1.25Gb in plus for that application and still continue using the old DX for others. Replacing 1 DX with 2 DX + AWS Client VPC should be very more expensive than 1 Site-to-site

jorgesoma 2 years, 2 months ago

Unclear correct answer. Please, provide correct answer.

https://zhangxuetu.online

[202610]

Question #90 Topic 1

A company has a global network and is using transit gateways to connect AWS Regions together. The company finds that two Amazon EC2 instances in different Regions are unable to communicate with each other. A network engineer needs to troubleshoot this connectivity issue.

What should the network engineer do to meet this requirement?

A. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables and in the VPC route tables. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

B. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. Use AWS Firewall Manager to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

C. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC. **Most Voted**

D. Use VPC Reachability Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

Correct Answer: C

Community vote distribution



Comments

ITgeek **Highly Voted** 2 years, 11 months ago

Selected Answer: C

Network analyzer with VPV flow logs

woorkim 1 year, 4 months ago

only c is correct!

Spaurito 1 year, 4 months ago

C - This the tool for the job to check TGW Route Tables. https://docs.aws.amazon.com/network-manager/latest/tgwnm/route-analyzer.html

Raphaello 1 year, 11 months ago

Selected Answer: C

When it comes to analyze routes through TGW, then use AWS Network Manager Route Analyzer. AWS Network Manager Route Analyzer analyzes routes in TGW route table ONLY. It does not analyze VPC route tables, SG's, nor ACL rules.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

task_7 2 years, 3 months ago

Selected Answer: D

. If the destination is not reachable, Reachability Analyzer identifies the blocking component. Network Access Analyzer is a feature that enables you to identify unintended network access to your resources on AWS. https://aws.amazon.com/about-aws/whats-new/2023/08/amazon-vpc-reachability-analyzer-vpc-network-access-analyzer-additional-region/#:~:text=If%20the%20destination%20is%20not,to%20your%20resources%20on%20AWS.

wmatos 2 years, 5 months ago

Selected Answer: C

CCCCCCCCCCCCC

chen0305_099 2 years, 6 months ago

Selected Answer: C

C C C C C C C

study_aws1 2 years, 11 months ago

C) is correct. https://docs.aws.amazon.com/network-manager/latest/tgwnm/route-analyzer.html

hankun 2 years, 11 months ago

AWS Network Manager Route Analyzer to analyze routes in the transit gateway. Route tables and in the VPC route tables will use VPC flow logs or Reachability Analyzer to analyze routes -> C

coolt2 2 years, 3 months ago

i see this on the link share "Note Route Analyzer does not work with intra-Region peering."

https://zhangxuetu.online

[202610]

Question #91 Topic 1

A company needs to transfer data between its VPC and its on-premises data center. The data must travel through a connection that has dedicated bandwidth. The data also must be encrypted in transit. The company has been working with an AWS Partner Network (APN) Partner to establish the connection.

Which combination of steps will meet these requirements? (Choose three.)

A. Request a hosted connection from the APN Partner. Most Voted

B. Request a hosted public VIF from the APN Partner.

C. Create an AWS Site-to-Site VPN connection. Most Voted

D. Create an AWS Client VPN connection.

E. Create a private VIF.

F. Create a public VIF. Most Voted

Correct Answer: ACF

Community vote distribution



Comments

lygf Highly Voted 2 years, 9 months ago

Selected Answer: ACF

You need public VIF in order to create a Site-to-Site VPN connection.

TravelKo Highly Voted 2 years, 8 months ago

ACF is correct. You need transit VIF for private VPN.

dcantos 9 months, 1 week ago

Selected Answer: ACF

This solution combines the benefits of the end-to-end secure IPsec connection with low latency and increased bandwidth of the AWS Direct Connect to provide a more consistent network experience than internet-based VPN connections. A BGP connection session is established between AWS Direct Connect and your router on the public VIF. Another BGP session or a static route will be established between the virtual private gateway and your router on the IPsec VPN tunnels.

ashk123456 11 months, 3 weeks ago

Selected Answer: ACE

The company needs: 1⃣ A dedicated bandwidth connection → This means they need AWS Direct Connect (DX). 2⃣ Encryption for data in transit → DX alone does not provide encryption, so they need AWS Site-to-Site VPN over DX. 3⃣ A connection established with an APN Partner → This suggests a hosted Direct Connect connection, since APN partners provide those.

49ca6f2 1 year, 2 months ago

Selected Answer: ACF

ACF , because you cannot create a S2S VPN on the Private VIF. You can either do it on Public VIF because it provides you with Public vpn endpoints or on Transit vif because you assign a TGW CIDR and then get the Private VPN IP from that CIDR

djangoGroup 1 year, 2 months ago

Selected Answer: ACE

A. Request a hosted connection from the APN Partner. • Reason: • A hosted connection provides dedicated bandwidth from the APN Partner. This satisfies the requirement for dedicated bandwidth. • APN Partners offer AWS Direct Connect hosted connections to simplify setup. • Correct. C. Create an AWS Site-to-Site VPN connection. • Reason: • A Site-to-Site VPN adds encryption to the traffic that flows over the Direct Connect connection. This satisfies the requirement for encryption in transit. • AWS Direct Connect alone does not provide encryption, so a VPN is necessary. • Correct. E. Create a private VIF. • Reason: • A private VIF connects the Direct Connect connection to a VPC. This enables private communication between the VPC and the on-premises environment. • Public VIFs are not suitable for this scenario because they expose public AWS endpoints. • Correct.

woorkim 1 year, 3 months ago

ACE Why not the other options? B. Request a hosted public VIF from the APN Partner: A public VIF is used to access AWS public services such as S3 and Systems Manager, not for private communication with a VPC. D. Create an AWS Client VPN connection: Client VPN is for remote user access, not for site-to-site connectivity. F. Create a public VIF: A public VIF does not support private communication with VPCs. It is used to access public AWS endpoints.

Spaurito 1 year, 4 months ago

ACE - Private VIF for the connection with Private IP VPN as per https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-site-to-site-vpn-private-ip-vpns/

1a17d1e 8 months, 1 week ago

This article is about private IP VPNs and says "Private IP VPN is deployed on top of Transit VIFs". The Q says nothing of transit GW's/VIFs.

hedglin 1 year, 7 months ago

Correct Answer : ACE. Option F is wrong. Private VIF (Virtual Interface) is the appropriate type of VIF for connecting to a VPC, as opposed to a public VIF which is used for accessing public AWS services.

michele_scar 2 years ago

Selected Answer: ACF

The PRIVATE VIF as a distractor is so bad :D

Spaurito 1 year, 4 months ago

I agree. A distractor for sure. So the question doesn't define private or public IP addressing. The only clue to me is the dedicated bandwidth which leads me to the Private VIF

Marfee400704 2 years, 1 month ago

I think that it's correct answer is ACE according to SPOTO products.

cumzle_com 2 years, 3 months ago

Selected Answer: ACF

Private IP VPN is deployed on top of Transit VIFs, so it allows you to use AWS Transit Gateway for centralized management of customers' Virtual Private Clouds (VPCs) and connections to the on-premises networks in a more secured, private and scalable manner.

Tofu13 2 years, 6 months ago

Selected Answer: ACF

U need a public VIF because traditionally the VPN tunnels in S2S VPN use public IPs. However, since last year it is possible to use private IPs as well with a transit VIF. https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-site-to-site-vpn-private-ip-vpns/

evargasbrz 2 years, 7 months ago

Selected Answer: ACF

ACF is the right option here. If we had a TGW, we could consider the following: Private IP VPN is deployed on top of Transit VIFs, so it allows you to use AWS Transit Gateway for centralized management of customers' Virtual Private Clouds (VPCs) and connections to the on-premises networks in a more secured, private and scalable manner." so, you must use a public VIF in order to create a Site-to-Site VPN connection

Wiss7 2 years, 8 months ago

Selected Answer: ACF

IPsec on DX is either on Transit VIF or Public VIF

JosMo 2 years, 8 months ago

Selected Answer: ACE

you don't need a public VIF for this, so F is wrong

JosMo 2 years, 8 months ago

quote "That's why we are announcing Private IP VPN, a new feature that provides customers the ability to deploy AWS Site-to-Site VPN connections over Direct Connect using private IP addresses (RFC1918). With this feature, customers can encrypt traffic between their on-premises networks and AWS via Direct Connect connections without the need for public IP addresses, thus enabling enhanced security and network privacy at the same time. Private IP VPN is deployed on top of Transit VIFs, so it allows you to use AWS Transit Gateway for centralized management of customers' Virtual Private Clouds (VPCs) and connections to the on-premises networks in a more secured, private and scalable manner." https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-site-to-site-vpn-private-ip-vpns/

cumzle_com 2 years, 3 months ago

Private IP VPN is deployed on top of Transit VIFs, so it allows you to use AWS Transit Gateway for centralized management of customers' Virtual Private Clouds (VPCs) and connections to the on-premises networks in a more secured, private and scalable manner.

Cheam 2 years, 5 months ago

"Private IP VPN is deployed on top of Transit VIFs" - there's no Transit VIF in the answer choices, so the answer is ACF. All the best.

Balasmaniam 2 years, 9 months ago

A Private IP VPN connection requires a Direct Connect gateway and a Transit VIF as the underlying transport. https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-site-to-site-vpn-private-ip-vpns/

Balasmaniam 2 years, 9 months ago

Answer : ACF

https://zhangxuetu.online

[202610]

Question #92 Topic 1

A company's security guidelines state that all outbound traffic from a VPC to the company's on-premises data center must pass through a security appliance. The security appliance runs on an Amazon EC2 instance. A network engineer needs to improve the network performance between the on-premises data center and the security appliance.

Which actions should the network engineer take to meet these requirements? (Choose two.)

A. Use an EC2 instance that supports enhanced networking. **Most Voted**

B. Send outbound traffic through a transit gateway.

C. Increase the EC2 instance size. **Most Voted**

D. Place the EC2 instance in a placement group within the VPC.

E. Attach multiple elastic network interfaces to the EC2 instance.

Correct Answer: AC

Community vote distribution



Comments

Training **Highly Voted** 2 years, 9 months ago

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-networking.html

Training 2 years, 9 months ago

Correct Answer: AD

hogtrough 1 year, 9 months ago

I'm sorry but this is not correct. It clearly states that Placement Groups improve networking for EC2 instances only. Since this is connectivity between on prem traffic and a single EC2 instance, placement groups have zero value in this scenario. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Cheam **Highly Voted** 2 years, 7 months ago

Selected Answer: AC

1) The security appliance runs on an Amazon EC2 instance 2) Needs to improve the network performance between the on-premises data center and the security appliance. Placement Groups is to allow better throughput between EC2 instances in your VPC. This does not improve throughput between the SINGULAR EC2 security appliance (security appliance runs on an Amazon EC2 instance) and on-prem DC. Therefore, increasing instance size (more vCPU/RAM) is the correct answer. Ref: Look at Table 1 and 2, last page of this document

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/vm-series-spec-sheet All the best.

8be7437 11 months ago

Selected Answer: AD

"To increase network performance and reduce latency, you can launch instances in a placement group." even the wording is exact

49ca6f2 1 year, 2 months ago

Selected Answer: AC

AC Sending traffic to TGW won't solve performance for EC2 . Placement group is good for increasing performance for inter-EC2 communication in a vpc. attaching multiple interfaces won't increase the performance for single flow.

AzureDP900 1 year, 2 months ago

A D is right A This feature provides better network performance by allowing the instance to communicate directly with a virtual local area network (VLAN) switch. It improves the instance's ability to handle large amounts of traffic and reduces latency. D Placement groups enable high-performance networking and storage for instances running in a high-throughput, low-latency configuration. This feature allows instances to communicate with each other faster than regular EC2 instances.

woorkim 1 year, 3 months ago

Selected Answer: AC

more CPU, more TP!

Spaurito 1 year, 4 months ago

A C are the answers. There is only a single EC2 instance, so placement groups have no benefit. Increasing the size for more resources or changing the instance type can offer better performance.

Blitz1 1 year, 8 months ago

Selected Answer: AC

Read https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-network-bandwidth.html The available network bandwidth of an instance depends on the number of vCPUs that it has. For example, an m5.8xlarge instance has 32 vCPUs and 10 Gbps network bandwidth, and an m5.16xlarge instance has 64 vCPUs and 20 Gbps network bandwidth. However, instances might not achieve this bandwidth; for example, if they exceed network allowances at the instance level, such as packet per second or number of tracked connections. How much of the available bandwidth the traffic can utilize depends on the number of vCPUs and the destination. For example, an m5.16xlarge instance has 64 vCPUs, so traffic to another instance in the Region can utilize the full bandwidth available (20 Gbps). However, traffic to another instance in a different Region can utilize only 50% of the bandwidth available (10 Gbps).

acloudguru 1 year, 11 months ago

Selected Answer: AD

C. Increase the EC2 instance size is not right, should change to 'type optimized for network performance, such as the C5n or R5n instance families.' not only sise

mrt261 2 years ago

Selected Answer: AE

Option A: Using an EC2 instance that supports enhanced networking can improve network performance by offloading network processing tasks to the underlying hardware, reducing latency and improving throughput. Option E: Attaching multiple elastic network interfaces (ENIs) to the EC2 instance can increase network capacity and distribute network traffic across multiple interfaces, effectively improving overall network performance.

evargasbrz 2 years, 7 months ago

Selected Answer: AC

A, C is the right. When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload. Take a look on this: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Certified101 2 years, 7 months ago

Selected Answer: AC

AC is correct - placement group is useless here It is used for multiple EC2's within a AZ (not VPC).

Wiss7 2 years, 8 months ago

Selected Answer: AD

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-networking.html

Rashen 2 years, 8 months ago

Agree as there is no use from the placement group if its a single ec2

JosMo 2 years, 8 months ago

Selected Answer: AC

like WartyWarthog mentioned, only one instance, so the placement groups are useless, increasing the instance size will give better througputs and cpu.

troopie22 2 years, 8 months ago

Selected Answer: AC

Placement groups are unrelated in this scenario with a single EC2 instance.

wartywarthog 2 years, 8 months ago

Should be AC. There is only one EC2 instance involved in this scenario so placement groups is not a good option.

https://zhangxuetu.online

[202610]

Question #93 Topic 1

A company's application team is unable to launch new resources into its VPC. A network engineer discovers that the VPC has run out of usable IP addresses. The VPC CIDR block is 172.16.0.0/16.

Which additional CIDR block can the network engineer attach to the VPC?

A. 172.17.0.0/29

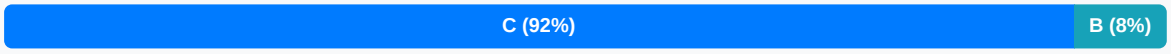
B. 10.0.0.0/16

C. 172.17.0.0/16 **Most Voted**

D. 192.168.0.0/16

Correct Answer: C

Community vote distribution



Comments

albertkr **Highly Voted** 2 years, 9 months ago

Selected Answer: C

option A prefix length is too long (/29) option B and D cannot be associated with CIDR block from range 172.16.0.0/12 due to cidr block restrictions. it leaves option C as the feasible option.

49ca6f2 1 year, 2 months ago

Selected Answer: B

This question has two correct answers : B and D. You can only add non overlapping CIDR as additional cidr.

Spaurito 1 year, 4 months ago

B is the correct answer. If you're adding a CIDR Block to the VPC you can't have overlap with the existing VPC CIDR. C would overlap adding that block and actually can't be done as mentioned by evargasbrz. The correct answer is B

Ravan 1 year, 7 months ago

Selected Answer: C

C. 172.17.0.0/16 Explanation: The current VPC has a CIDR block of 172.16.0.0/16, which falls within the 172.16.0.0/12 range. According to AWS documentation, you can add additional CIDR blocks from the 172.16.0.0/12 range (which includes 172.16.0.0/16 to 172.31.0.0/16), provided they do not overlap with the existing CIDR block. 172.17.0.0/16 is a valid CIDR block within the 172.16.0.0/12 range, and it does not overlap with the existing 172.16.0.0/16 CIDR block. Option A (172.17.0.0/29) and Option B (10.0.0.0/16) are also valid CIDR blocks, but the /29

block would provide too few IP addresses, and Option B is from a different RFC 1918 range, which is not the most straightforward choice for expanding within the same address space.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

evargasbrz 2 years, 7 months ago

Selected Answer: B

B -> is the right answer here. Guys, you are not able to add any one of the following CIDRs A. 172.17.0.0/29 C. 172.17.0.0/16 D. 192.168.0.0/16

shinzor 2 years, 4 months ago

You can't associate a different CIDR range if you already use a block from 172.16.0.0/12 (which includes A and C, so for sure not B and D. However A is way too less IP addresses, so only viable option would be C

demoras 2 years, 9 months ago

Selected Answer: C

The correct answer is C

demoras 2 years, 9 months ago

The correct answer is C

Ayptek 2 years, 9 months ago

Selected Answer: C

The correct answer is C

takecoffe 2 years, 9 months ago

Selected Answer: C

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html#add-cidr-block-restrictions Only it will also us to add 172.17.0.0/16

Training 2 years, 9 months ago

Important Some AWS services use the 172.17.0.0/16 CIDR range. To avoid future conflicts, don’t use this range when creating your VPC. For example, services like AWS Cloud9 or Amazon SageMaker can experience IP address conflicts if the 172.17.0.0/16 IP address range is already in use anywhere in your network. For more information, see Can't connect to EC2 environment because VPC's IP addresses are used by Docker in the AWS Cloud9 User Guide.

JosMo 2 years, 8 months ago

https://docs.aws.amazon.com/cloud9/latest/user-guide/troubleshooting.html#docker-bridge

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #94 Topic 1

A financial trading company is using Amazon EC2 instances to run its trading platform. Part of the company's trading platform includes a third-party pricing service that the EC2 instances communicate with over UDP on port 50000.

Recently, the company has had problems with the pricing service. Some of the responses from the pricing service appear to be incorrectly formatted and are not being processed successfully. The third-party vendor requests access to the data that the pricing service is returning. The third-party vendor wants to capture request and response data for debugging by logging in to an EC2 instance that accesses the pricing service. The company prohibits direct access to production systems and requires all log analysis to be performed in a dedicated monitoring account.

Which set of steps should a network engineer take to capture the data and meet these requirements?

A. 1. Configure VPC flow logs to capture the data that flows in the VPC.
2. Send the data to an Amazon S3 bucket.
3. In the monitoring account, extract the data that flows to the EC2 instance's IP address and filter the traffic for the UDP data.
4. Provide the data to the third-party vendor.

B. 1. Configure a traffic mirror filter to capture the UDP data.
2. Configure Traffic Mirroring to capture the traffic for the EC2 instance's elastic network interface.
3. Configure a packet inspection package on a new EC2 instance in the production environment. Use the elastic network interface of the new EC2 instance as the target for the traffic mirror.
4. Extract the data by using the packet inspection package.
5. Provide the data to the third-party vendor.

C. 1. Configure a traffic mirror filter to capture the UDP data.
2. Configure Traffic Mirroring to capture the traffic for the EC2 instance's elastic network interface.
3. Configure a packet inspection package on a new EC2 instance in the monitoring account. Use the elastic network interface of the new EC2 instance as the target for the traffic mirror.
4. Extract the data by using the packet inspection package.
5. Provide the data to the third-party vendor. **Most Voted**

D. 1. Create a new Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to the EC2 instance.
2. Log in to the EC2 instance in the production environment. Run the tcpdump command to capture the UDP data on the EBS volume.
3. Export the data from the EBS volume to Amazon S3.
4. Provide the data to the third-party vendor.

Correct Answer: C

Community vote distribution

C (100%)

Comments

albertkr Highly Voted 2 years, 3 months ago

Selected Answer: C

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

Marfee400704 1 year, 7 months ago

I think that it's correct answer is C accorinding to SPOTO products.

Arad 1 year, 10 months ago

Selected Answer: C

C is the right answer.

Arad 1 year, 10 months ago

C is the right answer.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #95 Topic 1

A company's network engineer is configuring an AWS Site-to-Site VPN connection between a transit gateway and the company's on-premises network. The Site-to-Site VPN connection is configured to use BGP over two tunnels in active/active mode with equal-cost multi-path (ECMP) routing activated on the transit gateway.

When the network engineer attempts to send traffic from the on-premises network to an Amazon EC2 instance, traffic is sent over the first tunnel. However, return traffic is received over the second tunnel and is dropped at the customer gateway. The network engineer must resolve this issue without reducing the overall VPN bandwidth.

Which solution will meet these requirements?

A. Configure the customer gateway to use AS PATH prepending and local preference to prefer one tunnel over the other.

B. Configure the Site-to-Site VPN options to set the first tunnel as the primary tunnel to eliminate asymmetric routing.

C. Configure the virtual tunnel interfaces on the customer gateway to allow asymmetric routing. **Most Voted**

D. Configure the Site-to-Site VPN to use static routing in active/active mode to ensure that traffic flows over a preferred path.

Correct Answer: C

Community vote distribution

C (100%)

Comments

tcp22 **Highly Voted** 2 years, 9 months ago

it's C Note: With an Active/Active configuration, the customer gateway must have Asymmetric routing activated on the virtual tunnel interfaces. https://repost.aws/knowledge-center/vpn-configure-tunnel-preference

woorkim 1 year, 3 months ago

only C is correct!

Spaurito 1 year, 4 months ago

C - The tunnel needs Asymmetric Routing Static VPNs created between a customer gateway and either a virtual private gateway or a transit gateway In this scenario, the virtual private gateway or transit gateway sends traffic from AWS to the on-premises network on a single VPN tunnel. This tunnel is randomly chosen by AWS and is referred to

as the preferred tunnel. If the AWS VPN connection (static routing type) has an Active/Active configuration (both tunnels are UP), then you can't configure AWS to prefer a specific tunnel to send traffic. For example, tunnel A was randomly chosen by AWS as the preferred VPN tunnel for sending traffic from AWS to the on-premises network. If tunnel A goes down, then traffic from AWS automatically fails over to tunnel B. Note: With an Active/Active configuration, the customer gateway must have Asymmetric routing activated on the virtual tunnel interfaces.

mrt261 2 years ago

Selected Answer: C

In an Active/Active configuration with ECMP routing, where both tunnels are utilized simultaneously, enabling asymmetric routing on the virtual tunnel interfaces of the customer gateway is indeed necessary to accommodate the bidirectional flow of traffic over the two tunnels.

WherecanIstart 2 years, 1 month ago

Selected Answer: C

Asymmetric Routing has to be allowed on the customer gateway...

vikasj1in 2 years, 1 month ago

Selected Answer: C

Configure the virtual tunnel interfaces on the customer gateway to allow asymmetric routing. This will: Allow return traffic to flow over different tunnel than initial traffic Maintain full bandwidth of both tunnels with active/active VPN Not require modifying BGP settings or preferring a tunnel The other options do not fully meet the needs: A – AS PATH prepending impacts overall BGP behavior B – Specifying a primary tunnel reduces equal bandwidth use D – Static routing disables ECMP and load balancing

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: C

C is the right answer.

Josh1217 2 years, 8 months ago

Selected Answer: C

Every other option except option C will reduce overall bandwidth.

Balasmaniam 2 years, 9 months ago

Selected Answer: C

Must be C, The static route will prefer specific link so without reducing BW, we can enable asymmetric routing to utilize both links.

AJ7428 2 years, 9 months ago

Should be D.

tcp22 2 years, 9 months ago

it's C Note: With an Active/Active configuration, the customer gateway must have Asymmetric routing activated on the virtual tunnel interfaces. https://repost.aws/knowledge-center/vpn-configure-tunnel-preference

Training 2 years, 9 months ago

https://repost.aws/knowledge-center/vpn-configure-tunnel-preference

Training 2 years, 9 months ago

If the AWS VPN connection (static routing type) has an Active/Active configuration (both tunnels are UP), then you can't configure AWS to prefer a specific tunnel to send traffic. For example, tunnel A was randomly chosen by AWS as the preferred VPN tunnel for sending traffic from AWS to the on-premises network. If tunnel A goes down, then traffic from AWS automatically fails over to tunnel B.

AJ7428 2 years, 9 months ago

Changing to C.

https://zhangxuetu.online

[202610]

Question #96 Topic 1

A company runs an application on Amazon EC2 instances. A network engineer implements a NAT gateway in the application's VPC to replace self-managed NAT instances. After the network engineer shifts traffic from the self-managed NAT instances to the NAT gateway, users begin to report issues.

During troubleshooting, the network engineer discovers that the connection to the application is closing after approximately 6 minutes of inactivity.

What should the network engineer do to resolve this issue?

A. Check for increases in the IdleTimeoutCount Amazon CloudWatch metric for the NAT gateway. Configure TCP keepalive on the application EC2 instances. **Most Voted**

B. Check for increases in the ErrorPortAllocation Amazon CloudWatch metric for the NAT gateway. Configure an HTTP timeout value on the application EC2 instances.

C. Check for increases in the PacketsDropCount Amazon CloudWatch metric for the NAT gateway. Configure an HTTPS timeout value on the application EC2 instances.

D. Check for decreases in the ActiveConnectionCount Amazon CloudWatch metric for the NAT gateway. Configure UDP keepalive on the application EC2 instances.

Correct Answer: A

Community vote distribution

A (100%)

Comments

Balasmaniam **Highly Voted** 2 years, 9 months ago

Selected Answer: A

Answer : A Internet connection drops after 350 seconds Problem Your instances can access the internet, but the connection drops after 350 seconds. Cause If a connection that's using a NAT gateway is idle for 350 seconds or more, the connection times out. When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet). Solution To prevent the connection from being dropped, you can initiate more traffic over the connection. Alternatively, you can enable TCP keepalive on the instance with a value less than 350 seconds.

woorkim 1 year, 3 months ago

ONLY A is correct!

Arad 2 years, 4 months ago

Selected Answer: A

A is the right answer.

tcp22 2 years, 9 months ago

A for sure

https://zhangxuetu.online

[202610]

Question #97 Topic 1

A software-as-a-service (SaaS) company is migrating its private SaaS application to AWS. The company has hundreds of customers that connect to multiple data centers by using VPN tunnels. As the number of customers has grown, the company has experienced more difficulty in its effort to manage routing and segmentation of customers with complex NAT rules.

After the migration to AWS is complete, the company's AWS customers must be able to access the SaaS application directly from their VPCs. Meanwhile, the company's on-premises customers still must be able to connect through IPsec encrypted tunnels.

Which solution will meet these requirements?

A. Connect the AWS customer VPCs to a shared transit gateway. Use AWS Site-to-Site VPN connections to the transit gateway for the on-premises customers

B. Use AWS PrivateLink to connect the AWS customers. Use a third-party routing appliance in the SaaS application VPC to terminate onpremises Site-to-Site VPN connections. Most Voted

C. Peer each AWS customer's VPCs to the VPC that hosts the SaaS application. Create AWS Site-to-Site VPN connections on the SaaS VPC virtual private gateway.

D. Use Site-to-Site VPN tunnels to connect each AWS customer's VPCs to the VPC that hosts the SaaS application. Use AWS Site-to-Site VPN to connect the on-premises customers.

Correct Answer: B

Community vote distribution



Comments

lygf Highly Voted 2 years, 9 months ago

Selected Answer: B

You don't want to mess with customer's AWS VPC, whether via VPC peering or Transit gateway. The standard solution is always VPC endpoint with AWS Privatelink.

albertkr 2 years, 9 months ago

it is very unlikely that the solution expected from the question is from a different appliance from AWS. in this answer, it uses another routing appliance to provide the VPN solution for on-prem customers.

Balasmaniam Highly Voted 2 years, 9 months ago

Selected Answer: B

kry point " the company has experienced more difficulty in its effort to manage routing and segmentation of customers with complex NAT rules." do again routing on TGW required ? Ans B.

Balasmaniam 2 years, 9 months ago

key point " the company has experienced more difficulty in its effort to manage routing and segmentation of customers with complex NAT rules." do need routing again on TGW required ? Ans B.

steli0 6 months ago

Selected Answer: B

I chose A since I assumed that is more complicated to configure a 3rd part appliance rather than an AWS IPSec VPN BUT the key point as mentioned by Balasmaniam is the complex routing and NAT. With option A you need to configure all TGWs (Even auto propagation/route-table assignment would help) whereas with B is only to configure routing for on-premise customers so B wins. The question could be phrased better as which solution would have the least operational overhead.

572ffdd 1 year, 2 months ago

Selected Answer: A

AWS PrivateLink is ideal for connecting AWS customers but does not support routing or IPsec connections for on-premises customers. Using a third-party routing appliance introduces additional complexity, cost, and potential performance bottlenecks.

Christina666 1 year, 4 months ago

Selected Answer: A

should be A

Akivox 1 year, 7 months ago

A is the correct answer. Why do you even need private links and a third party appliance? Why complicate it again when this can be simply done using the Transit Gateway?

incorrigble_maverick 2 years, 3 months ago

agreed, B is the right answer

Fukat 2 years, 8 months ago

Selected Answer: B

Going with B Though A is correct as well but there are some problems choosing that option 1] Company already experienced issues in managing growing customer base. with Option A, company has to share TGW with each new customer then they will attach their VPC and configure routing on their VPC. Plus company will have to edit TGW route table as well as application VPC route table for connectivity. So it not a good option if company is switching to new option to better manage growing cx need 2] Question mentions that "Saas application should be accessible DIRECTLY from cx VPC". With Option A, it not accessed directly cause we are routing the traffic via TGW to VPC and then to the actual application EC2 Thus, overall Option B is correct

trap 2 years, 9 months ago

B is the correct The is an adjustable limit of 50 with s2s vpn connections and customer gateways per Region. https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-limits.html Private link for connecting from customer's vpc and third party appliances for multiple s2s vpn connections with customers data centers seems to be the best solution

albertkr 2 years, 9 months ago

Selected Answer: A

vote for A

Training 2 years, 9 months ago

Should be A

lygf 2 years, 9 months ago

and then allow each customer's VPC to access other customers' VPCs freely?

albertkr 2 years, 9 months ago

you can create multiple routing tables in TGW to prevent customer VPCs communicating each other.

Cheam 2 years, 7 months ago

This will not work as the VPC hosting the SaaS application can only be associated to a single TGW route table and therefore will lead to the condition has lygf has stated. Answer A is not correct. All the best.

sdey0008 2 years, 9 months ago

Yes A is the correct answer

https://zhangxuetu.online

[202610]

Question #98 Topic 1

A company's existing AWS environment contains public application servers that run on Amazon EC2 instances. The application servers run in a VPC subnet. Each server is associated with an Elastic IP address.

The company has a new requirement for firewall inspection of all traffic from the internet before the traffic reaches any EC2 instances. A security engineer has deployed and configured a Gateway Load Balancer (GLB) in a standalone VPC with a fleet of third-party firewalls.

How should a network engineer update the environment to ensure that the traffic travels across the fleet of firewalls?

A. Deploy a transit gateway. Attach a GLB endpoint to the transit gateway. Attach the application VPC to the transit gateway. Update the application subnet route table's default route destination to be the GLB endpoint. Ensure that the EC2 instances' security group allows traffic from the GLB endpoint.

B. Update the application subnet route table to have a default route to the GLOn the standalone VPC that contains the firewall fleet, add a route in the route table for the application VPC's CIDR block with the GLB endpoint as the destination. Update the EC2 instances' security group to allow traffic from the GLB.

C. Provision a GLB endpoint in the application VPC in a new subnet. Create a gateway route table with a route that specifies the application subnet CIDR block as the destination and the GLB endpoint as the target. Associate the gateway route table with the internet gateway in the application VPUpdate the application subnet route table's default route destination to be the GLB endpoint. Most Voted

D. Instruct the security engineer to move the GLB into the application VPC. Create a gateway route table. Associate the gateway route table with the application subnet. Add a default route to the gateway route table with the GLB as its destination. Update the route table on the GLB to direct traffic from the internet gateway to the application servers. Ensure that the EC2 instances' security group allows traffic from the GLB.

Correct Answer: C

Community vote distribution

C (73%) A (27%)

Comments

lygf Highly Voted 2 years, 9 months ago

Selected Answer: C

A is ridiculous -> attach a GWLB endpoint to transit gateway??? B is incorrect - need to inspect all traffic FROM the Internet, not the other way D. is incorrect -> IGW needs a route to re-direct traffic to GWLB, you can't do that from

GWLB's route table.

Balasmaniam 2 years, 9 months ago

Since GWLB Endpoints are a routable target, you can route traffic moving to and from Transit Gateway to the fleet of virtual appliances that are configured as targets behind a GWLB. https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/

trap 2 years, 9 months ago

That's correct: https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html GWLB endpoint in A answer doesn't make any sense.

albertkr 2 years, 9 months ago

why A is not possible? This reference architecture outlines that it is how it is supposed to be designed: https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/ my only confusion about A is the application vpc sets the default route to GLB endpoint. My understanding as of the reference above, the default route should be targeted to TGW, not GLB endpoint.

JoellaLi 1 year, 11 months ago

yes seems that this sentence is wrong

Balasmaniam Highly Voted 2 years, 9 months ago

Selected Answer: A

https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-gwlb-with-tg-for-cns.html

Spaurito 1 year, 4 months ago

C - as per AI "No, you cannot directly attach a gateway endpoint to a Transit Gateway in AWS; a Transit Gateway is designed to connect entire VPCs, not specific endpoints within a VPC, so you would attach the entire VPC containing the gateway endpoint to the Transit Gateway instead."

Arad 2 years, 4 months ago

Selected Answer: C

C is the correct answer.

luisfsm_111 2 years, 6 months ago

Selected Answer: A

Really hard to choose between A and C, but by this design it looks like A because of the "Provision a GLB endpoint in the application VPC in a new subnet" part: https://docs.paloaltonetworks.com/vm-series/10-1/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/vm-series-integration-with-gateway-load-balancer

JosMo 2 years, 8 months ago

Selected Answer: C

should be C

AJ7428 2 years, 9 months ago

Selected Answer: C

Should be C. We need a ingress route table associated with IGW for traffic coming from Internet and routed towards F/W subnet.

tcp22 2 years, 9 months ago

The only issue I have with A is no sign of appliance mode, I go with C.

scrawnyfeel 2 years, 9 months ago

Should be C.

papercuts23 2 years, 9 months ago

"Attach a GLB endpoint to the transit gateway". Is that possible?

[Removed] 2 years, 8 months ago

Yes it's possible. https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-gwlb-with-tg-for-cns.html

KobDragoon 1 year, 11 months ago

No it's not, you don't attach a GLB endpoint to the transit gateway. that's not a thing. You can have Transit gateway VPC attachements,VPN attachments, Peering connection attachments or Connect attachments. But not GWLB endpoints attachments.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #99 Topic 1

A company has an AWS Site-to-Site VPN connection between its office and its VPC. Users report occasional failure of the connection to the application that is hosted inside the VPC. A network engineer discovers in the customer gateway logs that the Internet Key Exchange (IKE) session ends when the connection to the application fails.

What should the network engineer do to bring up the IKE session if the IKE session goes down?

A. Set the dead peer detection (DPD) timeout action to Clear. Initiate traffic from the VPC to on premises.

B. Set the dead peer detection (DPD) timeout action to Restart. Initiate traffic from on premises to the VPC. **Most Voted**

C. Set the dead peer detection (DPD) timeout action to None. Initiate traffic from the VPC to on premises.

D. Set the dead peer detection (DPD) timeout action to Cancel. Initiate traffic from on premises to the VPC.

Correct Answer: B

Community vote distribution

B (100%)

Comments

vikasj1in **Highly Voted** 1 year, 7 months ago

Selected Answer: B

Dead Peer Detection (DPD) is a method used to detect if the peer in a VPN connection is no longer reachable. By setting the DPD timeout action to "Restart," the VPN endpoint will attempt to re-establish the IKE session if it detects that the peer is no longer reachable. Initiating traffic from on premises to the VPC can trigger this process and bring up the IKE session if it has gone down.

Arad 1 year, 10 months ago

Selected Answer: B

Correct answer is B.

takecoffe 2 years, 3 months ago

Selected Answer: B

https://docs.aws.amazon.com/vpn/latest/s2svpn/initiate-vpn-tunnels.html

Balasmaniam 2 years, 3 months ago

Selected Answer: B

correct ans : B

https://zhangxuetu.online

[202610]

Question #100 Topic 1

A network engineer is designing a hybrid networking environment that will connect a company's corporate network to the company's AWS environment. The AWS environment consists of 30 VPCs in 3 AWS Regions.

The network engineer needs to implement a solution to centrally filter traffic by using a firewall that the company's security team has approved. The solution must give all the VPCs the ability to connect to each other. Connectivity between AWS and the corporate network must meet a minimum bandwidth requirement of 2 Gbps.

Which solution will meet these requirements?

A. Deploy an IPsec VPN connection between the corporate network and a new transit gateway. Connect all VPCs to the transit gateway. Associate the approved firewall with the transit gateway.

B. Deploy a single 10 Gbps AWS Direct Connect connection between the corporate network and virtual private gateway of each VPC. Connect the virtual private gateways to a Direct Connect gateway. Build an IPsec tunnel to a new transit VPC. Deploy the approved firewall to the transit VPC.

C. Deploy two 1 Gbps AWS Direct Connect connections in different Direct Connect locations to connect to the corporate network. Build a transit VIF on each connection to a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway for each Region. Configure the VIFs to use equal-cost multipath (ECMP) routing. Connect all the VPCs in the three Regions to the transit gateway. Configure the transit gateway route table to route traffic to an inspection VPDeploy the approved firewall to the inspection VPC.

D. Deploy four 1 Gbps AWS Direct Connect connections in different Direct Connect locations to connect to the corporate network. Build a transit VIF on each connection to a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway for each Region. Connect the transit gateways by using a transit gateway peering attachment. Configure the VIFs to use equal-cost multipath (ECMP) routing. Configure transit gateway route tables to route traffic to an inspection VPC. Deploy the approved firewall to the inspection VPC. Most Voted

Correct Answer: D

Community vote distribution



Comments

Manh Highly Voted 2 years, 8 months ago

Selected Answer: D

This solution meets the requirements because: • It uses AWS Direct Connect, which provides a dedicated and private connection between the corporate network and AWS, with a minimum bandwidth of 2 Gbps (4 x 1 Gbps). • It uses a Direct Connect gateway, which allows multiple VPCs in different Regions to share the same Direct Connect connection. • It uses a transit gateway, which acts as a network hub that connects multiple VPCs and other networks, such as the corporate network and the inspection VPC. • It uses a transit gateway peering attachment, which enables routing between transit gateways in different Regions. • It uses ECMP routing, which allows traffic to be distributed across multiple paths for higher throughput and redundancy. • It uses an inspection VPC, which hosts the approved firewall and filters traffic between the corporate network and the AWS environment.

a0e6696 7 months ago

Selected Answer: D

Connectivity between the AWS is needed and TGW peering is needed. This rules out the Option-C and then correct answer is D

PRASAD180 1 year ago

Selected Answer: D

D is correct

AzureDP900 1 year, 2 months ago

D is right 1) Centrally filter traffic: The proposed solution involves a new transit gateway and an inspection VPC, which acts as a central point for filtering traffic. 2) All VPCs connect to each other: All VPCs in the three regions are connected to the transit gateway, allowing them to communicate with each other. 3)Minimum bandwidth requirement of 2 Gbps: The solution includes four 1 Gbps connections, which can be combined using ECMP routing and multi-attach attachments to provide a total minimum bandwidth of 2 Gbps.

woorkim 1 year, 3 months ago

D is correct!

Spaurito 1 year, 4 months ago

D - Key to the answer for VPC peering connectivity "Connect the transit gateways by using a transit gateway peering attachment."

Blitz1 1 year, 8 months ago

Selected Answer: D

i have read the answers several times and the debate is indeed between C and D. But i believe C) is excluded in the end because: 1) even if it is stating that is creating "a new transit gateway for each Region" after few phrases is saying "Connect all the VPCs in the three Regions to the transit gateway". Ups...you cannot connect all the VPCs in all the regions on only ONE transit gateway. Maybe is phrased bad(maybe they wanted to say something like: attach all the vpcs to their corresponding transit gateways in each region) or it's a big clue. And i believe is the clue. 2) in D we have a transit peering which is required by "The solution must give all the VPCs the ability to connect to each other" BUT this can be a benefit in the answer or a hint for actually disqualify the response. It is not saying in the question if traffic between regions should be inspected or not.(and i see that most of the ppl assumed that only traffic between on-prem and aws should be inspected) - this one is very tricky. So, yes i will go in the end with D just because of (1) and consider (2) a strange bonus.

Raphaello 1 year, 11 months ago

Selected Answer: D

D is the correct answer.

WherecanIstart 2 years, 1 month ago

Selected Answer: D

D is the correct answer. You need to peer the transit gateways.

Arad 2 years, 4 months ago

Selected Answer: D

I think the correct answer is D.

evargasbrz 2 years, 7 months ago

Selected Answer: C

C is the right, as D didn't say to Connect all the VPCs in the three Regions to the transit gateway. You have no VPCs connected to the TGW in each region, so C is the right.

DeathFrmAbv 2 years, 8 months ago

D provides transit gateway peering, the others don't, so D

troopie22 2 years, 8 months ago

Selected Answer: D

I think the key is the need for connecting all the VPCs in different regions together and you can only accomplish that with the TGW peering in D.

tcp22 2 years, 9 months ago

D for sure, C does not provide minimum2 Gbps in case of one DX goes down.

Balasmaniam 2 years, 9 months ago

Selected Answer: D

option C - each region has a DXGW but maximum 3 VPC can connect on single DXGW without TGW. Option : D , has TGW with DXGW can connect multiple VPC with TGW peering.

Balasmaniam 2 years, 9 months ago

one DXGW can connect maximum 10 VPC

albertkr 2 years, 9 months ago

correct

https://zhangxuetu.online

[202610]

Question #101 Topic 1

A company uses an AWS Direct Connect private VIF with a link aggregation group (LAG) that consists of two 10 Gbps connections. The company's security team has implemented a new requirement for external network connections to provide layer 2 encryption. The company's network team plans to use MACsec support for Direct Connect to meet the new requirement.

Which combination of steps should the network team take to implement this functionality? (Choose three.)

A. Create a new Direct Connect LAG with new circuits and ports that support MACsec. Most Voted

B. Associate the MACsec Connectivity Association Key (CAK) and the Connection Key Name (CKN) with the new LAG. Most Voted

C. Associate the Internet Key Exchange (IKE) with the existing LAG.

D. Configure the MACsec encryption mode on the existing LAG.

E. Configure the MACsec encryption mode on the new LAG. Most Voted

F. Configure the MACsec encryption mode on each Direct Connect connection that makes up the existing LAG.

Correct Answer: ABE

Community vote distribution

ABE (100%)

Comments

trap Highly Voted 2 years, 9 months ago

Correct:A,B,E To start using MACsec, you must turn the feature on when you create a dedicated connection
https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-lag.html
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-mac-sec-getting-started.html
https://docs.aws.amazon.com/directconnect/latest/UserGuide/associate-key-lag.html

Tofu13 2 years, 6 months ago

Perfect links, thanks.

woorkim 1 year, 3 months ago

Selected Answer: ABE

ABE is correct, no need to config old LAG.

cas_tori 1 year, 6 months ago

Selected Answer: ABE

this is ABE

Suresh108 2 years, 2 months ago

minus 'existing' keyword

passtest100 2 years, 5 months ago

should be C, D,F since LAG can be updated with MacSec mode rather than a new LAG should be created.
https://docs.aws.amazon.com/directconnect/latest/APIReference/API_UpdateLag.html

shinzor 2 years, 4 months ago

While it is true that you can update MacSec mode on an existing LAG. However the MacSec keys in this context are only based on CKN/CAK. So using IKE as an answer is a no and makes all the other "existing" answers invalid.

JosMo 2 years, 8 months ago

Selected Answer: ABE

abe is correct

https://zhangxuetu.online

[202610]

Question #102 Topic 1

A company recently implemented a security policy that prohibits developers from launching VPC network infrastructure. The policy states that any time a NAT gateway is launched in a VPC, the company's network security team must immediately receive an alert to terminate the NAT gateway. The network security team needs to implement a solution that can be deployed across AWS accounts with the least possible administrative overhead. The solution also must provide the network security team with a simple way to view compliance history.

Which solution will meet these requirements?

A. Develop a script that programmatically checks for NAT gateways in an AWS account, sends an email alert, and terminates the NAT gateway if a NAT gateway is detected. Deploy the script on an Amazon EC2 instance in each account. Use a cron job to run the script every 5 minutes. Log the results of the checks to an Amazon RDS for MySQL database.

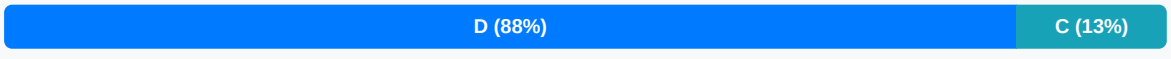
B. Create an AWS Lambda function that programmatically checks for NAT gateways in an AWS account, sends an email alert, and terminates the NAT gateway if a NAT gateway is detected. Deploy the Lambda function to each account by using AWS Serverless Application Model (AWS SAM) templates. Store the results of the checks on an Amazon OpenSearch Service cluster in each account.

C. Enable Amazon GuardDuty. Create an Amazon EventBridge rule for the Behavior:EC2/NATGatewayCreation GuardDuty finding type. Configure the rule to invoke an AWS Step Functions state machine to send an email alert and terminate a NAT gateway if a NAT gateway is detected. Store the runtime log as a text file in an Amazon S3 bucket.

D. Create a custom AWS Config rule that checks for NAT gateways in an AWS account. Configure the AWS Config rule to perform an AWS Systems Manager Automation remediation action to send an email alert and terminate the NAT gateway if a NAT gateway is detected. Deploy the AWS Config rule and the Systems Manager runbooks to each account by using AWS CloudFormation StackSets **Most Voted**

Correct Answer: D

Community vote distribution



Comments

trap **Highly Voted** 2 years, 9 months ago

Correct: D https://docs.aws.amazon.com/config/latest/developerguide/view-compliance-history.html
https://aws.amazon.com/blogs/mt/remediate-noncompliant-aws-config-rules-with-aws-systems-manager-automation-

runbooks/

woorkim 1 year, 3 months ago

Selected Answer: D

The best answer is D: Create a custom AWS Config rule that checks for NAT gateways in an AWS account. Configure the AWS Config rule to perform an AWS Systems Manager Automation remediation action to send an email alert and terminate the NAT gateway if a NAT gateway is detected. Deploy the AWS Config rule and the Systems Manager runbooks to each account by using AWS CloudFormation StackSets.

hcong 1 year, 7 months ago

Selected Answer: C

D is also a viable solution, but compared to GuardDuty, AWS Config may require more initial setup and ongoing management

Spaurito 1 year, 4 months ago

GaurdDuty can send alerts but is more usable with vulnerability compliance.

Tofu13 2 years, 6 months ago

Selected Answer: D

When in doubt regarding "Deploy the AWS Config rule and the Systems Manager runbooks to each account by using AWS CloudFormation StackSets " check below link: https://docs.aws.amazon.com/config/latest/developerguide/aws-config-managed-rules-cloudformation-templates.html

ISSDoksim 2 years, 7 months ago

agreed - D

Certified101 2 years, 7 months ago

Selected Answer: D

D is correct - Compliance = Config

https://zhangxuetu.online

[202610]

Question #103 Topic 1

A company is running an online game on AWS. The game is played globally and is gaining popularity. Users are reporting problems with the game's responsiveness. Replay rates are dropping, and the company is losing subscribers. Game servers are located in the us-west-2 Region and use an Elastic Load Balancer to distribute client traffic.

The company has decided to deploy game servers to 11 additional AWS Regions to reduce the round-trip times of network traffic to game clients. A network engineer must design a DNS solution that uses Amazon Route 53 to ensure that user traffic is delivered to game servers with an optimal response time.

What should the network engineer do to meet these requirements?

A. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a weighted routing policy. Calculate the weight by using the number of clients in each Region.

B. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a latency routing policy. Set the Region to the Region where the Elastic Load Balancer is deployed. Most Voted

C. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a multivalue answer routing policy. Test latency from the game client, and connect to the server with the best response.

D. Create Route 53 records for the Elastic Load Balancers in each Region. Specify a geolocation routing policy. Set the location to the Region where the Elastic Load Balancer is deployed.

Correct Answer: B

Community vote distribution



Comments

lygf Highly Voted 2 years, 3 months ago

Selected Answer: B

Route 53 multivalue answer option allows for checking for health status of backend resources, it can't test latencies.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is B according to SPOTO products.

TravelKo 2 years, 2 months ago

Latency based routing is the best option.

JosMo 2 years, 2 months ago

Selected Answer: B

Latency is a better choice

scrawnyfeel 2 years, 3 months ago

Selected Answer: B

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-latency.html

ryluis 2 years, 3 months ago

Selected Answer: C

Option C provides more flexibility by considering the actual response time from the game client's perspective. It allows the client to choose the server with the best response time based on latency tests. This approach can be more effective in situations where network latency alone may not accurately reflect the actual responsiveness of the game servers.

https://zhangxuetu.online

[202610]

Question #104 Topic 1

A network engineer needs to build an encrypted connection between an on-premises data center and a VPC. The network engineer attaches the VPC to a virtual private gateway and sets up an AWS Site-to-Site VPN connection. The VPN tunnel is UP after configuration and is working. However, during rekey for phase 2 of the VPN negotiation, the customer gateway device is receiving different parameters than the parameters that the device is configured to support.

The network engineer checks the IPsec configuration of the VPN tunnel. The network engineer notices that the customer gateway device is configured with the most secure encryption algorithms that the AWS Site-to-Site VPN configuration file provides.

What should the network engineer do to troubleshoot and correct the issue?

A. Check the native virtual private gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the virtual private gateway requires.

B. Check the native customer gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires. Most Voted

C. Check Amazon CloudWatch logs of the virtual private gateway. Restrict the VPN tunnel options to the specific VPN parameters that the virtual private gateway requires.

D. Check Amazon CloudWatch logs of the customer gateway. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires.

Correct Answer: B

Community vote distribution



Comments

lygf Highly Voted 2 years, 9 months ago

Selected Answer: B

You check Cloudwatch for AWS resources or your native/on-prem logs for your on prem resource. A&D is out. The problem statement indicates that customer gateway is misconfigured. So you need to work on Customer gateway.

JaffaDaffa Highly Voted 2 years, 7 months ago

Selected Answer: B

There are no cloudwatch logs for CGW only for VPN

woorkim 1 year, 3 months ago

b is correct! Reasoning: The problem occurs during VPN tunnel negotiation The customer gateway is receiving incompatible parameters Checking the native logs of the customer gateway will help identify the specific configuration mismatches By restricting the VPN tunnel options to match the customer gateway's supported parameters, the network engineer can resolve the compatibility issue The key steps would be: Review the customer gateway's native logs Identify the specific encryption and negotiation parameters it supports Adjust the VPN configuration to align with those parameters Ensure the configuration allows a secure but compatible connection

Blitz1 1 year, 8 months ago

Selected Answer: B

funny question...and has nothing to do with technical knowledge but more with english. Where is the problem: on customer vpn router Where to check: on customer router or in Cloudwatch for you own "router".(VPG) D is confusion because is saying " Check Amazon CloudWatch logs of the customer gateway". What you will see in CloudWatch are the logs from your own router (VPG) and not customer logs because customer is not sending logs to Cloudwatch. I would have choose an answer which will say: " Check Amazon CloudWatch logs of the virtual private gateway. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires. " - but this option is NOT available.

Sailor 1 year, 10 months ago

Selected Answer: D

each side logs can determine the problem! , the question even did not ask where to take action!, the problem can be solved by matching the configuration on both sides, which side to change is not the key point ! the question says: The network engineer notices that the customer gateway device is configured with the most secure encryption algorithms that the AWS Site-to-Site VPN configuration file provides. I feel he drive us to change the AWS side as long as the the customer is configured with the " the most secure encryption algorithms" accordingly we should change the AWS side ! this is logic question more than AWS question!!!

JoellaLi 1 year, 11 months ago

Selected Answer: D

Benefits of Site-to-Site VPN logs Simplified VPN troubleshooting: Site-to-Site VPN logs help you to pinpoint configuration mismatches between AWS and your customer gateway device, and address initial VPN connectivity issues. VPN connections can intermittently flap over time due to misconfigured settings (such as poorly tuned timeouts), there can be issues in the underlying transport networks (like internet weather), or routing changes or path failures can cause disruption of connectivity over VPN. This feature allows you to accurately diagnose the cause of intermittent connection failures and fine-tune low-level tunnel configuration for reliable operation. https://docs.aws.amazon.com/vpn/latest/s2svpn/monitoring-logs.html

BGKaZ 2 years ago

Selected Answer: D

Site-to-Site VPN logs help you to pinpoint configuration mismatches between AWS and your customer gateway device, and address initial VPN connectivity issues. >>> https://docs.aws.amazon.com/vpn/latest/s2svpn/monitoring-logs.html

Marfee400704 2 years, 1 month ago

I think that it's correct answer is B according to SPOTO products.

drake2020 2 years, 2 months ago

D is the right answer: the cloudwatch log will show the real issue and then action can be taken https://docs.aws.amazon.com/vpn/latest/s2svpn/log-contents.html TunnelIKEPhase2State VpnLogDetail

luisfsm_111 2 years, 6 months ago

Selected Answer: D

According to these links, it's D: https://aws.amazon.com/about-aws/whats-new/2022/08/aws-site-vpn-connection-logs-amazon-cloudwatch/?nc1=h_ls
https://aws.amazon.com/vpn/faqs/#:~:text=Q%3A%20What%20logs,best%20effort%20basis.

Certified101 2 years, 7 months ago

Selected Answer: D

Simplified VPN troubleshooting: Site-to-Site VPN logs help you to pinpoint configuration mismatches between AWS and your customer gateway device, and address initial VPN connectivity issues.
https://docs.aws.amazon.com/vpn/latest/s2svpn/monitoring-logs.html

johnconnor 2 years, 7 months ago

It is D, basically no answer on this exam is going to be to check a solution outside AWS. Plus we have this-> https://aws.amazon.com/about-aws/whats-new/2022/08/aws-site-vpn-connection-logs-amazon-cloudwatch/

JoellaLi 2 years ago

Lol Agree with you -basically no answer on this exam is going to be to check a solution outside AWS

Fukat 2 years, 8 months ago

Selected Answer: B

B We cannot enable Cloudwatch logs on CGW or VGW. It has to be enabled on the VPN Connection. So other options are totally incorrect.

DanyelBlood 2 years, 8 months ago

Selected Answer: D

Site-to-Site VPN logs can be published to Amazon CloudWatch Logs. This feature provides customers with a single consistent way to access and analyze detailed logs for all of their Site-to-Site VPN connections.

TravelKo 2 years, 8 months ago

Selected Answer: D

Logs are exported to cloudwatch .

Training 2 years, 9 months ago

Should be D Benefits of Site-to-Site VPN logs Simplified VPN troubleshooting: Site-to-Site VPN logs help you to pinpoint configuration mismatches between AWS and your customer gateway device, and address initial VPN connectivity issues. VPN connections can intermittently flap over time due to misconfigured settings (such as poorly tuned timeouts), there can be issues in the underlying transport networks (like internet weather), or routing changes or path failures can cause disruption of connectivity over VPN. This feature allows you to accurately diagnose the cause of intermittent connection failures and fine-tune low-level tunnel configuration for reliable operation.

Training 2 years, 9 months ago

https://aws.amazon.com/about-aws/whats-new/2022/08/aws-site-vpn-connection-logs-amazon-cloudwatch/

Training 2 years, 9 months ago

https://docs.aws.amazon.com/vpn/latest/s2svpn/monitoring-logs.html

JoellaLi 2 years ago

Your link mentions that "Site-to-Site VPN logs can be published to Amazon CloudWatch Logs.". So Site-to-Site VPN logs !== Amazon CloudWatch Logs.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #105 Topic 1

A company is growing rapidly. Data transfers between the company's on-premises systems and Amazon EC2 instances that run in VPCs are limited by the throughput of a single AWS Site-to-Site VPN connection between the company's on-premises data center firewall and an AWS Transit Gateway.

A network engineer must resolve the throttling by designing a solution that is highly available and secure. The solution also must scale the VPN throughput from on premises to the VPC resources to support the increase in traffic.

Which solution will meet these requirements?

A. Configure multiple dynamic BGP-based Site-to-Site VPN connections to the transit gateway. Configure equal-cost multi-path routing (ECMP). **Most Voted**

B. Configure multiple static routing-based Site-to-Site VPN connections to the transit gateway. Configure equal-cost multi-path routing (ECMP).

C. Configure a new Site-to-Site VPN connection to the transit gateway. Enable acceleration for the Site-to-Site VPN connection.

D. Configure a software appliance-based VPN connection over the internet from the on-premises firewall to an EC2 instance that has a large instance size and networking capabilities.

Correct Answer: A

Community vote distribution

A (100%)

Comments

vikasj1in 1 year, 7 months ago

Selected Answer: A

Dynamic BGP-Based VPN Connections: BGP (Border Gateway Protocol) is a dynamic routing protocol that allows for automatic discovery and propagation of routes. Using dynamic BGP-based VPN connections simplifies the addition or removal of VPN connections without manual configuration adjustments, providing scalability. ECMP (Equal-Cost Multi-Path) Routing: ECMP enables the distribution of traffic across multiple VPN connections, allowing for load balancing and improved throughput. By configuring ECMP, traffic can be distributed evenly across the available VPN connections, overcoming the throughput limitation of a single connection. Highly Available and Secure: Using multiple VPN connections with ECMP enhances both high availability and security. If one VPN connection fails, traffic can be rerouted through the remaining connections. Additionally, BGP can help detect and respond to changes in the network topology, ensuring a reliable and resilient solution.

mavik 1 year, 10 months ago

Selected Answer: A

only A

TravelKo 2 years, 2 months ago

Selected Answer: A

A is the option.

tcp22 2 years, 3 months ago

A https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-vpn-throughput-using-aws-transit-gateway/

Training 2 years, 3 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-vpn-throughput-using-aws-transit-gateway/

Balasmaniam 2 years, 3 months ago

Selected Answer: A

https://www.examtopics.com/exams/amazon/aws-certified-advanced-networking-specialty-ans-c01/view/

https://zhangxuetu.online

[202610]

Question #106 Topic 1

A company uses Amazon Route 53 to host a public hosted zone for example.com. A network engineer recently reduced the TTL on several records to 60 seconds. The network engineer wants to assess whether the change has increased the number of queries to Route 53 beyond the expected levels that the company identified before the change. The network engineer must obtain the number of queries that have been made to the example.com public hosted zone.

Which solution will provide this information?

A. Create a new trail in AWS CloudTrail to include Route 53 data events. Send logs to Amazon CloudWatch Logs. Set up a CloudWatch metric filter to count the number of queries and create graphs.

B. Use Amazon CloudWatch to access the AWS/Route 53 namespace and to check the DNSQueries metric for the public hosted zone. Most Voted

C. Use Amazon CloudWatch to access the AWS/Route 53 Resolver namespace and to check the InboundQueryVolume metric for a specific endpoint.

D. Configure logging to Amazon CloudWatch for the public hosted zone. Set up a CloudWatch metric filter to count the number of queries and create graphs.

Correct Answer: B

Community vote distribution

B (100%)

Comments

woorkim 1 year, 3 months ago

B is correct!

Certified101 2 years, 7 months ago

Selected Answer: B

B is correct

TravelKo 2 years, 8 months ago

Selected Answer: B

B is right choice. no need to configure anything for counts.

Balasmaniam 2 years, 9 months ago

B:- CloudWatch metric for Route 53 public hosted zones The AWS/Route53 namespace includes the following metric for Route 53 hosted zones: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/monitoring-hosted-zones-

https://zhangxuetu.online

[202610]

Question #107 Topic 1

A company is establishing connectivity between its on-premises site and an existing VPC on AWS to meet a new security requirement. According to the new requirement, all public DNS queries must use an on-premises DNS security solution. The company's security team has allowed an exception for the AWS service endpoints because the company is using VPC endpoints to access AWS services.

Which combination of steps should a network engineer take to configure the architecture to meet these requirements? (Choose three.)

A. Create a system rule for the domain name “.” (dot) with a target IP address of the on-premises DNS security solution.

B. Create a new DHCP options set that provides the IP address of the on-premises DNS security solution. Update the VPC to use this new DHCP options set.

C. Create an Amazon Route 53 Resolver inbound endpoint. Associate this endpoint with the VPC.

D. Create an Amazon Route 53 Resolver outbound endpoint. Associate this endpoint with the VPC. **Most Voted**

E. Create a system rule for the domain name amazonaws.com. **Most Voted**

F. Create a forwarding rule for the domain name “.” (dot) with a target IP address of the on-premises DNS security solution. **Most Voted**

Correct Answer: DEF

Community vote distribution



Comments

Balasmaniam **Highly Voted** 2 years, 9 months ago

Selected Answer: DEF

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

bluz **Highly Voted** 2 years ago

Selected Answer: CDF

"According to the new requirement, all public DNS queries must use an on-premises DNS security solution." - amazonaws.com is a public domain. "the company is using VPC endpoints to access AWS services." - inbound endpoint. We don't need need System Rule because "The dot rule applies to all domain names except some AWS

internal domain names and record names in private hosted zones."
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-domain-name-matches

Blitz1 1 year, 8 months ago

very good. From the the same article: "If you create a conditional forwarding rule for "." (dot) or "com", we recommend that you also create a system rule for amazonaws.com. (System rules cause Resolver to locally resolve DNS queries for specific domains and subdomains.) Creating this system rule improves performance, reduces the number of queries that are forwarded to your network, and reduces Resolver charges."

Wardove 11 months ago

Selected Answer: BCF

only BCF represents a valid technical solution that would allow on-premises systems to reach VPC endpoints while ensuring public DNS queries go through the on-premises security solution.

youonebe 1 year, 1 month ago

Selected Answer: BDF

Correct combination of steps is B, D, and F. The company needs to route all public DNS queries through their on-premises DNS security solution, except for AWS service endpoints. This requires: - Setting up a new DHCP options set with the on-premises DNS server as the primary DNS resolver (option B). - Creating a Route 53 Resolver outbound endpoint to forward DNS queries from the VPC to the on-premises network (option D). - Creating a forwarding rule for the root domain "." to send all DNS queries to the on-premises DNS security solution (option F).

youonebe 1 year, 1 month ago

E is not needed as it's already there. The company's security team HAS allowed an exception for the AWS service endpoints because the company is using VPC endpoints to access AWS services.

Tofu13 2 years, 6 months ago

Selected Answer: DEF

D -Create an outbound endpoint to be able to send queries from the VPC to the on-prem DNS solution F - Forward all (=".") queries over the outbound endpoint to the on-prem solution E - Only make an exception for AWS service endpoints.

RVD 2 years, 9 months ago

Selected Answer: DEF

Ans: DEF

papercuts23 2 years, 9 months ago

i think it is D E F

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #108 Topic 1

A network engineer is designing the DNS architecture for a new AWS environment. The environment must be able to resolve DNS names of endpoints on premises, and the on-premises systems must be able to resolve the names of AWS endpoints. The DNS architecture must give individual accounts the ability to manage subdomains.

The network engineer needs to create a single set of rules that will work across multiple accounts to control this behavior. In addition, the network engineer must use AWS native services whenever possible.

Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Create an Amazon Route 53 private hosted zone for the overall cloud domain. Plan to create subdomains that align to other AWS accounts that are associated with the central Route 53 private hosted zone. **Most Voted**

B. Create AWS Directory Service for Microsoft Active Directory server endpoints in the central AWS account that hosts the private hosted zone for the overall cloud domain. Create a conditional forwarding rule in Microsoft Active Directory DNS to forward traffic to a DNS resolver endpoint on premises. Create another rule to forward traffic between subdomains to the VPC resolver.

C. Create Amazon Route 53 Resolver inbound and outbound endpoints in the central AWS account that hosts the private hosted zone for the overall cloud domain. Create a forwarding rule to forward traffic to a DNS resolver endpoint on premises. Create another rule to forward traffic between subdomains to the Resolver inbound endpoint. **Most Voted**

D. Ensure that networking exists between the other accounts and the central account so that traffic can reach the AWS Directory Service for Microsoft Active Directory DNS endpoints.

E. Ensure that networking exists between the other accounts and the central account so that traffic can reach the Amazon Route 53 Resolver endpoints.

F. Share the Amazon Route 53 Resolver rules between accounts by using AWS Resource Access Manager (AWS RAM). Ensure that networking exists between the other accounts and the central account so that traffic can reach the Route 53 Resolver endpoints. **Most Voted**

Correct Answer: ACF

Community vote distribution

ACF (100%)

Comments

Balasmaniam Highly Voted 2 years, 3 months ago

ans:acf 100%

dspd 1 year, 1 month ago

Selected Answer: ACF

closest one... but still wrong.... no network require for PHZ and resolver rule to communicate... also no need to inbound endpoint for internal subdomain.... that should be done through PHZ associations

c1193d4 1 year, 3 months ago

Selected Answer: ACF

I not satisfied with F which says "Ensure that networking exists between the other accounts and the central account so that traffic can reach the Route 53 Resolver endpoints." : AFAIK no network is necessary to access cross-account endpoints with Route53 rules !?

michele_scar 1 year, 7 months ago

Selected Answer: ACF

No mentions about AD, so is useless

Marfee400704 1 year, 7 months ago

I think that it's correct answer is ACF according to SPOTO products.

nuzz 1 year, 8 months ago

ACF https://aws.amazon.com/blogs/security/simplify-dns-management-in-a-multiaccount-environment-with-route-53-resolver/

melodbkh 2 years, 1 month ago

C can't be true. can't create rules for the Resolver Inbound endpoint at the same time, E can't be False if F is true. they state the same thing answer: AEF

TravelKo 2 years, 2 months ago

Selected Answer: ACF

ACF are the choices

https://zhangxuetu.online

[202610]

Question #109 Topic 1

A company wants to migrate its DNS registrar and DNS hosting to Amazon Route 53. The company website receives tens of thousands of visits each day, and the company's current DNS provider cannot keep up. The company wants to migrate as quickly as possible but cannot tolerate any downtime.

Which solution will meet these requirements?

A. Transfer the domain name to Route 53. Create a Route 53 private hosted zone, and copy all the existing DNS records. Update the name servers on the domain to use the name servers that are specified in the newly created private hosted zone.

B. Copy all DNS records from the existing DNS servers to a Route 53 private hosted zone. Update the name servers with the existing registrar to use the private hosted zone name servers. Transfer the domain name to Route 53. Ensure that all the changes have propagated.

C. Transfer the domain name to Route 53. Create a Route 53 public hosted zone, and copy all the existing DNS records. Set the TTL value on each record to 1 second. Update the name servers on the domain to use the name servers that are specified in the newly created public hosted zone.

D. Copy all DNS records from the existing DNS servers to a Route 53 public hosted zone. Update the name servers with the existing registrar to use the Route 53 name servers for the hosted zone. When the changes have propagated, perform a domain name transfer to Route 53. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

Balasmaniam **Highly Voted** 2 years, 3 months ago

Selected Answer: D

docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html

ashk123456 11 months, 3 weeks ago

Selected Answer: D

1⃣ Set up a Route 53 public hosted zone and manually copy all DNS records from the current DNS provider. 2⃣ Update the name servers at the existing domain registrar to point to the new Route 53 name servers. 3⃣ Wait for DNS propagation (which can take up to 48 hours). 4⃣ Once the migration is stable, transfer the domain name registration to Route 53.

Maxyz42 1 year ago

Selected Answer: D

D is correct.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is B according to SPOTO products.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #110 Topic 1

A company has an AWS account with four VPCs in the us-east-1 Region. The VPCs consist of a development VPC and three production VPCs that host various workloads.

The company has extended its on-premises data center to AWS with AWS Direct Connect by using a Direct Connect gateway. The company now wants to establish connectivity to its production VPCs and development VPC from on premises. The production VPCs are allowed to route data to each other. However, the development VPC must be isolated from the production VPCs. No data can flow between the development VPC and the production VPCs.

In preparation to implement this solution, a network engineer creates a transit gateway with a single transit gateway route table. Default route table association and default route table propagation are turned off. The network engineer attaches the production VPCs, the development VPC, and the Direct Connect gateway to the transit gateway. For each VPC route table, the network engineer adds a route to 0.0.0.0/0 with the transit gateway as the next destination.

Which combination of steps should the network engineer take next to complete this solution? (Choose three.)

A. Associate the production VPC attachments with the existing transit gateway route table. Propagate the routes from these attachments. **Most Voted**

B. Associate all the attachments with the existing transit gateway route table. Propagate the routes from these attachments.

C. Associate the Direct Connect gateway attachment with the existing transit gateway route table. Propagate the Direct Connect gateway attachment to this route table. **Most Voted**

D. Change the security group inbound rules on the existing transit gateway network interfaces in the development VPC to allow connections to and from the on-premises CIDR range only.

E. Create a new transit gateway route table. Associate the new route table with the development VPC attachment. Propagate the Direct Connect gateway and development VPC attachment to the new route table. **Most Voted**

F. Create a new transit gateway with default route table association and default route table propagation turned on. Attach the Direct Connect gateway and development VPC to the new transit gateway.

Correct Answer: ACE

Community vote distribution



Comments

HTFhere Highly Voted 2 years, 3 months ago

Selected Answer: ACE

ACE are correct - Options B, D, and F don't adhere to the provided requirements. Option B would not provide the required isolation for the development VPC. Option D won't be effective as the restriction should be on the routing level, not on the security group level. Option F would create unnecessary complexity and potential overlap in connectivity.

alejo232425 1 year, 10 months ago

there is no route to development from the DX connection, hence there is no way that on prem can reach the development network.

secdaddy 1 year, 1 month ago

Has to be ACF as explained by radiyij492 as ACE does not establish DXGW-DEV routing

radiyij492 Highly Voted 1 year, 10 months ago

Selected Answer: ACF

With ACE - there is no route DX->DEV VPC for return traffic. As TGW ENIs are requestor-managed ones - Security group cannot be attached/edited. This leads us to the option "F" - create one more TGW for DX<->DEV VPC connectivity. Sounds stupid to spin up second TGW instead of one more route table, but that is limitation of the question.

secdaddy 1 year, 1 month ago

ACF is perhaps awkward but it meets the requirements of the question whereas ACE does not. Kudos radiyij492

a0e6696 7 months ago

Selected Answer: ACF

when the traffic from the on-prem to dev vpc, it lands on the old existing route table but that doesn't aware how to reach dev vpcs... Just selecting ACF as those are relavant.. otherwise still missing communication for the dev vpc from the on-prem

BasselBuzz 1 year, 7 months ago

F is also incorrect, there is no reason to create a new transit gateway at all.

Isaias 1 year, 8 months ago

ACE, but the you need to propagate the Devop Routes on the existing RT, so DX and Devops can reach each other, between Prod and Devop cannot reach each other because there is not propagation for the Prod Routes en de new RT

alejo232425 1 year, 10 months ago

Selected Answer: BDE

how if ACE is correct the the DX know how to reach the Development VPC? there is no route table attached that show it.

zendevloper 1 year, 10 months ago

D is not possible. Transit gateway network interfaces do NOT have a security group!

danDAZET 1 year, 3 months ago

Potentially, D is possible since AWS supports Security Group reference for the inbound direction to Transit Gateway. https://docs.aws.amazon.com/vpc/latest/tgw/tgw-sg-updates-update.html. ACD or ACE are both valid

https://zhangxuetu.online

[202610]

Question #111 Topic 1

A network engineer needs to provide dual-stack connectivity between a company's office location and an AWS account. The company's on-premises router supports dual-stack connectivity, and the VPC has been configured with dual-stack support. The company has set up two AWS Direct Connect connections to the office location. This connectivity must be highly available and must be reliable for latency-sensitive traffic.

Which solutions will meet these requirements? (Choose two.)

A. Configure a single private VIF on each Direct Connect connection. Add both IPv4 and IPv6 peering to each private VIF. Configure the on- premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6 peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions. **Most Voted**

B. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with the IPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6 peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions. **Most Voted**

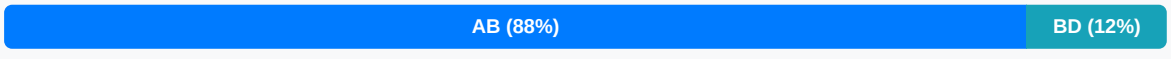
C. Configure a single private VIF and IPv4 peering on each Direct Connect connection. Configure the on-premises equipment with this peering to advertise the IPv6 routes in the same BGP neighbor configuration. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

D. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with the IPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise all IPv4 routes and IPv6 routes on all peering sessions. Keep the Bidirectional Forwarding Detection (BFD) configuration unchanged.

E. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with the IPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6 peering. Reduce the BGP hello timer to 5 seconds on both the on-premises equipment and the Direct Connect configuration.

Correct Answer: AB

Community vote distribution



Comments

norimune Highly Voted 2 years, 9 months ago

Selected Answer: AB

A&B Both ipv4 and ipv6 BGP sessions can be established with one private VIF After creating an ipv4 BGP peering on the VIF at the beginning, you can add an ipv6 peering with "add peering" And you have to enable BFD

TravelKo Highly Voted 2 years, 8 months ago

Selected Answer: AB

IP4 and IP6 BGP peerings can be created using one VIF, however advertise IP4 addresses on IP4 peering and IP6 on IP6 peering .

steli0 6 months ago

Selected Answer: AB

https://docs.aws.amazon.com/directconnect/latest/UserGuide/add-peer-to-vif.html Multiprotocol BGP is not supported. Nevertheless A should be better phrased since it mentions to add a bgp peering to each VIF (when there's only one VIF).

AWSLoverLoverLoverLoverLover 11 months, 4 weeks ago

Selected Answer: AB

A & B D is incorrect because advertising all IPv4 and IPv6 routes on all peering sessions could lead to suboptimal routing.

Jonalb 1 year, 3 months ago

Selected Answer: AB

its AB

46f094c 1 year, 4 months ago

Selected Answer: AB

already commented

46f094c 1 year, 4 months ago

1.- "must be highly available and must be reliable for latency-sensitive traffic" 2.- BFD is not enabled by default. Only A, B and C mention to enable BFD. Then C is not an option to publish IPv6 over IPv4 peers, not good practice So A and B

cerifyme85 1 year, 11 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/dual-stack-ipv6-architectures-for-aws-and-hybrid-networks/#:~:text=AWS%20Direct%20Connect,prefixes%20or%20larger. Looks like A and B

vikasj1in 2 years, 1 month ago

Selected Answer: BD

B) This option provides separate VIFs for IPv4 and IPv6, allowing for distinct routing and peering sessions. BFD helps detect connectivity issues more quickly, improving reliability. D) Similar to Option B, this option provides separate VIFs for IPv4 and IPv6. It advertises all routes on all peering sessions, ensuring redundancy. Bidirectional Forwarding Detection (BFD) is optional in this case. Option A: Mixing IPv4 and IPv6 on the same peering session may not provide the desired separation of traffic. Option C: Advertising IPv6 routes on an IPv4 peering session is not a recommended practice. Option E: Reducing the BGP hello timer to 5 seconds may increase the BGP control plane traffic and could lead to unnecessary overhead. The BFD solution in Options B and D is more specific to failure detection.

johnconnor 2 years, 7 months ago

I also think is BD, they are asking for solutions that could work, B & D would meet the requirements. They are not asking for steps for one solution, A is not HA

johnconnor 2 years, 7 months ago

Changing it to AB, you can achieve HA with two single connections too.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/high_resiliency.html

norimune 2 years, 9 months ago

Bは確実。 Dも正解だと思うが、BFDを有効化しないのは引っかかる。

demoras 2 years, 9 months ago

Should it be B & D?

https://zhangxuetu.online

[202610]

Question #112 Topic 1

A company recently started using AWS Client VPN to give its remote users the ability to access resources in multiple peered VPCs and resources in the company's on-premises data center. The Client VPN endpoint route table has a single entry of 0.0.0.0/0. The Client VPN endpoint is using a new security group that has no inbound rules and a single outbound rule that allows all traffic to 0.0.0.0/0.

Multiple remote users report that web search results are showing incorrect geographic location information for the users.

Which combination of steps should a network engineer take to resolve this issue with the LEAST amount of service interruption? (Choose three.)

A. Switch users to AWS Site-to-Site VPNs.

B. Enable the split-tunnel option on the Client VPN endpoint. Most Voted

C. Add routes for the peered VPCs and for the on-premises data center to the Client VPN route table. Most Voted

D. Remove the 0.0.0.0/0 outbound rule from the security group that the Client VPN endpoint uses.

E. Delete and recreate the Client VPN endpoint in a different VPC.

F. Remove the 0.0.0.0/0 entry from the Client VPN endpoint route table. Most Voted

Correct Answer: BCF

Community vote distribution



Comments

Balasmaniam Highly Voted 2 years, 3 months ago

Selected Answer: BCF

https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/split-tunnel-vpn.html

Maxyz42 1 year ago

Selected Answer: BCF

Split tunnel divides the Internet traffic and corpora VPN network traffic so you can route only specific traffic over the client VPN.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is BCF according to SPOTO products.

Neo00 2 years, 2 months ago

BCF Split tunnel allows only 'Internal' destination traffic will be sent to VPN tunnel and remove '0.0.0.0' default routing from route table allows internet traffic go through user's local internet provider

https://zhangxuetu.online

[202610]

Question #113 Topic 1

A company has set up hybrid connectivity between its VPCs and its on-premises data center. The company has the on-premises.example.com subdomain configured at its DNS server in the on-premises data center. The company is using the aws.example.com subdomain for workloads that run on AWS across different VPCs and accounts. Resources in both environments can access each other by using IP addresses. The company wants workloads in the VPCs to be able to access resources on premises by using the on-premises.example.com DNS names.

Which solution will meet these requirements with MINIMUM management of resources?

A. Create an Amazon Route 53 Resolver outbound endpoint. Configure a Resolver rule that conditionally forwards DNS queries for on-premises.example.com to the on-premises DNS server. Associate the rule with the VPCs. **Most Voted**

B. Create an Amazon Route 53 Resolver inbound endpoint and a Resolver outbound endpoint. Configure a Resolver rule that conditionally forwards DNS queries for on-premises.example.com to the on-premises DNS server. Associate the rule with the VPCs.

C. Launch an Amazon EC2 instance. Install and configure BIND software to conditionally forward DNS queries for on-premises.example.com to the on-premises DNS server. Configure the EC2 instance's IP address as a custom DNS server in each VPC.

D. Launch an Amazon EC2 instance in each VPC. Install and configure BIND software to conditionally forward DNS queries for on-premises.example.com to the on-premises DNS server. Configure the EC2 instance's IP address as a custom DNS server in each VPC.

Correct Answer: A

Community vote distribution

A (100%)

Comments

lygf Highly Voted 2 years, 9 months ago

Selected Answer: A

If you missed this question, you seriously need to go back and study you ass off. There's no chance you can pass the exam if you can't answer this easy-level question.

albertkr 2 years, 9 months ago

yep agree hahaha. i think this question is the easiest one amongst hundreds of questions here.

norimune Highly Voted 2 years, 9 months ago

Selected Answer: A

we need an outbound endpoint because we want to resolve it with an on-premises DNS query

ankit_agarwal 2 months, 3 weeks ago

Selected Answer: A

Yes A is correct because Outbound Route 53 Resolver endpoint and associated resolver rules will allow conditional forwarding the traffic from AWS to On-Prem dns resolver.

ankit_agarwal 2 months, 3 weeks ago

Question could have provided details about DNS resolver for aws.on-premise.com domain so that it is clear how AWS resources are being resolved. Question also states that both env are accessing each other via IP Address. In that case, Inbound resolver endpoint is required with forwarding rules setup from on-prem dns resolver server as well.

ankit_agarwal 2 months, 3 weeks ago

scratch that, question says vpc resources should resolve not on-prem

woorkim 1 year, 3 months ago

definitely A is correct!

seochan 1 year, 10 months ago

Selected Answer: A

It sceams....

Arad 2 years, 4 months ago

Selected Answer: A

A is correct, no brainer.

https://zhangxuetu.online

[202610]

Question #114 Topic 1

A company is in the early stage of AWS Cloud adoption. The company has an application that is running in an on-premises data center in Asia. The company needs to deploy new applications in the us-east-1 Region. The applications in the cloud need connectivity to the on-premises data center.

The company needs to set up a communication channel between AWS and the data center. The solution must improve latency, minimize the possibility of performance impact from transcontinental routing over the public internet, and encrypt data in transit.

Which solution will meet these requirements in the LEAST amount of time?

A. Create an AWS Site-to-Site VPN connection with acceleration turned on. Create a virtual private gateway. Attach the Site-to-Site VPN connection to the virtual private gateway. Attach the virtual private gateway to the VPC where the applications will be deployed.

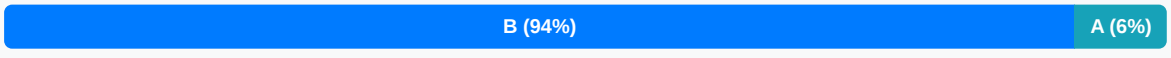
B. Create an AWS Site-to-Site VPN connection with acceleration turned on. Create a transit gateway. Attach the Site-to-Site VPN connection to the transit gateway. Create a transit gateway attachment to the VPC where the applications will be deployed. **Most Voted**

C. Create an AWS Direct Connect connection. Create a virtual private gateway. Create a public VIF and a private VIF that use the virtual private gateway. Create an AWS Site-to-Site VPN connection over the public VIF.

D. Create an AWS Site-to-Site VPN connection with acceleration turned off. Create a transit gateway. Attach the Site-to-Site VPN connection to the transit gateway. Create a transit gateway attachment to the VPC where the applications will be deployed.

Correct Answer: B

Community vote distribution



Comments

lygf Highly Voted 1 year, 9 months ago

Selected Answer: B

Site to Site VPN with acceleration re-routes your data to AWS Global Acceleration endpoints first, then packets travel on AWS wires to its AWS destination, thus it's faster than traditional VPN connection via direct-connect. In order to do that, a transit gateway is a must.

albertkr Highly Voted 1 year, 9 months ago

Acceleration is only supported for Site-to-Site VPN connections that are attached to a transit gateway. Virtual private gateways do not support accelerated VPN connections. https://docs.aws.amazon.com/vpn/latest/s2svpn/accelerated-vpn.html

94b9222 7 months ago

Selected Answer: A

Prefiro a A. Porque é mais simples.

habros 1 year, 5 months ago

Selected Answer: B

B. Transit gateway is needed for S2SVPN acceletation

norimune 1 year, 9 months ago

Selected Answer: B

Answer: B You can choose to speed up your connection with the Site-to-Site VPN option. However, it must be a Transit VIF to take advantage of this

Balasmaniam 1 year, 9 months ago

Selected Answer: B

Correct Answer : B

https://zhangxuetu.online

[202610]

Question #115 Topic 1

A company is moving its record-keeping application to the AWS Cloud. All traffic between the company's on-premises data center and AWS must be encrypted at all times and at every transit device during the migration.

The application will reside across multiple Availability Zones in a single AWS Region. The application will use existing 10 Gbps AWS Direct Connect dedicated connections with a MACsec capable port. A network engineer must ensure that the Direct Connect connection is secured accordingly at every transit device.

The network engineer creates a Connection Key Name and Connectivity Association Key (CKN/CAK) pair for the MACsec secret key.

Which combination of additional steps should the network engineer take to meet the requirements? (Choose two.)

A. Configure the on-premises router with the MACsec secret key. **Most Voted**

B. Update the connection's MACsec encryption mode to must_encrypt. Then associate the CKN/CAK pair with the connection.

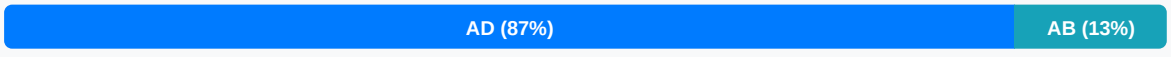
C. Update the connection's MACsec encryption mode to should encrypt. Then associate the CKN/CAK pair with the connection.

D. Associate the CKN/CAK pair with the connection. Then update the connection's MACsec encryption mode to must_encrypt. **Most Voted**

E. Associate the CKN/CAK pair with the connection. Then update the connection's MACsec encryption mode to should_encrypt.

Correct Answer: AD

Community vote distribution



Comments

lygf **Highly Voted** 2 years, 9 months ago

Selected Answer: AD

According to AWS, you need to do the following 4 steps in order. 1. Create a new connection with MACsec support 2. Associate the CKN/CAK with the connection 3. Verify the connection status 4. Migrate traffic to new connection as appropriate When you first create the DX connection, the default encryption mode is should encrypt. You need to update it to must encrypt in step 3. There's no way to specify that during the creation of DX.

https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

woorkim 1 year, 3 months ago

Selected Answer: AD

https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

JoellaLi 2 years ago

You cannot modify a MACsec secret key after you associate it with a connection. If you need to modify the key, disassociate the key from the connection, and then associate a new key with the connection.
https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

arturogomezb 1 year, 9 months ago

But you can change the encryption mode
https://docs.aws.amazon.com/directconnect/latest/UserGuide/updateconnection.html

MohamedSherif1 2 years, 7 months ago

Selected Answer: AD

The default value for the encryption mode is “should_encrypt”, and this can be changed using the new DirectConnect API UpdateConnection.

norimune 2 years, 9 months ago

Selected Answer: AB

Update the MACsec encryption mode before binding.

Spaurito 1 year, 4 months ago

Agree, the key was created. You then have to update the mode and associate the key.

Balasmaniam 2 years, 9 months ago

Selected Answer: AD

docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-mac-sec-getting-started.html

https://zhangxuetu.online

[202610]

Question #116 Topic 1

A network engineer is designing hybrid connectivity with AWS Direct Connect and AWS Transit Gateway. A transit gateway is attached to a Direct Connect gateway and 19 VPCs across different AWS accounts. Two new VPCs are being attached to the transit gateway. The IP address administrator has assigned 10.0.32.0/21 to the first VPC and 10.0.40.0/21 to the second VPC. The prefix list has one CIDR block remaining before the prefix list reaches the quota for the maximum number of entries.

What should the network engineer do to advertise the routes from AWS to on premises to meet these requirements?

A. Add 10.0.32.0/21 and 10.0.40.0/21 to both AWS managed prefix lists.

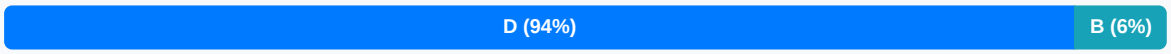
B. Add 10.0.32.0/21 and 10.0.40.0/21 to the allowed prefix list.

C. Add 10.0.32.0/20 to both AWS managed prefix lists.

D. Add 10.0.32.0/20 to the allowed prefix list. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

norimune **Highly Voted** 2 years, 3 months ago

Selected Answer: D

Correct Answer: D The VPC route to send to on-premises is sent by entering the allowed prefix value of DXGW. Since only one remaining frame is used for route information, it is necessary to aggregate two routes

Certified101 **Highly Voted** 2 years, 1 month ago

Selected Answer: D

If only one CIDR block can be added to the prefix list (due to reaching the maximum quota), then it will be impossible to add both 10.0.32.0/21 and 10.0.40.0/21 separately. However, by aggregating the two CIDR blocks into a single CIDR block (10.0.32.0/20), the network engineer can still add the routes for both VPCs to the allowed prefix list. This is because 10.0.32.0/20 covers IP addresses from 10.0.32.0 to 10.0.47.255, which includes the addresses from both 10.0.32.0/21 (10.0.32.0 to 10.0.39.255) and 10.0.40.0/21 (10.0.40.0 to 10.0.47.255).

WherecanIstart 1 year, 6 months ago

Selected Answer: D

D is correct as you have to summarize both subnets into one. x.x.32.0/21 x.x.40.0/21 Both routes/subnets have 4 bits in common in the third octet. 0 0 1 0 0 0 0 0 = 32 0 0 1 0 1 0 0 0 = 40 When summarized you will have 20 network bits

which gives you a /20.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is D.

Balasmaniam 2 years, 3 months ago

Selected Answer: B

I think its should be answer : B

Balasmaniam 2 years, 3 months ago

back with answer : D..

https://zhangxuetu.online

[202610]

Question #117 Topic 1

Two companies are merging. The companies have a large AWS presence with multiple VPCs and are designing connectivity between their AWS networks. Both companies are using AWS Direct Connect with a Direct Connect gateway. Each company also has a transit gateway and multiple AWS Site-to-Site VPN connections from its transit gateway to on-premises resources. The new solution must optimize network visibility, throughput, logging, and monitoring.

Which solution will meet these requirements?

A. Configure a Site-to-Site VPN connection between each company's transit gateway to establish reachability between the respective networks. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use VPC Reachability Analyzer to monitor connectivity.

B. Configure a Site-to-Site VPN connection between each company's transit gateway to establish reachability between the respective networks. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use AWS Transit Gateway Network Manager to monitor the transit gateways and their respective connections.

C. Configure transit gateway peering between each company's transit gateway. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use VPC Reachability Analyzer to monitor connectivity.

D. Configure transit gateway peering between each company's transit gateway. Configure VPC Flow Logs for all VPCs. Publish the flow logs to Amazon CloudWatch. Use AWS Transit Gateway Network Manager to monitor the transit gateways, their respective connections, and the transit gateway peering link. Most Voted

Correct Answer: D

Community vote distribution



Comments

albertkr Highly Voted 2 years, 9 months ago

Selected Answer: D

transit gateway peering will allow the communication between all networks. To monitor the overall infrastructure, AWS Transit Gateway Network Manager is utilized for this purpose. https://aws.amazon.com/transit-gateway/network-manager/

woorkim 1 year, 3 months ago

Selected Answer: D

Option D offers the most comprehensive solution by utilizing transit gateway peering for efficient inter-company connectivity, VPC Flow Logs for traffic visibility, and AWS Transit Gateway Network Manager for advanced monitoring and optimization of network resources.

Arad 2 years, 4 months ago

Selected Answer: D

Correct answer is D.

Balasmaniam 2 years, 9 months ago

https://aws.amazon.com/blogs/aws/new-vpc-insights-analyzes-reachability-and-visibility-in-vpcs/ Ans: A

albertkr 2 years, 9 months ago

VPC Reachability Analyzer is a network diagnostics tool that troubleshoots reachability between two endpoints in a VPC, or within multiple VPCs. this is not in the requirement. Moreover, site-to-site vpn only allows 1.25Gbps which seems not allowing throughput optimization between companies as in the requirement.

Balasmaniam 2 years, 9 months ago

Selected Answer: D

link speed wise, Peering will provide more speed than vpn connection.

https://zhangxuetu.online

[202610]

Question #118 Topic 1

A company has a single VPC in the us-east-1 Region. The company is planning to set up a new VPC in the us-east-2 Region. The existing VPC has an AWS Site-to-Site VPN connection to the company's on-premises environment and uses a virtual private gateway.

A network engineer needs to implement a solution to establish connectivity between the existing VPC and the new VPC. The solution also must implement support for IPv6 for the new VPC. The company has new on-premises resources that need to connect to VPC resources by using IPv6 addresses.

Which solution will meet these requirements?

A. Create a new virtual private gateway in us-east-1. Attach the new virtual private gateway to the new VPC. Create two new Site-to-Site VPN connections to the new virtual private gateway with IPv4 and IPv6 support. Configure routing between the VPCs by using VPC peering.

B. Create a transit gateway in us-east-1 and in us-east-2. Attach the existing VPC and the new VPC to each transit gateway. Create a new Site-to-Site VPN connection to each transit gateway with IPv4 and IPv6 support. Configure transit gateway peering. Configure routing between the VPCs and the on-premises environment. **Most Voted**

C. Create a new virtual private gateway in us-east-2. Attach the new virtual private gateway to the new VPCreate two new Site-to-Site VPN connections to the new virtual private gateway with IPv4 and IPv6 support. Configure routing between the VPCs by using VPC peering.

D. Create a transit gateway in us-east-1. Attach the existing VPC and the new VPC to the transit gateway. Create two new Site-to-Site VPN connections to the transit gateway with IPv4 and IPv6 support. Configure transit gateway peering. Configure routing between the VPCs and the on-premises environment.

Correct Answer: B

Community vote distribution



Comments

papercuts23 **Highly Voted** 2 years, 3 months ago

Selected Answer: B

Transit gateway attachment can only be in the same region as the TGW itself

JoellaLi 1 year, 6 months ago

What's wrong with C?

JoellaLi 1 year, 5 months ago

Support for IPv6 traffic for VPN connections on a transit gateway. IPv6 traffic is not supported for VPN connections on a virtual private gateway. Site-to-Site VPN connections on a virtual private gateway do not support IPv6.

sanalainen Highly Voted 1 year, 10 months ago

B is ok, but creates a lot of TGW processing cost at this point. What's wrong with C?

JoellaLi 1 year, 5 months ago

Support for IPv6 traffic for VPN connections on a transit gateway. IPv6 traffic is not supported for VPN connections on a virtual private gateway. Site-to-Site VPN connections on a virtual private gateway do not support IPv6.

Rollizo 1 year, 1 month ago

Selected Answer: B

cannot be C because of: VGWs are region-specific and cannot connect across regions. VPC peering does not support IPv6 across regions.

vic614 1 year, 3 months ago

Selected Answer: B

Virtual Private Gateway doesn't support IPv6

seochan 1 year, 4 months ago

Selected Answer: C

It's not B guys.. A Site-to-Site VPN connection cannot support both IPv4 and IPv6 traffic.
https://docs.aws.amazon.com/vpn/latest/s2svpn/ipv4-ipv6.html

seochan 1 year, 4 months ago

I changed my mind. It's B "Create a new Site-to-Site VPN connection to each transit gateway with IPv4 and IPv6 support." might not meaning that they will use dual stack-mode. And I clearly cannot create an IPv6 s2s VPN connection with VGW.

JoellaLi 1 year, 6 months ago

Selected Answer: C

VPCs across accounts and AWS Regions can also be peered together. But AWS Transit Gateway is an regional network transit hub.

JoellaLi 1 year, 6 months ago

Change to B. Inter-Region gateway peering uses the same network infrastructure as VPC peering. You can peer both intra-Region and inter-Region transit gateways, and route traffic between them, which includes IPv4 and IPv6 traffic.
https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html

JoellaLi 1 year, 6 months ago

Actually not sure about B or C ...

Jordarlu 1 year, 4 months ago

https://docs.aws.amazon.com/vpn/latest/s2svpn/ipv4-ipv6.html#:~:text=IPv6%20addresses%20are%20only%20supported,gateway%20do%20not%20support%20IPv6.
Site-to-Site VPN connections on a virtual private gateway do not support IPv6.

ogrefighter 1 year, 6 months ago

Selected Answer: C

A: not correct because the new VPC is in us-east-2 so no need for a new Virual private gateway in us-east-1 b: not correct because creates only one site-to-site VPN connection, but requirement to offer both ipv4 and ipv6 mandates two connections: https://docs.aws.amazon.com/vpn/latest/s2svpn/ipv4-ipv6.html c - correct because will work and be economical d - not correct because VPC cannot connect to Transit Gateway in another region (which is the second sentence)

mavik 1 year, 7 months ago

Selected Answer: C

Correct answer is C VPC to VPC by peering VPCs to on-prem by different S2S VPN - will have 1.25 Gb for each VPC

mavik 1 year, 7 months ago

++ this design is more cost-effective

Arad 1 year, 10 months ago

Selected Answer: B

B is the right answer.

ISSDoksim 2 years, 1 month ago

B - A Site-to-Site VPN connection cannot support both IPv4 and IPv6 traffic.

albertkr 2 years, 2 months ago

transit gateway peering will allow the communication between all networks. To monitor the overall infrastructure, AWS Transit Gateway Network Manager is utilized for this purpose. https://aws.amazon.com/transit-gateway/network-manager/

albertkr 2 years, 2 months ago

Moderator, pls erase comment, as this comment is supposed to be for no 117.

tcp22 2 years, 3 months ago

B for sure

demoras 2 years, 3 months ago

Selected Answer: B

Answer should be B

Awadhesh 2 years, 3 months ago

Answer should be B

https://zhangxuetu.online

[202610]

Question #119 Topic 1

A network engineer is working on a private DNS design to integrate AWS workloads and on-premises resources. The AWS deployment consists of five VPCs in the eu-west-1 Region that connect to the on-premises network over AWS Direct Connect. The VPCs communicate with each other by using a transit gateway. Each VPC is associated with a private hosted zone that uses the aws.example.internal domain. The network engineer creates an Amazon Route 53 Resolver outbound endpoint in a shared services VPC and attaches the shared services VPC to the transit gateway.

The network engineer is implementing a solution for DNS resolution. Queries for hostnames that end with aws.example.internal must use the private hosted zone. Queries for hostnames that end with all other domains must be forwarded to a private on-premises DNS resolver.

Which solution will meet these requirements?

A. Add a forwarding rule for “*” that targets the on-premises server's DNS IP address. Add a system rule for aws.example.internal that targets Route 53 Resolver.

B. Add a forwarding rule for aws.example.internal that targets Route 53 Resolver. Add a system rule for “.” that targets the Route 53 Resolver outbound endpoint.

C. Add a forwarding rule for “*” that targets the Route 53 Resolver outbound endpoint.

D. Add a forwarding rule for “.” that targets the Route 53 Resolver outbound endpoint. Most Voted

Correct Answer: D

Community vote distribution



Comments

JosMo Highly Voted 2 years, 8 months ago

Selected Answer: D

Answer is : D don't need a rules for aws.external. Quote: "If the domain name in a query doesn't match the domain name in any other rules, Resolver forwards the query based on the settings in the autodefined "." (dot) rule. The dot rule applies to all domain names except some AWS internal domain names and record names in private hosted zones" ref : https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-domain-name-matches

Neo00 2 years, 8 months ago

Agree, should be D "The dot rule applies to all domain names except some AWS internal domain names and record names in private hosted zones."

DeathFrmAbv 2 years, 8 months ago

Agree, from the doc mentioned "If you want to forward all queries to the DNS resolvers on your network, you can create a custom forwarding rule, specify "." for the domain name, specify Forwarding for Type, and specify the IP addresses of those resolvers."

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: D

In this case, a dot (".") is used as a wildcard to match all other domains. So, by adding a forwarding rule for "." that targets the Route 53 Resolver outbound endpoint, all DNS queries for hostnames that end with any domain other than aws.example.internal will be forwarded to the on-premises DNS resolver through the outbound endpoint. Meanwhile, AWS automatically resolves DNS namespaces for VPCs that are associated with private hosted zones, so queries for hostnames that end with aws.example.internal will be resolved using the private hosted zone without requiring any additional configuration.

Spaurito 1 year, 4 months ago

D - The auto defined rules will resolve for internal DNS queries and everything else to the outbound endpoint. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

Ravan 1 year, 6 months ago

Selected Answer: A

D. Add a forwarding rule for . that targets the Route 53 Resolver outbound endpoint. This rule would forward all DNS queries to the Route 53 Resolver, which is incorrect as it would not differentiate between queries for aws.example.internal and other domains.

Newbies 1 year, 12 months ago

A - Add a fwd rule for "*" that targets the on-premises server's DNS IP address, add aws.example.internal that targets Route 53 Resolver.

RVD 2 years, 9 months ago

Selected Answer: B

RuleType When you want to forward DNS queries for specified domain name to resolvers on your network, specify FORWARD. When you have a forwarding rule to forward DNS queries for a domain to your network and you want Resolver to process queries for a subdomain of that domain, specify SYSTEM. For example, to forward DNS queries for example.com to resolvers on your network, you create a rule and specify FORWARD for RuleType. To then have Resolver process queries for apex.example.com, you create a rule and specify SYSTEM for RuleType. Currently, only Resolver can create rules that have a value of RECURSIVE for RuleType.

dyaz208 2 years, 9 months ago

Selected Answer: D

I agree with D.

AJ7428 2 years, 9 months ago

Selected Answer: D

I agree answer should be D. PHZ resolve by system define rule. https://d1.awsstatic.com/events/reinvent/2019/Deep_dive_on_DNS_in_the_hybrid_cloud_NET410.pdf

devilman222 2 years, 9 months ago

I would think you use forwarding rule . for on prem. So D. I just hope I don't get this question since no one know the answer.

lygf 2 years, 9 months ago

Selected Answer: B

You use "." to forward all queries to the destination -> A&C out. Despite of that, "Resolver automatically creates autodefined system rules that define how queries for selected domains are resolved by default: For private hosted zones and for Amazon EC2–specific domain names (such as compute.amazonaws.com and compute.internal), autodefined rules ensure that your private hosted zones and EC2 instances continue to resolve if you create conditional forwarding rules for less specific domain names such as "." (dot) or "com"."
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-domain-name-matches
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

lygf 2 years, 9 months ago

Sorry, I meant D. You don't need to create a separate rule for aws.example.internal. It will continue to resolve in the PHZ

papercuts23 2 years, 9 months ago

Selected Answer: D

I think it is D. aws.example.internal will already be using private hosted zone, and does not need any rule.

papercuts23 2 years, 9 months ago

changed my mind. Route 53 use * as wildcard, not '.'. Should be C

lygf 2 years, 9 months ago

No it's "." If you want to forward all queries to your network, you create a rule, specify "." (dot) for the domain name, and associate the rule with the VPCs for which you want to forward all DNS queries to your network.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-domain-name-matches

ryluis 2 years, 9 months ago

In AWS Route 53, to reach public domains and on-premises networks, you would typically use a forwarding rule. A forwarding rule allows you to forward DNS queries for a specific domain or subdomain to another DNS resolver. This is useful when you want to forward DNS queries from your Route 53 Resolver to an on-premises DNS server or to another DNS service provider for resolution. On the other hand, a system rule is used to specify how the Route 53 Resolver handles DNS queries that don't match any forwarding rules or DNS rules that you've configured. It is typically used for fallback or default behavior. So, to reach public domains and on-premises networks, you would configure a forwarding rule in Route 53 to forward the DNS queries to the appropriate DNS resolver for resolution.
answer is A

demoras 2 years, 9 months ago

Selected Answer: B

Should be B

AJ7428 2 years, 9 months ago

Should be B.

https://zhangxuetu.online

[202610]

Question #120 Topic 1

A global film production company uses the AWS Cloud to encode and store its video content before distribution. The company's three global offices are connected to the us-east-1 Region through AWS Site-to-Site VPN links that terminate on a transit gateway with BGP routing activated.

The company recently started to produce content at a higher resolution to support 8K streaming. The size of the content files has increased to three times the size of the content files from the previous format. Uploads of files to Amazon EC2 instances are taking 10 times longer than they did with the previous format.

Which actions should a network engineer recommend to reduce the upload times? (Choose two.)

A. Create a second VPN tunnel from each office location to the transit gateway. Activate equal-cost multi-path (ECMP) routing. Most Voted

B. Modify the transit gateway to activate Jumbo MTU on the VPN tunnels to each office location.

C. Replace the existing VPN tunnels with new tunnels that have acceleration activated. Most Voted

D. Upgrade each EC2 instance to a modern instance type. Activate Jumbo MTU in the operating system.

E. Replace the existing VPN tunnels with new tunnels that have IGMP activated.

Correct Answer: AC

Community vote distribution



Comments

JosMo Highly Voted 2 years, 2 months ago

Selected Answer: AC

Like balasmaniam said, internet have an MTU of 1500, so B and D are wrong, IGMP won't help, so AC is the answer

papercuts23 Highly Voted 2 years, 3 months ago

Selected Answer: AC

I vote for AC too

acloudguru 1 year, 5 months ago

Selected Answer: AC

transit gateway, do not support jumbo MTU sizes. The maximum supported MTU size is 1500 bytes. so B is out. D is also useless, no impact for the network side.

vikasj1in 1 year, 7 months ago

Selected Answer: BD

B) Activating Jumbo MTU (Maximum Transmission Unit) can increase the efficiency of data transfer by allowing larger packets to be transmitted, reducing the overhead associated with smaller packets. D) Upgrading to a modern EC2 instance type ensures that the instance has better performance capabilities. Additionally, activating Jumbo MTU at the operating system level can further optimize the data transfer. These actions address both the network infrastructure (MTU settings on the transit gateway) and the EC2 instances to improve overall upload performance for the larger content files.

Jordarlu 1 year, 4 months ago

The MTU of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data that can be passed in a single packet. A transit gateway supports an MTU of 8500 bytes for traffic between VPCs, AWS Direct Connect, Transit Gateway Connect, and peering attachments. Traffic over VPN connections can have an MTU of 1500 bytes. https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-quotas.html#:~:text=A%20transit%20gateway%20supports%20an,an%20MTU%20of%201500%20bytes.

GaryQian 1 year, 7 months ago

Selected Answer: AC

Jumbo MTU is very limited on internet

Arad 1 year, 10 months ago

Selected Answer: AC

AC is the correct answer.

MohamedSherif1 2 years, 1 month ago

Selected Answer: AC

Jumbo frames are not supported for Site-to-Site VPN

Balasmaniam 2 years, 3 months ago

A transit gateway supports an MTU of 8500 bytes for traffic between VPCs, AWS Direct Connect, Transit Gateway Connect, and peering attachments. Traffic over VPN connections can have an MTU of 1500 bytes.

ryluis 2 years, 3 months ago

Selected Answer: BD

Equal-Cost Multipath (ECMP) routing does not directly reduce upload time. ECMP is a routing technique that allows for the distribution of network traffic across multiple paths or links of equal cost. It is primarily used to increase network capacity and provide redundancy by utilizing multiple parallel paths. the use of jumbo frames can lead to more efficient data transfer and reduced transmission overhead. This can result in improved throughput and potentially reduced upload time for large file transfers or data-intensive applications.

Neo00 2 years, 2 months ago

you can use Equal Cost Multi-Path (ECMP) routing to get a higher VPN bandwidth by aggregating multiple VPN tunnels. https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html

demoras 2 years, 3 months ago

Selected Answer: AC

should be AC

Awadhesh 2 years, 3 months ago

yes, should be AC

AJ7428 2 years, 3 months ago

Should be AC

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #121 Topic 1

An application team for a startup company is deploying a new multi-tier application into the AWS Cloud. The application will be hosted on a fleet of Amazon EC2 instances that run in an Auto Scaling group behind a publicly accessible Network Load Balancer (NLB). The application requires the clients to work with UDP traffic and TCP traffic.

In the near term, the application will serve only users within the same geographic location. The application team plans to extend the application to a global audience and will move the deployment to multiple AWS Regions around the world to bring the application closer to the end users. The application team wants to use the new Regions to deploy new versions of the application and wants to be able to control the amount of traffic that each Region receives during these rollouts. In addition, the application team must minimize first-byte latency and jitter (randomized delay) for the end users.

How should the application team design the network architecture for the application to meet these requirements?

A. Create an Amazon CloudFront distribution to align to each Regional deployment. Set the NLB for each Region as the origin for each CloudFront distribution. Use an Amazon Route 53 weighted routing policy to control traffic to the newer Regional deployments.

B. Create an AWS Global Accelerator accelerator and listeners for the required ports. Configure endpoint groups for each Region. Configure a traffic dial for the endpoint groups to control traffic to the newer Regional deployments. Register the NLBs with the endpoint groups. Most Voted

C. Use Amazon S3 Transfer Acceleration for the application in each Region. Adjust the amount of traffic that each Region receives from the Transfer Acceleration endpoints to the Regional NLBs.

D. Create an Amazon CloudFront distribution that includes an origin group. Set the NLB for each Region as the origins for the origin group. Use an Amazon Route 53 latency routing policy to control traffic to the new Regional deployments.

Correct Answer: B

Community vote distribution

B (100%)

Comments

Neo00 Highly Voted 2 years, 2 months ago

Selected Answer: B

CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP. and CloudFront doesn't support NLB

vikasj1in Highly Voted 1 year, 7 months ago

Selected Answer: B

AWS Global Accelerator: It is a service that uses static IP addresses as Anycast, which provides a fixed entry point for your applications. Global Accelerator directs traffic over the AWS global network to optimal AWS endpoint based on health, geography, and routing policies you configure. Listeners and Endpoint Groups: Global Accelerator allows you to configure listeners for the required ports and endpoint groups for each Region where your application is deployed. Traffic Dial: The traffic dial allows you to control the percentage of traffic that is directed to each endpoint group. This is particularly useful during rollouts or canary deployments, where you want to gradually shift traffic to a new version of the application. Minimizing Latency: AWS Global Accelerator is designed to provide low-latency, high-throughput, and fault-tolerant access to your applications.

Adzz 1 year, 9 months ago

Selected Answer: B

B, because UDP has come into picture, so no better option than a Global Accelerator.

Certified101 2 years, 1 month ago

Selected Answer: B

B is correct

Neo00 2 years, 2 months ago

B. CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP.

TravelKo 2 years, 2 months ago

Selected Answer: B

NLB is not in the list of Cloud Front Origins.

wartywarthog 2 years, 2 months ago

B. CloudFront doesn't support NLB as an origin:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html
Also S3 transfer acceleration is the wrong answer since nothing file related is mentioned in the question.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #122 Topic 1

A company is deploying a new stateless web application on AWS. The web application will run on Amazon EC2 instances in private subnets behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The web application has a stateful management application for administration that will run on EC2 instances that are in a separate Auto Scaling group.

The company wants to access the management application by using the same URL as the web application, with a path prefix of/management. The protocol, hostname, and port number must be the same for the web application and the management application. Access to the management application must be restricted to the company's on-premises IP address space. An SSL/TLS certificate from AWS Certificate Manager (ACM) will protect the web application.

Which combination of steps should a network engineer take to meet these requirements? (Choose two.)

A. Insert a rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the source-ip condition type for the on-premises IP address space. Forward requests to the management application target group if there is a match. Edit the management application target group and enable stickiness. **Most Voted**

B. Modify the default rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the source-ip condition type for the on-premises IP address space. Forward requests to the management application target group if there is not a match. Enable group-level stickiness in the rule attributes.

C. Insert a rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the X-Forwarded-For HTTP header for the on-premises IP address space. Forward requests to the management application target group if there is a match. Enable group-level stickiness in the rule attributes.

D. Modify the default rule for the load balancer HTTPS listener. Configure the rule to check the path-pattern condition type for the /management prefix and to check the source-ip condition type for the on-premises IP address space. Forward requests to the web application target group if there is not a match.

E. Forward all requests to the web application target group. Edit the web application target group and disable stickiness. **Most Voted**

Correct Answer: AE

Community vote distribution

AE (75%) AD (23%) AC (2%)

Comments

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: AE

DEFAULT RULES CANNOT HAVE CONDITIONS so B & D are out. Changing to A & E. A to forward people to managment with stickiness E to forward people to the web application without stickiness https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

JoseCC 2 years, 7 months ago

AE correct for me as well.

Certified101 2 years, 7 months ago

Also see - https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-update-rules.html#edit-rule Step 8 - "(Optional) Modify the conditions and actions as needed. For example, you can edit a condition or action (pencil icon), add a condition, add an authenticate action to a rule for an HTTPS listener, or delete a condition or action (trash can icon). You can't add conditions to the default rule."

papercuts23 Highly Voted 2 years, 9 months ago

Selected Answer: AD

AD is correct. Default rule does not need stickiness because it is stateless

awskiller007 2 years, 7 months ago

why does the new rule in A requires enable stickiness?

Ravan 1 year, 6 months ago

Selected Answer: AD

E: Disabling stickiness on the web application target group would not fulfill the requirement for the management application, which needs stickiness for stateful sessions.

cerifyme85 1 year, 11 months ago

Selected Answer: AE

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#listener-rules:~:text=When%20you%20create%20a%20listener%2C%20you%20define%20actions%20for%20the%20default%20rule.%20Default%20rules%20can%27t%20have%20conditions.%20If%20the%20conditions%20for%20none%20of%20a%20listener%27s%20rules%20are%20met%2C%20then%20the%20action%20for%20the%20default%20rule%20is%20performed.

patanjali 2 years ago

Selected Answer: AE

Default rule cant have condition

michele_scar 2 years ago

Selected Answer: AE

Eliminating the answers with "Update default rule" remains A, C, E. Obv C is uncorrect: A and E.

vikasj1in 2 years, 1 month ago

Selected Answer: AE

Option B is incorrect because it suggests forwarding requests to the management application target group if there is not a match, which contradicts the requirement to restrict access to the management application to the company's on-premises IP address space. Option C is incorrect because it suggests checking the X-Forwarded-For HTTP header

for the on-premises IP address space, which is unnecessary and potentially less secure than directly checking the source IP address. Option D is incorrect because it suggests forwarding requests to the web application target group if there is not a match, which would not meet the requirement to access the management application via the same URL prefix. Therefore, options A and E are the most suitable for meeting the requirements outlined in the scenario.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is AC according to SPOTO products.

michele_scar 2 years, 1 month ago

Selected Answer: AE

cannot modify default rule

cumzle_com 2 years, 3 months ago

Selected Answer: AE

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html Default rules When you create a listener, you define actions for the default rule. Default rules can't have conditions. If the conditions for none of a listener's rules are met, then the action for the default rule is performed.

aws_god 2 years, 4 months ago

Selected Answer: AD

correct answer is A and D

Cheam 2 years, 6 months ago

Selected Answer: AD

1) By default, sticky-sessions is not enabled on the ALB, and therefore answer E does not apply. Ref: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html 2) You can modify the default rule to check against the source-ip condition, CLI. Ref: https://docs.aws.amazon.com/cli/latest/reference/elbv2/modify-listener.html All the best.

Certified101 2 years, 7 months ago

Selected Answer: AC

Default rules can't have conditions.https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html So I think its AC

ISSDoksim 2 years, 7 months ago

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

ISSDoksim 2 years, 7 months ago

AC - Default rules can't have conditions.

https://zhangxuetu.online

[202610]

Question #123 Topic 1

A company deploys a software solution on Amazon EC2 instances that are in a cluster placement group. The solution's UI is a single HTML page. The HTML file size is 1,024 bytes. The software processes files that exceed 1,024 MB in size. The software shares files over the network to clients upon request. The files are shared with the Don't Fragment flag set. Elastic network interfaces of the EC2 instances are set up with jumbo frames.

The UI is always accessible from all allowed source IP addresses, regardless of whether the source IP addresses are within a VPC, on the internet, or on premises. However, clients sometimes do not receive files that they request because the files fail to travel successfully from the software to the clients.

Which options provide a possible root cause of these failures? (Choose two.)

A. The source IP addresses are from on-premises hosts that are routed over AWS Direct Connect.

B. The source IP addresses are from on-premises hosts that are routed over AWS Site-to-Site VPN. Most Voted

C. The source IP addresses are from hosts that connect over the public internet. Most Voted

D. The security group of the EC2 instances does not allow ICMP traffic.

E. The operating system of the EC2 instances does not support jumbo frames.

Correct Answer: BC

Community vote distribution



Comments

albertkr Highly Voted 2 years, 9 months ago

Selected Answer: BC

Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, traffic is limited to a maximum MTU of 1500 in the following cases: Traffic over an internet gateway Traffic over an inter-region VPC peering connection Traffic over VPN connections Traffic outside of a given AWS Region for EC2-Classic If packets are over 1500 bytes, they are fragmented, or they are dropped if the Don't Fragment flag is set in the IP header. regardless the security group allows icmp traffic to enable pmtud or not, the oversized packets will be dropped anyway due to don't fragment flag set.

JosMo Highly Voted 2 years, 8 months ago

Selected Answer: BC

Answer: BC Internet and VPN doesn't work with jumbo frame (MTU 1501+) so it will be fragmented. " The files are shared with the Don't Fragment flag set"

AikAWS 6 months, 2 weeks ago

Selected Answer: BD

Path MTU discovery (PMTUD) relies on ICMP “fragmentation needed” messages to inform the sender to reduce packet size. If the EC2 security group (or any firewall on the path) blocks ICMP, those ICMP messages never reach the sender and PMTUD cannot work. With DF set, the sender will keep sending large packets that get dropped, causing intermittent file-transfer failures.

steli0 6 months ago

That could be a valid point if the issue was persistent.

secdaddy 1 year, 1 month ago

Selected Answer: BD

The question isn't about packets dropping but about file transfer failure. Client requests file, server sends jumbo back towards client and it gets dropped but with ICMP fragmentation required but DF bit set. If ICMP isn allowed to the servers they'll adjust MTU and send non-jumbo allowing the file transfer to succeed so D is valid. The question says "source IP addresses are within a VPC, on the internet, or on premises." There is no mention of VPN in the question so I think this must be the trick.

secdaddy 1 year, 1 month ago

Selected Answer: BC

The question isn't about packets dropping but about file transfer failure. Client requests file, server sends jumbo back towards client and it gets dropped but with ICMP fragmentation required but DF bit set. If ICMP isn allowed to the servers they'll adjust MTU and send non-jumbo allowing the file transfer to succeed. The question has three perfectly valid answers (and yes I know can only choose two). Stupid question.

secdaddy 1 year, 1 month ago

moderator please cancel this ; changing to a different answer

woorkim 1 year, 3 months ago

Selected Answer: BC

traffic is limited to a maximum MTU of 1500 in the following cases: Traffic over an internet gateway Traffic over an inter-region VPC peering connection Traffic over VPN connections Traffic between AWS Regions, unless a transit gateway is used

Arad 2 years, 4 months ago

Selected Answer: BC

BC is the right answer.

habros 2 years, 5 months ago

Selected Answer: BC

BC. S2SVPN doesn’t support jumbo frames. Internet communication can also contribute to 1500 bytes MTU limit (best is use Direct Connect)

Certified101 2 years, 7 months ago

Selected Answer: BC

As albertkr said - its BC

Manh 2 years, 8 months ago

answer is BC https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, traffic is limited to a maximum MTU of 1500 in the following cases: Traffic over an internet gateway Traffic over an inter-region VPC peering connection Traffic over VPN connections Traffic outside of a given AWS Region for EC2-Classic If packets are over 1500 bytes, they are fragmented, or they are dropped if the Don't Fragment flag is set in the IP header.

tcp22 2 years, 9 months ago

I would go with B and C I don't know how not be able to ping the server would be related.

AJ7428 2 years, 9 months ago

Selected Answer: BD

Should be BD.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #124 Topic 1

A company has users who work from home. The company wants to move these users to Amazon WorkSpaces for additional security visibility.

The company has deployed WorkSpaces in its own AWS account in VPC A. A network engineer decides to provide the security visibility by using two firewall appliances behind a Gateway Load Balancer (GWLB). The network engineer provisions another VPC, VPC B, in a separate account and deploys the two firewall appliances in separate Availability Zones.

What should the network engineer do to configure the network connectivity for this solution?

A. Create a GWLB in VPC A with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the default route to the VPC endpoint.

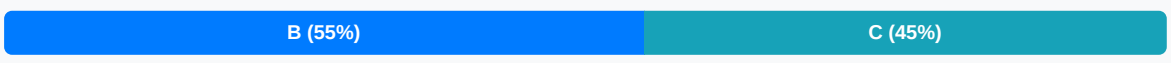
B. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the default route to the GWLB endpoint. **Most Voted**

C. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the WorkSpaces subnet to the VPC endpoint.

D. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWS principal ARN of the account that contains the firewall appliances to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables of VPC A to point the default route to the VPC endpoint.

Correct Answer: B

Community vote distribution



Comments

troopie22 Highly Voted 2 years, 2 months ago

Selected Answer: B

Since the users are at home, default route must point to GWLB endpoint

Rollizo 1 year ago

cannot be B, VPCA has to create a endpoint in AWS account referencing GLWB. But when you create the route from VPCA in AWS A, you have to reference that endpoint, no the GLWB endpoint directly

Balasmaniam Highly Voted 2 years, 3 months ago

b: CORRECT ANS https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/gateway-load-balancer-inspection-east-west-ra.pdf

Rollizo 1 year ago

this scenario is for all the VPCs in the same AWS account

steli0 6 months ago

Selected Answer: B

I think the wording in both B and C needs a bit of correction. In B I understand the service endpoint (as per the diagram here https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html the endpoint will be at the consumer VPC). In Option C what doesn't make sense is to point the VPC subnet to the GWLB which I understand as creating a route with destination the local subnet and next hop the VPC Endpoint.

AikAWS 6 months, 2 weeks ago

Selected Answer: C

Not B. You cannot directly route to a GWLB living in VPC B.

94b9222 7 months ago

Selected Answer: C

Got it. Here is the short and direct version, only text: --- The correct answer is C. In a cross account GWLB setup, the provider VPC (VPC B) hosts the GWLB and exposes it through an endpoint service. The consumer VPC (VPC A) must create its own VPC endpoint of type GatewayLoadBalancer, which places ENIs locally in VPC A. Route tables in VPC A can only point to local resources, so the routes must target this local VPC endpoint, not the remote GWLB. This matches the AWS documentation for GWLB cross account deployments.

1a17d1e 8 months, 1 week ago

Selected Answer: C

In answer B, what was the point of creating the VPC endpoint if we're not refencing/using it? Answer C: You're using the VPC endpoint to reach the GLBP endpoint since the WS VPC is in a separate account.

PRASAD180 1 year ago

Selected Answer: B

B is correct

acloudguru 1 year, 4 months ago

Selected Answer: C

claud 3 told me the answer is C,Modify the route tables of VPC A to point the WorkSpaces subnet to the VPC endpoint: By updating the route tables in VPC A, you ensure that traffic from the WorkSpaces subnet is routed through the VPC endpoint, which then forwards the traffic to the GWLB endpoint and the firewall appliances in VPC B

Newbies 1 year, 5 months ago

B - Routing all traffic from VPCA to the VPC endpoint is unnecessary and potentially risky. Only the WS subnet needs the route to the VPC endpoint for comms with the firewall appliance

mrt261 1 year, 6 months ago

Selected Answer: C

Regarding the option B, Modifying the route tables of VPC A to point the default route to the GWLB endpoint is incorrect because the GWLB is not directly accessible from VPC A. The route tables should be modified to route traffic destined for the WorkSpaces subnet to the appropriate endpoint that facilitates connectivity to the GWLB.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is A according to SPOTO products.

Arad 1 year, 10 months ago

Selected Answer: B

B is the correct answer.

Balasmaniam 2 years, 3 months ago

Important to know: • Using AWS PrivateLink, GWLB Endpoint routes traffic to GWLB. Traffic is routed securely over Amazon network without any additional configuration. B: correct

Balasmaniam 2 years, 3 months ago

Traffic from IP 10.0.1.10 wants to reach IP 10.1.2.20 in the App2 virtual private cloud (VPC). The subnet’s route table routes it to the TGW via the default route (0.0.0.0/0).

takecoffe 2 years, 3 months ago

Selected Answer: C

VPC A need to be modified to direct the traffic from the WorkSpaces subnet to the VPC endpoint

Balasmaniam 2 years, 3 months ago

i think workspace subnet will be used to point to local vpc communication. default route can be used for inspection vpc communication other than more specific route. 10.1.0.0 ---> local 0.0.0.0/0 ---> GWLBE

https://zhangxuetu.online

[202610]

Question #125 Topic 1

A company plans to run a computationally intensive data processing application on AWS. The data is highly sensitive. The VPC must have no direct internet access, and the company has applied strict network security to control access.

Data scientists will transfer data from the company's on-premises data center to the instances by using an AWS Site-to-Site VPN connection. The on-premises data center uses the network range 172.31.0.0/20 and will use the network range 172.31.16.0/20 in the application VPC.

The data scientists report that they can start new instances of the application but that they cannot transfer any data from the on-premises data center. A network engineer enables VPC flow logs and sends a ping to one of the instances to test reachability. The flow logs show the following:

```
2 123456789010 eni-1235b8ca123456789 172.31.8.29 172.31.18.139 0 0 1 4 336 1622433184 1622433194 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.18.139 172.31.8.29 0 0 1 3 252 1622433216 1622433232 REJECT OK
```

The network engineer must recommend a solution that will give the data scientists the ability to transfer data from the on-premises data center.

Which solution will meet these requirements?

A. Modify the security group for the application. Add an inbound rule to allow traffic from the on-premises data center network range to the application.

B. Modify the network ACLs for the VPC subnet. Add an inbound rule to allow traffic from the on-premises data center network range to the VPC subnet range.

C. Modify the network ACLs for the VPC subnet. Add an outbound rule to allow traffic from the VPC subnet range to the on-premises data center network range. **Most Voted**

D. Modify the security group for the application. Add an outbound rule to allow traffic from the application to the on-premises data center network range.

Correct Answer: C

Community vote distribution

C (100%)

Comments

46f094c 1 year, 2 months ago

Selected Answer: C

First the NACL is evaluated (stateless), and then if the traffic is allowed the SG will be evaluated (statefulll). The first packet arrives and is allowed, so NACL ok and SG OK, but the second packet returning is denied. This discard the problem in a SG, because the SG being stateful would allow the traffic. And so must be the NACL denying

woorkim 1 year, 3 months ago

Selected Answer: C

C is correct. because NACL is stateless so thus need to add permit!

Newbies 1 year, 12 months ago

Ans is A - B:Modifying the outbound ACL wouldn't address the inability to initiate data transfer from the on-premises side.

Newbies 1 year, 12 months ago

Sorry D is the answer

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

GaryQian 2 years, 1 month ago

Selected Answer: C

Only ACL can add rules for CIDER range. And the reject happen from AWS to On-prem so it is outbound issue

Arad 2 years, 4 months ago

Selected Answer: C

Obviously C.

Neo00 2 years, 8 months ago

Selected Answer: C

C. Return traffic was blocked by NACL, outbound should be allowed

tcp22 2 years, 9 months ago

C for sure

RVD 2 years, 9 months ago

Selected Answer: C

issue with Outbound NACL

Balasmaniam 2 years, 9 months ago

Selected Answer: C

NACL rejects outbound

papercuts23 2 years, 9 months ago

Selected Answer: C

Agreed. Outbound is reject.

takecoffe 2 years, 9 months ago

Selected Answer: C

yeah outbound is rules needs to added

demoras 2 years, 9 months ago

Selected Answer: C

Answer should be C

Awadhesh 2 years, 9 months ago

Answer should be C

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #126 Topic 1

A company needs to temporarily scale out capacity for an on-premises application and wants to deploy new servers on Amazon EC2 instances. A network engineer must design the networking solution for the connectivity and for the application on AWS.

The EC2 instances need to share data with the existing servers in the on-premises data center. The servers must not be accessible from the internet. All traffic to the internet must route through the firewall in the on-premises data center. The servers must be able to access a third-party web application.

Which configuration will meet these requirements?

A. Create a VPC that has public subnets and private subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a NAT gateway in a public subnet. Create a route table, and associate the public subnets with the route table. Add a default route to the internet gateway. Create a route table, and associate the private subnets with the route table. Add a default route to the NAT gateway. Add routes for the data center subnets to the virtual private gateway. Deploy the application to the private subnets.

B. Create a VPC that has private subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a route table, and associate the private subnets with the route table. Add a default route to the virtual private gateway. Deploy the application to the private subnets. Most Voted

C. Create a VPC that has public subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a route table, and associate the public subnets with the route table. Add a default route to the internet gateway. Add routes for the on-premises data center subnets to the virtual private gateway. Deploy the application to the public subnets.

D. Create a VPC that has public subnets and private subnets. Create a customer gateway, a virtual private gateway, and an AWS Site-to-Site VPN connection. Create a route table, and associate the public subnets with the route table. Add a default route to the internet gateway. Create a route table, and associate the private subnets with the route table. Add routes for the on-premises data center subnets to the virtual private gateway. Deploy the application to the private subnets.

Correct Answer: B

Community vote distribution



Comments

ryluis Highly Voted 2 years, 9 months ago

Selected Answer: B

note this requirement : The servers must not be accessible from the internet. All traffic to the internet must route through the firewall in the on-premises data center. So why do we use NAT GW here, if the requirement said ' All traffic to the internet must route through the firewall in the on-premises data center'

a0e6696 7 months, 1 week ago

Selected Answer: B

If option is B is correct, VPC should have internetgateway attached to form the IPsec S2S vpn

hkh2 1 year, 7 months ago

Nat Gateway required as question asked for access to third party application

cerifyme85 1 year, 11 months ago

Selected Answer: B

B.. this is correct, the other options say "default gateway through IGW" which would not hit the on prem firewall... B is the only plausible answer.. Just always thought we need the IGW to establish public access, but it seems VPG takes care of that

cerifyme85 1 year, 11 months ago

Answer is D.. How do u establish public connectivity first? U need to have a connectivity to the firewall, either using an existing DX connection or setu connection using the public subnet

[Removed] 1 year, 11 months ago

Deploy the application servers to the private subnets. They can access the data center over the VPN connection but are not exposed to the internet.

cerifyme85 1 year, 11 months ago

Yep.. this is correct, the other options say "default gateway through IGW" which would not hit the on prem firewall... B is the only plausible answer.. Just always thought we need the IGW to establish public access, but it seems VPG takes care of that

Marfee400704 2 years, 1 month ago

I think that it's correct answer is D according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: B

B is the correct answer.

ojy 2 years, 6 months ago

Selected Answer: D

Must be D. Direct Connect is required to set up a Private IP Site-to-Site VPN. If there is no Direct Connect, a VPN connection is required through a public subnet.

evargasbrz 2 years, 7 months ago

Selected Answer: B

B is the right. An Internet gateway is not required to establish a Site-to-Site VPN connection. Please, take a look on this: https://aws.amazon.com/vpn/faqs/ Q: How does an AWS Site-to-Site VPN connection work with Amazon VPC? A: An AWS Site-to-Site VPN connection connects your VPC to your datacenter. Amazon supports Internet Protocol

security (IPsec) VPN connections. Data transferred between your VPC and datacenter routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. An Internet gateway is not required to establish a Site-to-Site VPN connection.

Neo00 2 years, 8 months ago

Selected Answer: D

Must be D. Customer GW and Virtual Private Gateway won't work if your VPC doesn't have Public Subnet. In order to establishing S2S VPN, B is wrong.

Cheam 2 years, 7 months ago

"Customer GW and Virtual Private Gateway won't work if your VPC doesn't have Public Subnet." - This is completely false. The creation of the VPG/CGW is tied to your VPC not to the subnet in the VPC. Please refer to this reference guide on how to setup a VPN tunnel to a VPC.
https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html All the best.

tcp22 2 years, 9 months ago

B, you want the default route to point to VGW

devilman222 2 years, 9 months ago

Answer should be B. You don't need to a private subnet as you should only be able to get to the instances from on prem, also you don't need a public subnet with a nat gateway as internet traffic goes through on prem firewall. They should fix "the show answer" to be correct at least 50% of the time. You would be lost going by there answers as they are terrible.

papercuts23 2 years, 9 months ago

Selected Answer: B

i agree with B

takecoffe 2 years, 9 months ago

Selected Answer: B

Why do we need public subnet..

takecoffe 2 years, 9 months ago

changing this to Answer A .. for site -site vpn public subnet is required

Awadhesh 2 years, 9 months ago

Answer should be B. Internet connection must be through firewall at on-prem. No need of public subnet in the VPC.

https://zhangxuetu.online

[202610]

Question #127 Topic 1

A company is deploying a web application into two AWS Regions. The company has one VPC in each Region. Each VPC has three Amazon EC2 instances as web servers behind an Application Load Balancer (ALB). The company already has configured an Amazon Route 53 public hosted zone for example.com. Users will access the application by using the fully qualified domain name (FQDN) of app.example.com.

The company needs a DNS solution that allows global users to access the application. The solution must route the users' requests to the Region that provides the lowest response time. The solution must fail over to the Region that provides the next-lowest response time if the application is unavailable in the initially intended Region.

Which solution will meet these requirements?

A. For each ALB, create an A record that has a geolocation routing policy to route app.example.com to the IP addresses of the ALB. Configure a Route 53 HTTP health check that monitors each ALB by IP address. Associate the health check with the A records.

B. Create an A record that has a geolocation routing policy to route app.example.com to the IP addresses for both ALBs. Configure a Route 53 health check that monitors TCP port 80 for each ALB by IP address. Associate the health check with the A records.

C. Create an A record that has a latency-based routing policy to route app.example.com as an alias to one of the ALBs. Configure a Route 53 health check that monitors TCP port 80 for each ALB by IP address. Associate the health check with the A records.

D. For each ALB, create an A record that has a latency-based routing policy to route app.example.com as an alias to the ALB. Set the value for Evaluate Target Health to Yes for the records. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

Balasmaniam **Highly Voted** 2 years, 9 months ago

D :- ans

woorkim 1 year, 3 months ago

D is correct The correct answer is D. Key DNS and Routing Principles: Latency-based routing optimizes for user experience by routing to the lowest-latency endpoint Health check-based failover ensures application availability Alias

records provide direct integration with AWS resources Multiple records with latency routing allow intelligent global traffic management

vikasj1in 2 years, 1 month ago

Selected Answer: D

Latency-Based Routing Policy: Latency-based routing is suitable for directing traffic to the AWS Region that provides the lowest latency or response time for users. This helps ensure that users are directed to the Region that can deliver the best performance. ALB Configuration: For each ALB, create an A record with a latency-based routing policy. This allows Route 53 to route traffic based on the latency observed from users' locations to the ALBs. Evaluate Target Health: Setting "Evaluate Target Health" to Yes ensures that Route 53 considers the health of the targets (ALBs) when making routing decisions. If the ALB in the initially intended Region becomes unavailable, Route 53 will automatically route traffic to the next healthiest Region.

Tofu13 2 years, 6 months ago

Selected Answer: D

For both latency alias records, you set the value of Evaluate Target Health to Yes. This causes Route 53 to determine whether there are any healthy resources in a region before trying to route traffic there.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html

Certified101 2 years, 7 months ago

Selected Answer: D

D is correct

ISSDoksim 2 years, 7 months ago

agreed - D

https://zhangxuetu.online

[202610]

Question #128 Topic 1

A consulting company manages AWS accounts for its customers. One of the company's customers needs to add intrusion prevention for its environment without having to re-architect the environment. The customer's environment includes five VPCs in two AWS Regions in the United States. VPC-to-VPC connectivity is achieved through VPC peering. The customer does not plan to increase the number of VPCs within the next 2 years. The solution must accommodate unencrypted traffic.

Which solution will meet these requirements?

A. Configure VPC security groups and network ACLs.

B. Use an AWS Network Firewall centralized deployment model in each VPC.

C. Use an AWS Network Firewall distributed deployment model in each VPC. **Most Voted**

D. Deploy AWS Shield in each VPC.

Correct Answer: C

Community vote distribution



Comments

lygf **Highly Voted** 2 years, 9 months ago

Selected Answer: C

Nope, you can't do centralized deployment. "For centralized deployment model, AWS Transit Gateway is a prerequisite." https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/

JosMo 2 years, 8 months ago

Quote: "You can use the same model for inspection of traffic to other AWS Regions using AWS Transit Gateway Inter-Region Peering feature as shown in Figure 8. Remote AWS Regions are treated as spokes." https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/

Josh1217 **Highly Voted** 2 years, 8 months ago

Selected Answer: C

For centralized deployment model, AWS Transit Gateway is a prerequisite. Cannot add a new Shared VPC which is required for Centralized deployment.

woorkim 1 year, 3 months ago

Selected Answer: C

For centralized deployment model, AWS Transit Gateway is a prerequisite.

Spaurito 1 year, 4 months ago

C - The question states - "One of the company's customers needs to add intrusion prevention for its environment without having to re-architect the environment.". This indicates low architectural re-design regardless of time frame.

JoellaLi 1 year, 12 months ago

Selected Answer: C

As the environment spans two AWS Regions with VPC peering, a centralized model would require establishing a separate inspection VPC in each Region. This increases complexity versus directly protecting each VPC.

Arad 2 years, 4 months ago

Selected Answer: C

C is the right answer.

tcp22 2 years, 9 months ago

C The distributed deployment model supports unencrypted traffic and can be set up to protect traffic within each VPC.

Balasmaniam 2 years, 9 months ago

Deployment models There are multiple deployment models available with AWS Network Firewall. The right model depends on the use case and requirements. The following models are most common: Distributed AWS Network Firewall deployment model: AWS Network Firewall is deployed into each individual VPC. Centralized AWS Network Firewall deployment model: AWS Network Firewall is deployed into centralized VPC for East-West (VPC-to-VPC) and/or North-South (internet egress and ingress, on-premises) traffic. We refer to this VPC as inspection VPC throughout this blog post. Combined AWS Network Firewall deployment model: AWS Network Firewall is deployed into centralized inspection VPC for East-West (VPC-to-VPC) and subset of North-South (On Premises/Egress) traffic. Internet ingress is distributed to VPCs which require dedicated inbound access from the internet and AWS Network Firewall is deployed accordingly.

Balasmaniam 2 years, 9 months ago

Centralized AWS Network Firewall deployment model: AWS Network Firewall is deployed into centralized VPC for East-West (VPC-to-VPC) and/or North-South (internet egress and ingress, on-premises) traffic. We refer to this VPC as inspection VPC throughout this blog post. B is correct ans

tcp22 2 years, 9 months ago

it is mentioned company does not have plans to add VPC for next 2 years

Balasmaniam 2 years, 9 months ago

Selected Answer: B

https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/

Training 2 years, 9 months ago

Centralized deployment model is complex and requires architectural changes. It should be C.

Awadhesh 2 years, 9 months ago

C is the answer, each VPC has network firewall in distributed deployment model only.

https://zhangxuetu.online

[202610]

Question #129 Topic 1

A company hosts its IT infrastructure in an on-premises data center. The company wants to migrate the infrastructure to the AWS Cloud in phases. A network engineer wants to set up a 10 Gbps AWS Direct Connect dedicated connection between the on-premises data center and VPCs. The company's network provider needs 3 months to provision the Direct Connect connection.

In the meantime, the network engineer implements a temporary solution by deploying an AWS Site-to-Site VPN connection that terminates to a virtual private gateway. The network engineer observes that the bandwidth of the Site-to-Site VPN connection is capped at 1.25 Gbps despite a powerful customer gateway device.

What should the network engineer do to improve the VPN connection bandwidth before the implementation of the Direct Connect connection?

A. Contact AWS Support to request a bandwidth quota increase for the existing Site-to-Site VPN connection.

B. Discuss the issue with the hardware vendor. Buy a bigger and more powerful customer gateway device that has faster encryption and decryption capabilities.

C. Create several additional Site-to-Site VPN connections that terminate on the same virtual gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.

D. Create a transit gateway. Attach the VPCs to the transit gateway. Create several additional Site-to-Site VPN connections that terminate on the transit gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: D

Transit Gateway : A transit gateway is an AWS service that allows you to create a centralized network hub, making it easier to connect and manage multiple VPCs. Attaching VPCs to the transit gateway : By attaching the VPCs to the transit gateway, you can extend your existing Site-to-Site VPN connections across the different regions or accounts. Creating additional Site-to-Site VPN connections : Adding more Site-to-Site VPN connections that terminate on the transit gateway will increase the available bandwidth and improve overall network throughput. Equal-cost multi-path (ECMP) routing : By configuring ECMP routing, you can direct traffic across multiple VPN connections, increasing the utilization of each connection and improving the overall performance.

woorkim 1 year, 3 months ago

Selected Answer: D

• TGW – Enable BGP and ECMP for VPN connections. • 2 VPN connection x 2 Tunnels per connection x 1.25 Gbps/tunnel = ~5 Gbps • Single flow is still limited to 1.25Gbps

evargasbrz 2 years, 7 months ago

Selected Answer: D

D is the right ECMP is not supported for Site-to-Site VPN connections on a virtual private gateway. You can check this document: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html

Certified101 2 years, 7 months ago

Selected Answer: D

D is correct

Neo00 2 years, 8 months ago

Selected Answer: D

D If you establish multiple VPN tunnels to an ECMP-enabled transit gateway, it can scale beyond the default maximum limit of 1.25 Gbps.

Balasmaniam 2 years, 9 months ago

D:- Ans why is high speed is need to below Per VPN connection, you can achieve 1.25 Gbps of throughput and 140,000 packets per second. When terminating the VPN connections in the Transit Gateway, you can use Equal Cost Multi-Path (ECMP) routing to get a higher VPN bandwidth by aggregating multiple VPN tunnels. To use ECMP, you need to configure dynamic routing in the VPN connections – ECMP is not supported using static routing. https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html

tcp22 2 years, 9 months ago

D for sure

tcp22 2 years, 9 months ago

https://repost.aws/knowledge-center/transit-gateway-ecmp-multiple-tunnels

devilman222 2 years, 9 months ago

The selected answer D, is actually correct this time.

https://zhangxuetu.online

[202610]

Question #130 Topic 1

A company has business operations in the United States and in Europe. The company's public applications are running on AWS and use three transit gateways. The transit gateways are located in the us-west-2, us-east-1, and eu-central-1 Regions. All the transit gateways are connected to each other in a full mesh configuration.

The company accidentally removes the route to the eu-central-1 VPCs from the us-west-2 transit gateway route table. The company also accidentally removes the route to the us-west-2 VPCs from the eu-central-1 transit gateway route table.

How can a network engineer identify the misconfiguration with the LEAST operational overhead?

A. Use the Route Analyzer feature for AWS Transit Gateway Network Manager. **Most Voted**

B. Use the AWSSupport-SetupIPMonitoringFromVPC AWS Systems Manager Automation runbook. Push network telemetry data to Amazon CloudWatch Logs for analysis.

C. Use VPC flow logs in eu-central-1 and us-west-2 to analyze the missing routes.

D. Use Amazon VPC Traffic Mirroring in eu-central-1 or us-west-2 to take packet captures and troubleshoot the connectivity issues.

Correct Answer: A

Community vote distribution

A (100%)

Comments

woorkim 1 year, 3 months ago

Selected Answer: A

Route Analyzer to perform an analysis of the routes in your transit gateway route tables. Through AWS Network Manager, Route Analyzer analyzes the routing path between a specified source and destination, and returns information about the connectivity between components. You can use the Route Analyzer to do the following: Verify that the transit gateway route table configuration will work as expected before you start sending traffic. Validate your existing route configuration. Diagnose route-related issues that are causing traffic disruption in your global network.

Akshay0403 1 year, 8 months ago

You can use the Route Analyzer to do the following: 1.Verify that the transit gateway route table configuration will work as expected before you start sending traffic. 2.Validate your existing route configuration. 3.Diagnose route-related issues that are causing traffic disruption in your global network.

Arad 2 years, 4 months ago

Selected Answer: A

A is the correct answer.

ISSDoksim 2 years, 7 months ago

agreed - A

Balasmaniam 2 years, 9 months ago

Selected Answer: A

https://docs.aws.amazon.com/network-manager/latest/tgwnm/route-analyzer.html

https://zhangxuetu.online

[202610]

Question #131 Topic 1

A marketing company is using hybrid infrastructure through AWS Direct Connect links and a software-defined wide area network (SD-WAN) overlay to connect its branch offices. The company connects multiple VPCs to a third-party SD-WAN appliance transit VPC within the same account by using AWS Site-to-Site VPNs.

The company is planning to connect more VPCs to the SD-WAN appliance transit VPC. However, the company faces challenges of scalability, route table limitations, and higher costs with the existing architecture. A network engineer must design a solution to resolve these issues and remove dependencies.

Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Configure a transit gateway to attach the VPCs. Configure a Site-to-Site VPN connection between the transit gateway and the third-party SD-WAN appliance transit VPC. Use the SD-WAN overlay links to connect to the branch offices.

B. Configure a transit gateway to attach the VPCs. Configure a transit gateway Connect attachment for the third-party SD-WAN appliance transit VPC. Use transit gateway Connect native integration of SD-WAN virtual hubs with AWS Transit Gateway. Most Voted

C. Configure a transit gateway to attach the VPCs. Configure VPC peering between the VPCs and the third-party SD-WAN appliance transit VPUse the SD-WAN overlay links to connect to the branch offices.

D. Configure VPC peering between the VPCs and the third-party SD-WAN appliance transit VPC. Use transit gateway Connect native integration of SD-WAN virtual hubs with AWS Transit Gateway.

Correct Answer: B

Community vote distribution

B (100%)

Comments

Balasmaniam Highly Voted 2 years, 9 months ago

Selected Answer: B

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-sd-wan.html

Akshay0403 1 year, 8 months ago

With the launch of AWS Transit Gateway Connect, there is now a native way to connect your SD-WAN infrastructure with AWS. This makes it easy to extend your SD-WAN into AWS without having to set up IPsec VPNs between SD-WAN network virtual appliances and Transit Gateway.

vikasj1in 2 years, 1 month ago

Selected Answer: B

the use of AWS Transit Gateway with Transit Gateway Connect is a scalable and cost-effective solution to address the challenges of scalability, route table limitations, and higher costs associated with the existing architecture.

Arad 2 years, 4 months ago

Selected Answer: B

B is the right answer.

rarunach 2 years, 5 months ago

Selected Answer: B

Transit gateway connect is the preferred method for SD-WAN.

https://zhangxuetu.online

[202610]

Question #132 Topic 1

A company is running a hybrid cloud environment. The company has multiple AWS accounts as part of an organization in AWS Organizations. The company needs a solution to manage a list of IPv4 on-premises hosts that will be allowed to access resources in AWS. The solution must provide version control for the list of IPv4 addresses and must make the list available to the AWS accounts in the organization.

Which solution will meet these requirements?

A. Create a customer-managed prefix list. Add entries for the initial list of on-premises IPv4 hosts. Create a resource share in AWS Resource Access Manager. Add the managed prefix list to the resource share. Share the resource with the organization. **Most Voted**

B. Create a customer-managed prefix list. Add entries for the initial list of on-premises IPv4 hosts. Use AWS Firewall Manager to share the managed prefix list with the organization.

C. Create a security group. Add inbound rule entries for the initial list of on-premises IPv4 hosts. Create a resource share in AWS Resource Access Manager. Add the security group to the resource share. Share the resource with the organization.

D. Create an Amazon DynamoDB table. Add entries for the initial list of on-premises IPv4 hosts. Create an AWS Lambda function that assumes a role in each AWS account in the organization to authorize inbound rules on security groups based on entries from the DynamoDB table.

Correct Answer: A

Community vote distribution

A (100%)

Comments

Balasmaniam **Highly Voted** 2 years, 9 months ago

Selected Answer: A

https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html

Akshay0403 1 year, 8 months ago

Selected Answer: A

Customer-managed prefix lists — Sets of IP address ranges that you define and manage. AWS Resource Access Manager (AWS RAM) - Helps you securely share your resources across AWS accounts, within your organization or organizational units (OUs).

vikasj1in 2 years, 1 month ago

Selected Answer: A

A customer-managed prefix list in AWS allows you to create a list of IPv4 addresses and prefixes that can be shared with multiple resources across accounts and regions. This makes it suitable for managing a list of on-premises IPv4 hosts that need access to AWS resources. This solution provides a centralized and version-controlled way to manage the list of IPv4 addresses, ensuring consistency and ease of updates across multiple accounts in the AWS organization.

Arad 2 years, 4 months ago

Selected Answer: A

A is correct.

tycho 2 years, 8 months ago

A 100%; answers B C D clearly wrong

https://zhangxuetu.online

[202610]

Question #133 Topic 1

A company's application is deployed on Amazon EC2 instances in a single VPC in an AWS Region. The EC2 instances are running in two Availability Zones. The company decides to use a fleet of traffic inspection instances from AWS Marketplace to inspect traffic between the VPC and the internet. The company is performing tests before the company deploys the architecture into production.

The fleet is located in a shared inspection VPC behind a Gateway Load Balancer (GWLB). To minimize the cost of the solution, the company deployed only one inspection instance in each Availability Zone that the application uses.

During tests, a network engineer notices that traffic inspection works as expected when the network is stable. However, during maintenance of the inspection instances, the internet sessions time out for some application instances. The application instances are not able to establish new sessions.

Which combination of steps will remediate these issues? (Choose two.)

A. Deploy one inspection instance in the Availability Zones that do not have inspection instances deployed.

B. Deploy one additional inspection instance in each Availability Zone where the inspection instances are deployed. Most Voted

C. Enable the cross-zone load balancing attribute for the GWLB. Most Voted

D. Deploy inspection instances in an Auto Scaling group. Define a scaling policy that is based on CPU load.

E. Attach the GWLB to all Availability Zones in the Region.

Correct Answer: BC

Community vote distribution

BC (53%) CD (40%) CE (7%)

Comments

Balasmaniam Highly Voted 2 years, 9 months ago

Ans :BC https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/

ExamTopix01 2 years, 7 months ago

It's CD

dspd 1 year, 1 month ago

Selected Answer: BC

""during maintenance of the inspection instances". So deploying additional instances in each AZ will fix this issue

AzureDP900 1 year, 2 months ago

Selected Answer: BC

Deploying additional inspection instances : When an instance is maintained, other instances can become unavailable. By deploying an extra instance in each Availability Zone, the company can maintain availability of at least one instance per zone. Enabling cross-zone load balancing attribute for GWLB : This ensures that traffic sent to a GWLB can be routed to any available inspection instance in the network, regardless of its location within the region. This helps ensure that application instances remain connected even if an inspection instance is temporarily unavailable.

46f094c 1 year, 4 months ago

Selected Answer: CE

C is clear to LB... But E... why E? because even if it is useless, at least it has no cost. A,B and D has the costs of the new Instances, and they are not needed

chang4li 1 year, 2 months ago

lol, E is not that useless as it appears - it enables other zones to utilize instances in these two zones

Spaurito 1 year, 4 months ago

CD - There are only 2 AZ's. They already have one inspection instance in place. A - is an option but not optimal C - allows for the use of both AZ's. D - allows for scaling when needed. May not be the best metric but will work for this scenario.

Akshay0403 1 year, 8 months ago

Selected Answer: BC

Clearly BC. Questions says ""during maintenance of the inspection instances". So deploying additional instances in each AZ will address this issue

hogtrough 1 year, 9 months ago

Selected Answer: CD

Answer is CD. Not only is autoscaling cost-effective compared to a deploying an instance that will run forever simply for maintenance purposes, it will ensure that the performance needs are met.

steli0 6 months ago

Yes but how scaling based on CPU relates to maintenance ?

seochan 1 year, 10 months ago

Selected Answer: CD

I think it's CD, because the purpose is to "remediate" the problem, and just adding one additional inspection instance cannot assure remediation of this problem.

michele_scar 2 years, 1 month ago

Selected Answer: BC

A and E wrong. It's between B C D. Should be correct D but autoscaling gruop with CPU load not solve the issue, you have to detach the instance, make maintenance and after re-attach to ASG. It's complicated. Finally B C correct.

vikasj1in 2 years, 1 month ago

Selected Answer: CD

A. might distribute the load better across Availability Zones, but it does not directly address the issue of sessions timing out during maintenance. B. could help distribute the load and provide redundancy, but it might not fully address the issue of sessions timing out during maintenance. C. This helps maintain session persistence during maintenance

activities. D. Deploying inspection instances in an Auto Scaling group allows the system to automatically replace instances that are undergoing maintenance or experiencing issues. Defining a scaling policy based on CPU load ensures that additional instances are added to handle increased traffic during maintenance, reducing the impact on existing sessions. E. This helps maintain session persistence during maintenance activities. However, this alone may not fully address the issue if there are not enough healthy instances to handle the traffic.

jorgesoma 2 years, 2 months ago

It's a confused answer. Could be CD or BC... Non clear question from AWS dump.

Arad 2 years, 4 months ago

Selected Answer: CD

I think CD is correct. The solution should be cost-effective, so why deploying an extra instance to site there when it is not necessary all the time, autoscaling group deploys an extra instance just when it is required, not always.

mavik 2 years, 4 months ago

The solution should be cost-effective - there is not a requiremet. BC.

Tofu13 2 years, 6 months ago

Selected Answer: BC

Same Link as Balasmaniam. Point 3 When you enable cross-zone load balancing, GWLB distributes traffic across all registered and healthy targets regardless of which AZs these targets are in.

MohamedSherif1 2 years, 7 months ago

Selected Answer: CD

why not CD?

Certified101 2 years, 7 months ago

Selected Answer: BC

BC is correct

ISSDoksim 2 years, 7 months ago

BC - https://aws.amazon.com/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer/

https://zhangxuetu.online

[202610]

Question #134 Topic 1

A company has developed a new web application on AWS. The application runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate behind an Application Load Balancer (ALB) in the us-east-1 Region. The application uses Amazon Route 53 to host the DNS records for the domain. The content that is served from the website is mostly static images and files that are not updated frequently. Most of the traffic to the website from end users will originate from the United States. Some traffic will originate from Canada and Europe.

A network engineer needs to design a solution that will reduce latency for end users at the lowest cost. The solution also must ensure that all traffic is encrypted in transit until the traffic reaches the ALB.

Which solution will meet these requirements?

A. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that is assigned to the accelerator for the ALB.

B. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point to the DNS record that is assigned to the ALConfigure the CloudFront distribution to use an SSL certificate. Set all behaviors to force HTTPS. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that is assigned to the ALB.

C. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point to the DNS record that is assigned to the ALB. Configure the CloudFront distribution to use an SSL certificate and redirect HTTP to HTTPS. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the CloudFront distribution. Most Voted

D. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create a second application stack on Amazon ECS on Fargate in the eu-west-1 Region. Create another secure HTTPS listener. Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to use a latency-based routing policy to route to the DNS name that is assigned to the accelerator for the ALBs.

Correct Answer: C

Community vote distribution



Comments

TravelKo Highly Voted 2 years, 8 months ago

Selected Answer: C

C is the right answer. Route 53 record points to Cloudfront default DNS name.

lygf Highly Voted 2 years, 9 months ago

Selected Answer: C

Global Accelerator needs NLB and static IP address which ALB won't have. A & D is out. When you create a distribution, CloudFront assigns a domain name to the distribution, such as d111111abcdef8.cloudfront.net. You can use this domain name in the URLs for your content. When you use a Route 53 domain name with a CloudFront distribution, use Amazon Route 53 to create an alias record that points to your CloudFront distribution. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

fmunozse 2 years, 8 months ago

Fyi, Global accelerator works With alb, https://aws.amazon.com/blogs/networking-and-content-delivery/improving-availability-and-performance-for-application-load-balancers-using-one-click-integration-with-aws-global-accelerator/

Hubabi 1 year ago

Selected Answer: C

A) Configure the alias record to route to the DNS name that is assigned to the accelerator for the ALB --> Wrong, then users bypass the Global Accelerator B) Configure the alias record to route to the DNS name that is assigned to the ALB --> Wrong, then users bypass the CloudFront Distribution D) Use R53 latency-based routing to route to Global Accelerator --> :clown: C is the only one that fits the requirements (and that makes sense)

6e5b127 1 year, 8 months ago

Selected Answer: A

The solution also MUST ensure that all traffic is encrypted in transit until the traffic reaches the ALB. CloudFront terminates SSL at the edge. This means that while traffic is encrypted from the user to CloudFront, CloudFront would then establish a new SSL connection to the origin. So the answer is A.

JoellaLi 1 year, 12 months ago

Selected Answer: C

We choose CloudFront not Accelerator since the sentence 'The content that is served from the website is mostly static images and files that are not updated frequently. '

JosMo 2 years, 8 months ago

Selected Answer: C

Answer: C because it redirect the HTTP to HTTPS. B, enforce HTTPS, which is good but not optimal

Pratap 2 years, 9 months ago

Selected Answer: B

B seems to be the right Answer

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #135 Topic 1

A company deploys an internal website behind an Application Load Balancer (ALB) in a VPC. The VPC has a CIDR block of 172.31.0.0/16. The company creates a private hosted zone for the domain example.com for the website in Amazon Route 53. The company establishes an AWS Site-to-Site VPN connection between its office network and the VPC.

A network engineer needs to set up a DNS solution so that employees can visit the internal webpage by accessing a private domain URL (https://example.com) from the office network.

Which combination of steps will meet this requirement? (Choose two.)

A. Create an alias record that points to the ALB in the Route 53 private hosted zone. **Most Voted**

B. Create a CNAME record that points to the ALB internal domain in the Route 53 private hosted zone.

C. Create a Route 53 Resolver inbound endpoint. On the office DNS server, configure a conditional forwarder to forward the DNS queries to the Route 53 Resolver inbound endpoint. **Most Voted**

D. Create a Route 53 Resolver outbound endpoint. On the office DNS server, configure a conditional forwarder to forward the DNS queries to the Route 53 Resolver outbound endpoint.

E. On the office DNS server, configure a conditional forwarder for the private domain to the VPC DNS at 172.31.0.2.

Correct Answer: AC

Community vote distribution

AC (68%) AB (32%)

Comments

Certified101 **Highly Voted** 2 years, 7 months ago

Selected Answer: AC

AC is correct - why would you select A & B ? makes no sense, Alias records are free for AWS resources, you would get charged for lookups for CNAME records.

Tofu13 2 years, 6 months ago

Also, u can't create a CNAME record that has the same name as the hosted zone (the zone apex). So B is out.

Pratap **Highly Voted** 2 years, 9 months ago

Selected Answer: AC

Alias record in Route 53 and conditional forwarding from on premise DNS to INBOUND endpoint

Ohnet 3 months, 3 weeks ago

Selected Answer: AC

AC.....

46f094c 1 year, 2 months ago

Selected Answer: AC

A- you need an ALIAS record to point to the APEX root example.com B- can't point to the APEX root domain example.com C- You need an inbound endpoint to resolve from the office to AWS D- no, outbound is to resolve from AWS to the office E- even if it works and it's free, I wouldn't use this as it doesn't scale and can't customize rules

woorkim 1 year, 3 months ago

A,C is answer. CNAME is not allowed for same domain name in hosted zone.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is AC.

TravelKo 2 years, 8 months ago

Selected Answer: AC

Question is for combination not for various options. So it is AC.

JosMo 2 years, 8 months ago

Selected Answer: AB

Answer: AC, Can't be AB because you wont create an ALIAS and a CNAME for the same record

JosMo 2 years, 8 months ago

remove my comments please wrong selected answer

ryluis 2 years, 9 months ago

Selected Answer: AB

The question doesn't mention any existence of on prem DNS server.

AJ7428 2 years, 9 months ago

The question clearly mentioned access from the office network, some sort of DNS required at least for forwarding dns query so answer should be AC, where on prem query goes to inbound route 53 resolver.

tcp22 2 years, 9 months ago

A and C

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #136 Topic 1

A company is deploying AWS Cloud WAN with edge locations in the us-east-1 Region and the ap-southeast-2 Region. Individual AWS Cloud WAN segments are configured for the development environment, the production environment, and the shared services environment at each edge location. Many new VPCs will be deployed for the environments and will be configured as attachments to the AWS Cloud WAN core network.

The company's network team wants to ensure that VPC attachments are configured for the correct segment. The network team will tag the VPC attachments by using the Environment key with a value of the corresponding environment segment name. The segment for the production environment in us-east-1 must require acceptance for attachment requests. All other attachment requests must not require acceptance.

Which solution will meet these requirements?

A. Create a rule with a number of 100 that requires acceptance for attachments to the production segment. In the rule, set the condition logic to the "or" value. Include conditions that require a tag:Environment value of Production or a Region value of us-east-1. Create a rule with a number of 200 that does not require acceptance to map any tag:Environment values to their respective segments.

B. Create a rule with a number of 100 that requires acceptance for attachments to the production segment. In the rule, set the condition logic to the "and" value. Include conditions that require a tag:Environment value of Production and a Region value of us-east-1. Create a rule with a number of 200 that does not require acceptance to map any tag.Environment values to their respective segments. Most Voted

C. Create a rule with a number of 100 that does not require acceptance to map any tag:Environment values to their respective segments. Create a rule with a number of 200 that requires acceptance for attachments to the production segment. In the rule, set the condition logic to the "and" value. Include conditions that require a tag:Environment value of Production and a Region value of us-east-1.

D. Create a rule with a number of 100 that does not require acceptance to map any tag:Environment values to their respective segments. Create a rule with a number of 200 that requires acceptance for attachments to the production segment. In the rule, set the condition logic to the "or" value. Include conditions that require a tag:Environment value of Production or a Region value of us-east-1.

Correct Answer: B

Community vote distribution

B (100%)

Comments

TravelKo Highly Voted 2 years, 8 months ago

Selected Answer: B

I think B is correct.

Blitz1 1 year, 8 months ago

Selected Answer: B

CD - are not ok because the rules are processed in order and if first rule is matched will not go to second rule (like in NACL) and we want to enforce attachment acceptance Now discussion is between A and B. Because question is saying: The segment for the production environment in us-east-1 must require acceptance" you basically need an AND between production env and us-east-1. If the question was saying " The segment for the production environment must require acceptance" then the answer will become A because you need to match production env without taking care about region.

[Removed] 1 year, 11 months ago

Funny thing on this question is you do not need to understand a single bit on CloudWAN. All you need to know here is production = us-east-1 (-> and condition) and acceptance.

Sailor 1 year, 11 months ago

Hahahahah

Newbies 1 year, 12 months ago

C for sure

ISSDoksim 2 years, 7 months ago

B - I guess https://docs.aws.amazon.com/network-manager/latest/cloudwan/cloudwan-policy-attachments.html

ISSDoksim 2 years, 7 months ago

change to A

JoellaLi 1 year, 12 months ago

why A?

mmiravet 2 years, 8 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/achieving-traffic-segmentation-in-multi-aws-region-environments-using-aws-transit-gateway-and-aws-cloud-wan/

https://zhangxuetu.online

[202610]

Question #137 Topic 1

A company is migrating applications from a data center to AWS. Many of the applications will need to exchange data with the company's on-premises mainframe.

The company needs to achieve 4 Gbps transfer speeds to meet peak traffic demands. A network engineer must design a highly available solution that maximizes resiliency. The solution must be able to withstand the loss of circuits or routers.

Which solution will meet these requirements?

A. Order four 10 Gbps AWS Direct Connect connections that are evenly spread over two locations. Terminate one connection from each Direct Connect location to a router at the company location. Terminate the other connection from each Direct Connect location to a different router at the company location. **Most Voted**

B. Order two 10 Gbps AWS Direct Connect connections that are evenly spread over two locations. Terminate the connection from each Direct Connect location to a different router at the company location.

C. Order four 1 Gbps AWS Direct Connect connections that are evenly spread over two locations. Terminate one connection from each Direct Connect location to a router at the company location. Terminate the other connection from each Direct Connect location to a different router at the company location.

D. Order two 1 Gbps AWS Direct Connect connections that are evenly spread over two locations. Terminate the connection from each Direct Connect location to a different router at the company location.

Correct Answer: A

Community vote distribution



Comments

tcp22 Highly Voted 2 years, 9 months ago

I go with B, Option A suggests ordering four 10 Gbps Direct Connect connections, which may be unnecessary for achieving the required 4 Gbps transfer speeds and could increase costs without providing significant benefits.

Pratap Highly Voted 2 years, 9 months ago

Selected Answer: A

A is the right ans

mardensilva 7 months ago

Selected Answer: A

English is not my native language, but, rereading, it is in fact alternative A, I believe it refers to this doc: https://docs.aws.amazon.com/directconnect/latest/UserGuide/resiliency_toolkit.html

ryuhei 8 months, 2 weeks ago

Selected Answer: B

A and B meet the requirements, but I think A is over-designed. B is considered sufficient in terms of availability and fault tolerance.

ron1601 1 year, 9 months ago

Selected Answer: A

https://docs.aws.amazon.com/directconnect/latest/UserGuide/maximum_resiliency.html maximum resiliency

rltk8029 1 year, 11 months ago

So, Answer - A -- because they checking your english again not a engineering skills. 'B' - is OPTIMIZED option. 'A' is MAXIMIZED. Question is about MXIMAZIED solution -'A network engineer must design a highly available solution that **maximizes** resiliency.

ankit_agarwal 2 months, 3 weeks ago

loved the way you explained. Agree. Based on the Question, it is asking for Maximizing resiliency.

Stants 2 years ago

The correct solution is A. Order four 10 Gbps AWS Direct Connect connections that are evenly spread over two locations. Terminate one connection from each Direct Connect location to a router at the company location. Terminate the other connection from each Direct Connect location to a different router at the company location. This solution meets the requirements because it provides the necessary 4 Gbps transfer speed and maximizes resiliency. By spreading the Direct Connect connections over two locations and terminating them at different routers, the solution can withstand the loss of circuits or routers, ensuring high availability. Please note that the other options do not fully meet the requirements. Options B, C, and D do not provide the necessary redundancy and resiliency. Option C does not provide the required 4 Gbps transfer speed.

billgoldberg14 1 year, 11 months ago

Option B: Order two 10 Gbps AWS Direct Connect connections that are evenly spread over two locations. Terminate the connection from each Direct Connect location to a different router at the company location. It's 2 completely different circuits at 2 different locations and terminates on different routers on-prem, how does this not meet the requirements?

vikasj1in 2 years, 1 month ago

Selected Answer: A

To achieve 4 Gbps transfer speeds with high availability and resiliency, you would typically want to aggregate multiple AWS Direct Connect connections. Option A and Option B both involve ordering multiple 10 Gbps AWS Direct Connect connections, making them potential solutions. However, Option A provides additional redundancy by terminating connections to different routers at the company location, which enhances resiliency.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is A.

ChinkSantana 2 years, 1 month ago

A is an overkill but the question focuses on RESILIENCY. So A is the correct answer

Reyad789 2 years, 2 months ago

If English is not your first language and you answer "B", then frankly, you are stupid.

Reyad789 2 years, 2 months ago

*sorry, I meant (is) your first language. Just trying to remove the confusion, the answer is definitely (A), because the solution can withstand circuit and router failures in each location.

ChinkSantana 2 years, 2 months ago

You dont have to use such words in learning platform.

Marchel_EU 2 years, 2 months ago

Selected Answer: A

maximum resiliency architecture

mavik 2 years, 4 months ago

Selected Answer: A

A network engineer MUST design a highly available solution that MAXIMIZES RESILIENCY

Arad 2 years, 4 months ago

Selected Answer: B

I think the right answer is B.

sanalainen 2 years, 4 months ago

Selected Answer: B

B provides high-availability and enough capacity during peaks.

Cheam 2 years, 5 months ago

Selected Answer: B

Everyone voted for answer A but the answer does not even make sense. 1) Order *four* 10 Gbps AWS Direct Connect connections that are evenly spread over two locations. 2)Terminate *one connection* (not connections) from each Direct Connect location to a router at the company location. 3) Terminate the *other connection* (didn't say connections) from each Direct Connect location to a different router at the company location. What happened to the other two Direct Connect lines that was ordered? And there's no mention of LAG either. All the best.

Cheam 2 years, 5 months ago

I re-read that answer again and it is a connection per DX location (2x) per router. So I change my answer to A to fulfil the maximum resiliency requirement of the question. All the best.

payelix795 2 years, 7 months ago

Selected Answer: A

My guess is that the answer lies in the following statement in the question "that maximizes resiliency" ie Maximum Resiliency DX Connection Design

https://zhangxuetu.online

[202610]

Question #138 Topic 1

A company has 10 web server Amazon EC2 instances that run in an Auto Scaling group in a production VPC. The company has 10 other web servers that run in an on-premises data center. The company has a 10 Gbps AWS Direct Connect connection between the on-premises data center and the production VPC.

The company needs to implement a load balancing solution that receives HTTPS traffic from thousands of external users. The solution must distribute the traffic across the web servers on AWS and the web servers in the on-premises data center. Regardless of the location of the web servers, HTTPS requests must go to the same web server throughout the entire session.

Which solution will meet these requirements?

A. Create a Network Load Balancer (NLB) in the production VPC. Create a target group. Specify ip as the target type. Register the EC2 instances and the on-premises servers with the target group Enable connection draining on the NLB

B. Create an Application Load Balancer (ALB) in the production VPC. Create a target group Specify ip as the target type. Register the EC2 instances and the on-premises servers with the target group. Enable application-based session affinity (sticky sessions) on the ALB. Most Voted

C. Create a Network Load Balancer (NLB) in the production VPCreate a target group. Specify instance as the target type. Register the EC2 instances and the on-premises servers with the target group. Enable session affinity (sticky sessions) on the NLB.

D. Create an Application Load Balancer (ALB) in the production VPC. Create a target group. Specify instance as the target type Register the EC2 instances and the on-premises servers with the target group Enable application-based session affinity (sticky sessions) on the ALB.

Correct Answer: B

Community vote distribution



Comments

Josh1217 Highly Voted 2 years, 8 months ago

Selected Answer: B

Only 'IP' target type will allow load balancing across On-Prem and Cloud. Plus need Stickiness. So Option B.

Blitz1 1 year, 8 months ago

Selected Answer: B

Something is wrong with question or answers. When you create target groups you can specify the target type either: 1) Instances (and here you can add also EC2 scaling groups) 2) IP Address (Supports load balancing to VPC and on-premises resources.) But when you have both EC2 scaling and on-prem IP what can you do ? Plus it is saying "receives HTTPS traffic from thousands of external users" which implies that autoscale should work to accommodate. A very complex solution will be to have ALB in ALB meaning that in the target groups of first ALB you will have IP of the on-prem server and the IP of a load-balancer which includes the EC2 auto-scalling group but it's kinda a nightmare to proper manage this thing but technically possible. So only because of that i will go for B but i strongly believe something is wrong with the question.

mavik 2 years, 4 months ago

Selected Answer: B

NLB doesn't support sticky session

Arad 2 years, 4 months ago

Selected Answer: B

B is the right answer.

awskiller007 2 years, 7 months ago

B https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/

JosMo 2 years, 8 months ago

Selected Answer: B

aggred on B

Balasmaniam 2 years, 9 months ago

B is correct ans

Balasmaniam 2 years, 9 months ago

doubt on answer: C, because when using an instance ID as a target, an EC2 instance could only receive traffic from the load balancer on its primary IP address and primary network interface. This limits hosting multiple applications on the same instance where each application requires different IP address, network interface, or security group. Using IP addresses as targets removes this limitation as the load balancer can route to multiple IP addresses and network interfaces on the same instance.

Spaurito 1 year, 4 months ago

If the instance gets terminated, the target group will remove the instance as well. You will need to add the new instance back to the target group.

AJ7428 2 years, 9 months ago

Selected Answer: C

Answer to the key is thousands of users connecting..

AJ7428 2 years, 9 months ago

changing to Answer B.

ryluis 2 years, 9 months ago

Selected Answer: B

ALB support on prem's ip address as a target group, and you need session affinity for this.
https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/

Pratap 2 years, 9 months ago

Selected Answer: B

Applcation LB and IP address in TG

takecoffe 2 years, 9 months ago

Selected Answer: C

you need network load balancer to add ips of the onpremise servers

Pratap 2 years, 9 months ago

on premise instances can be added as targets to ALB

https://zhangxuetu.online

[202610]

Question #139 Topic 1

A company has an AWS environment that includes multiple VPCs that are connected by a transit gateway. The company has decided to use AWS Site-to-Site VPN to establish connectivity between its on-premises network and its AWS environment.

The company does not have a static public IP address for its on-premises network. A network engineer must implement a solution to initiate the VPN connection on the AWS side of the connection for traffic from the AWS environment to the on-premises network.

Which combination of steps should the network engineer take to establish VPN connectivity between the transit gateway and the on-premises network? (Choose three.)

A. Configure the Site-to-Site VPN tunnel options to use Internet Key Exchange version 1 (IKEv1).

B. Configure the Site-to-Site VPN tunnel options to use Internet Key Exchange version 2 (IKEv2). Most Voted

C. Use a private certificate authority (CA) from AWS Private Certificate Authority to create a certificate. Most Voted

D. Use a public certificate authority (CA) from AWS Private Certificate Authority to create a certificate.

E. Create a customer gateway. Specify the current dynamic IP address of the customer gateway device's external interface.

F. Create a customer gateway without specifying the IP address of the customer gateway device. Most Voted

Correct Answer: BCF

Community vote distribution



Comments

Neo00 Highly Voted 2 years, 8 months ago

For people who said F is wrong, please read this 'An IP address is not required when you are using a private certificate from AWS Private Certificate Authority.' https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html

AJ7428 Highly Voted 2 years, 9 months ago

Selected Answer: BCF

BCF is the right answer.

Nouwara 10 months, 3 weeks ago

Selected Answer: BCF

F. Create a customer gateway without specifying the IP This is only allowed when using certificate-based VPNs. You do not specify a static IP when using AWS-initiated VPNs, as the customer gateway has a dynamic public IP.

Spaurito 1 year, 4 months ago

Option D doesn't makes sense. Once it changes, it is no longer valid for the configuration.

Spaurito 1 year, 4 months ago

BCF - If your customer gateway IP address is dynamic, then leave the IP Address field empty. If your customer gateway IP address is static, then you can choose to leave this field empty, or specify the IP address.

YogiB1 1 year, 10 months ago

Selected Answer: ACF

ACF --> https://repost.aws/knowledge-center/vpn-certificate-based-site-to-site

YogiB1 1 year, 10 months ago

BCF I meant

acloudguru 1 year, 11 months ago

Selected Answer: BCE

E is correct based on Amazon Q's answer

mrt261 2 years ago

Selected Answer: BCF

An IP address is not required when you are using a private certificate from AWS Private Certificate Authority and a public VPN. https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html

vikasj1in 2 years, 1 month ago

Selected Answer: BCE

b) IKEv2 provides better security and flexibility compared to IKEv1, making it a preferred choice for VPN connections. c) Since the on-premises network does not have a static public IP address, using a private CA allows for the issuance of certificates for authentication without relying on public infrastructure. e) In this scenario, the customer gateway represents the on-premises VPN device. By specifying the current dynamic IP address of the customer gateway's external interface, AWS can establish the VPN connection even if the IP address changes dynamically.

Arad 2 years, 4 months ago

Selected Answer: BCF

BCF is the right answer.

luisfsm_111 2 years, 6 months ago

Selected Answer: BCF

It's BCF: https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html#:~:text=(Optional)%20The%20IP,for%20more%20info.

MohamedSherif1 2 years, 7 months ago

Selected Answer: BCF

An IP address is not required when you are using a private certificate from AWS Private Certificate Authority.

MohamedSherif1 2 years, 7 months ago

Selected Answer: BCE

You can't create customer gateway without Specify the IP address

wartywarthog 2 years, 8 months ago

The IP address needs to be static, so E can't be a right answer.

Balasmaniam 2 years, 9 months ago

https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-tunnel-authentication-options.html V BCF

RVD 2 years, 9 months ago

Selected Answer: BCF

An IP address is not required when you are using a private certificate from AWS Private Certificate Authority.

demoras 2 years, 9 months ago

BCF might be the right answer: An IP address is not required when you are using a private certificate from AWS Private Certificate Authority. https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html

https://zhangxuetu.online

[202610]

Question #140 Topic 1

A company's AWS environment has two VPCs. VPC A has a CIDR block of 192.168.0.0/16. VPC B has a CIDR block of 10.0.0.0/16. Each VPC is deployed in a separate AWS Region. The company has remote users who work outside the company's offices. These users need to connect to an application that is running in the VPCs.

Traffic to and from the VPCs over the internet must be encrypted. A network engineer must set up connectivity between the remote users and the VPCs.

Which combination of steps should the network engineer take to meet these requirements with the LEAST management overhead? (Choose three.)

A. Establish an AWS Site-to-Site VPN connection between VPC A and VPC B.

B. Establish a VPC peering connection between VPC A and VPC B. Most Voted

C. Create an AWS Client VPN endpoint in VPC A and VPC B Add an authorization rule to grant access to VPC A and VPC B.

D. Create an AWS Client VPN endpoint in VPC A Add an authorization rule to grant access to VPC A and VPC B. Most Voted

E. Add a route to the AWS Client VPN endpoint's route table to direct traffic to VPC B. Most Voted

F. Add a route to the AWS Client VPN endpoint's route table to direct traffic to VPC A.

Correct Answer: BDE

Community vote distribution



Comments

JosMo Highly Voted 2 years, 2 months ago

Selected Answer: BDE

BDE, i was doubting but here's what I found. Quote: "The procedure for allowing access to a peered VPC outlined below, is only required if the Client VPN endpoint was configured for split-tunnel mode. In full-tunnel mode, access to the peered VPC is allowed by default." https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html

papercuts23 Highly Voted 2 years, 3 months ago

Selected Answer: BDE

i think it;s BDE

secdaddy 1 year, 1 month ago

Selected Answer: ADE

B is out as the VPCs are in different regions so I think ADE : one endpoint in VPC A + Site to Site VPN for VPCA to VPCB + add the VPCB route (as to my understanding the VPCA route is there by default as the client is connecting to VPCA)

vikasj1in 1 year, 7 months ago

Selected Answer: CEF

C) This step involves setting up AWS Client VPN endpoints in both VPC A and VPC B to allow remote users to connect securely. Adding an authorization rule will control access to both VPCs. E) By adding a route in the AWS Client VPN endpoint's route table, the traffic from remote users can be directed to the resources in VPC B. F) Similarly, adding a route for VPC A ensures that traffic from remote users can reach the resources in VPC A.

nuzz 1 year, 8 months ago

BDE
https://aws.amazon.com/vpn/faqs/#:~:text=A%3A%20You%20can%20achieve%20this,in%20the%20Client%20VPN%20endpoint.

Arad 1 year, 10 months ago

Selected Answer: BDE

BDE is the correct answer.

habros 1 year, 11 months ago

Selected Answer: BDE

BDE. Create VPN endpoint in VPC A -> peer with VPC B -> hence clients will be able to connect to VPC B, via VPC A. Client -> VPC A -> VPC B

RVD 2 years, 3 months ago

Selected Answer: BDE

ANS: BDE

lygf 2 years, 3 months ago

Selected Answer: CEF

Inter-region VPC peering is only available in certain AWS regions. Therefore, B is evidently wrong as the question didn't mention the specific region names. You will need to create two VPN connections.
https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/

lygf 2 years, 3 months ago

Sorry my bad. Inter-region peering is now fully supported on AWS. So BDE is correct.
https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

sdey0008 2 years, 3 months ago

VPN peering will not work here as both VPC are in different region.

Balasmaniam 2 years, 3 months ago

Selected Answer: BDE

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

demoras 2 years, 3 months ago

Should it be CEF? https://aws.amazon.com/blogs/networking-and-content-delivery/building-multi-region-aws-client-vpn-with-microsoft-active-directory-and-amazon-route-53/

https://zhangxuetu.online

[202610]

Question #141 Topic 1

A company uses Amazon Route 53 to register a public domain, example.com, in an AWS account. A central services group manages the account. The company wants to create a subdomain, test.example.com, in another AWS account to offer name services for Amazon EC2 instances that are hosted in the account. The company does not want to migrate the parent domain to the subdomain account.

A network engineer creates a new Route 53 hosted zone for the subdomain in the second account.

Which combination of steps must the network engineer take to complete the task? (Choose two.)

A. Add records for the hosts of the new subdomain to the new Route 53 hosted zone. Most Voted

B. Update the DNS service for the parent domain by adding name server (NS) records for the subdomain. Most Voted

C. Update the DNS service for the subdomain by adding name server (NS) records for the parent domain.

D. Create an alias record from the parent domain that points to the hosted zone for the subdomain in the second account.

E. Add a start of authority (SOA) record in the parent domain for the subdomain.

Correct Answer: AB

Community vote distribution



Comments

Balasmaniam Highly Voted 1 year, 9 months ago

Selected Answer: AB

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingNewSubdomain.html

Arad 1 year, 4 months ago

Selected Answer: AB

AB is correct.

Pratap 1 year, 9 months ago

Selected Answer: AC

Create a record for test.example.com in new AWS account Add example.com in the NS for the newly created record

takecoffe 1 year, 9 months ago

its wrong, you will have to add NS server in the parent dns

johnconnor 1 year, 8 months ago

Respectfully, "After your changes to Amazon Route 53 records have propagated (see Checking the status of your changes (API only)), update the DNS service for the parent domain by adding NS records for the subdomain." So it is A and B

Pratap 1 year, 9 months ago

Yup AB is the right combination

https://zhangxuetu.online

[202610]

Question #142 Topic 1

An IoT company collects data from thousands of sensors that are deployed in the Unites States and South Asia. The sensors use a proprietary communication protocol that is built on UDP to send the data to a fleet of Amazon EC2 instances. The instances are in an Auto Scaling group and run behind a Network Load Balancer (NLB). The instances, Auto Scaling group, and NLB are deployed in the us-west-2 Region.

Occasionally, the data from the sensors in South Asia gets lost in transit over the internet and does not reach the EC2 instances.

Which solutions will resolve this issue? (Choose two.)

A. Use AWS Global Accelerator with the existing NLB. **Most Voted**

B. Create an Amazon CloudFront distribution. Specify the existing NLB as the origin.

C. Create a second deployment of the EC2 instances and the NLB in the ap-south-1 Region. Use an Amazon Route 53 latency routing policy to resolve to the Region that provides the least latency. **Most Voted**

D. Create a second deployment of the EC2 instances and the NLB in the ap-south-1 Region. Use an Amazon Route 53 failover routing policy to resolve to an alternate Region in case packets are dropped.

E. Turn on enhanced networking on the EC2 instances by using the most recent Elastic Network Adapter (ENA) drivers.

Correct Answer: AC

Community vote distribution

AC (100%)

Comments

Pratap **Highly Voted** 2 years, 3 months ago

Selected Answer: AC

Global Accelerator is one option Another option is to have a second fleet of ec2 instances deployed in South Asia region and then have Route 53 latency based routing policy enabled Hence A and C are the right answers

ogrefighter 1 year, 6 months ago

Selected Answer: AC

Link for Global Accelerator high-level discussion: https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

Arad 1 year, 10 months ago

Selected Answer: AC

AC is the correct answer.

ISSDoksim 2 years, 1 month ago

agreed - AC

TravelKo 2 years, 2 months ago

Selected Answer: AC

A and C are the better choices.

https://zhangxuetu.online

[202610]

Question #143 Topic 1

A company has an application that runs on a fleet of Amazon EC2 instances. A new company regulation mandates that all network traffic to and from the EC2 instances must be sent to a centralized third-party EC2 appliance for content inspection.

Which solution will meet these requirements?

A. Configure VPC flow logs on each EC2 network interface. Publish the flow logs to an Amazon S3 bucket. Create a third-party EC2 appliance to acquire flow logs from the S3 bucket. Log in to the appliance to monitor network content.

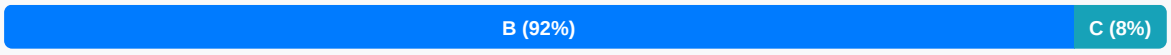
B. Create a third-party EC2 appliance in an Auto Scaling group fronted by a Network Load Balancer (NLB). Configure a mirror session. Specify the NLB as the mirror target. Specify a mirror filter to capture inbound and outbound traffic. For the source of the mirror session, specify the EC2 elastic network interfaces for all the instances that host the application. **Most Voted**

C. Configure a mirror session. Specify an Amazon Kinesis Data Firehose delivery stream as the mirror target. Specify a mirror filter to capture inbound and outbound traffic. For the source of the mirror session, specify the EC2 elastic network interfaces for all the instances that host the application. Create a third-party EC2 appliance. Send all traffic to the appliance through the Kinesis Data Firehose delivery stream for content inspection.

D. Configure VPC flow logs on each EC2 network interface. Send the logs to Amazon CloudWatch. Create a third-party EC2 appliance. Configure a CloudWatch filter to send the flow logs to Amazon Kinesis Data Firehose to load the logs into the appliance.

Correct Answer: B

Community vote distribution



Comments

Wiss7 **Highly Voted** 2 years, 8 months ago

Selected Answer: B

You can use the following resources as traffic mirror targets: Network interfaces of type interface Network Load Balancers Gateway Load Balancer endpoints https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

Spaurito 1 year, 4 months ago

B - Traffic must be sent to and from the 3rd party for inspection. Doesn't define before connecting to endpoints but assuming it does, B would be the solution. C is just capturing the data. Then what.

Arad 2 years, 4 months ago

Selected Answer: B

B is the right answer.

Cheam 2 years, 5 months ago

Selected Answer: B

Similar question to #21. All the best.

[Removed] 2 years, 8 months ago

Selected Answer: B

B because the question is also using a third party tool.

wartywarthog 2 years, 8 months ago

Answer is B. Kinesis Firehose is not a mirror target https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-target.html

AJ7428 2 years, 9 months ago

Selected Answer: B

NLB configured as mirror target, can't use Amazon Kinesis Data Firehose delivery stream.

Balasmaniam 2 years, 9 months ago

Route 53 – Resolver Query Logging • Logs all DNS queries made by resources within a VPC • Private Hosted Zones • Resolver Inbound & Outbound Endpoints • Resolver DNS Firewall • Can send logs to CloudWatch Logs, S3 bucket, or Kinesis Data Firehose • Configurations can be shared with other AWS Accounts using AWS Resource Access Manager (AWS RAM) Resolver Query Logging VPC Route 53 Resolver EC2 Instance example.com? example.com? S3

Balasmaniam 2 years, 9 months ago

SORRY C IS BEST ANS

Balasmaniam 2 years, 9 months ago

B ans 100 %

takecoffe 2 years, 9 months ago

Selected Answer: B

Option C is incorrect because configuring a mirror session to an Amazon Kinesis Data Firehose delivery stream does not involve the use of a third-party EC2 appliance for content inspection.

Pratap 2 years, 9 months ago

Selected Answer: C

The best solution for meeting the requirements is to configure a mirror session and specify an Amazon Kinesis Data Firehose delivery stream as the mirror target. This will allow all network traffic to be sent to the third-party appliance for content inspection without adding any latency to the network traffic.

Pratap 2 years, 9 months ago

C he best solution for meeting the requirements is to configure a mirror session and specify an Amazon Kinesis Data Firehose delivery stream as the mirror target. This will allow all network traffic to be sent to the third-party appliance for content inspection without adding any latency to the network traffic.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #144 Topic 1

A company has two AWS Direct Connect links. One Direct Connect link terminates in the us-east-1 Region, and the other Direct Connect link terminates in the af-south-1 Region. The company is using BGP to exchange routes with AWS.

How should a network engineer configure BGP to ensure that af-south-1 is used as a secondary link to AWS?

A. • On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7100
• On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7300
• On the Direct Connect BGP peer to us-east-1, set the local preference value to 200
• On the Direct Connect BGP peer to af-south-1, set the local preference value to 50

B. • On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7300
• On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7100
• On the Direct Connect BGP peer to us-east-1, set the local preference value to 200
• On the Direct Connect BGP peer to af-south-1, set the local preference value to 50 Most Voted

C. • On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7100
• On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7300
• On the Direct Connect BGP peer to us-east-1, set the local preference value to 50
• On the Direct Connect BGP peer to af-south-1, set the local preference value to 200

D. • On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7300
• On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7100
• On the Direct Connect BGP peer to us-east-1, set the local preference value to 50
• On the Direct Connect BGP peer to af-south-1, set the local preference value to 200

Correct Answer: B

Community vote distribution

B (100%)

Comments

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: B

B is correct

AzureDP900 1 year, 2 months ago

Selected Answer: B

The local preference value determines the relative importance of routes received from different BGP peers; a higher value indicates a more preferred path. By setting the local preference value to 50 on the Direct Connect peer to us-east-1 and 200 on the Direct Connect peer to af-south-1, the network engineer ensures that the af-south-1 link is preferred over the us-east-1 link unless the primary link fails. If the af-south-1 link goes down, BGP will use the us-east-1 link because it has a lower local preference value (50) than the af-south-1 link (200).

ankit_agarwal 2 months, 3 weeks ago

I think you swapped the region name. Answer is B only.

woorkim 1 year, 3 months ago

Selected Answer: B

higher LP, higher community tag# is preffered!

GaryQian 2 years, 1 month ago

Selected Answer: B

B should be correct

Fukat 2 years, 8 months ago

Selected Answer: B

https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

Neo00 2 years, 8 months ago

B. The higher the LOCAL_PREF value, the more preferred the route is.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #145 Topic 1

A team of infrastructure engineers wants to automate the deployment of Application Load Balancer (ALB) components by using the AWS Cloud Development Kit (AWS CDK). The CDK application must deploy an infrastructure stack that is reusable and consistent across multiple environments, AWS Regions, and AWS accounts.

The lead network architect on the project has already bootstrapped the target accounts. The lead network architect also has deployed core network components such as VPCs and Amazon Route 53 private hosted zones across the multiple environments and Regions. The infrastructure engineers must design the ALB components in the CDK application to use the existing core network components.

Which combination of steps will meet this requirement with the LEAST manual effort between environment deployments? (Choose two.)

A. Design the CDK application to read AWS CloudFormation parameters for the values that vary across environments and Regions. Reference these variables in the CDK stack for resources that require the variables.

B. Design the CDK application to read environment variables that contain account and Region details at runtime. Use these variables as properties of the CDK stack. Use context methods in the CDK stack to retrieve variable values. **Most Voted**

C. Create a dedicated account for shared application services in the multi-account environment. Deploy a CDK pipeline to the dedicated account. Create stages in the pipeline that deploy the CDK application across different environments and Regions. **Most Voted**

D. Write a script that automates the deployment of the CDK application across multiple environments and Regions. Distribute the script to engineers who are working on the project.

E. Use the CDK toolkit locally to deploy stacks to each environment and Region. Use the --context flag to pass in variables that the CDK application can reference at runtime.

Correct Answer: BC

Community vote distribution



Comments

4bed5ff **Highly Voted** 2 years, 8 months ago

Selected Answer: BC

B not A:
https://docs.aws.amazon.com/cdk/v2/guide/parameters.html#:~:text=In%20general,we%20recommend%20against%20using%20AWS%20CloudFormation%20parameters%20with%20the%20AWS%20CDK

Manh Highly Voted 2 years, 8 months ago

BC. https://docs.aws.amazon.com/cdk/v2/guide/environments.html you can use environment variables to pass in values that vary across environments and Regions. You can use the --context flag when running cdk deploy to set environment variables for the CDK application. You can also use the CDK_DEFAULT_ACCOUNT and CDK_DEFAULT_REGION environment variables provided by the AWS CDK CLI to specify the target account and Region for deployment.

woorkim 1 year, 3 months ago

B,C is correct! In general, we recommend against using AWS CloudFormation parameters with the AWS CDK. The usual ways to pass values into AWS CDK apps are context values and environment variables. Because they are not available at synthesis time, parameter values cannot be easily used for flow control and other purposes in your CDK app.

vikasj1in 2 years, 1 month ago

Selected Answer: AC

By utilizing AWS CloudFormation parameters for environment-specific values and setting up a CDK pipeline, you can achieve a consistent deployment across multiple environments and Regions with minimal manual effort.

JoellaLi 1 year, 12 months ago

In general, we recommend AGAINST using AWS CloudFormation parameters with the AWS CDK.
https://docs.aws.amazon.com/cdk/v2/guide/parameters.html

Spaurito 1 year, 4 months ago

Something to review for option A In general, we recommend against using AWS CloudFormation parameters with the AWS CDK. The usual ways to pass values into AWS CDK apps are context values and environment variables. Because they are not available at synthesis time, parameter values cannot be easily used for flow control and other purposes in your CDK app.

Suresh108 2 years, 2 months ago

BC.....

habros 2 years, 5 months ago

BC Multi account = AWS organization Fetch such values automatically in CDK via contexts
https://docs.aws.amazon.com/cdk/v2/guide/context.html

Neo00 2 years, 8 months ago

Selected Answer: AC

I think should be AC, the concern I have is A - you can use AWS CloudFormation outputs to read parameters across stacks in the same Region, but you can’t do this across Regions

https://zhangxuetu.online

[202610]

Question #146 Topic 1

A company has critical VPC workloads that connect to an on-premises data center through two redundant active-passive AWS Direct Connect connections. However, a recent outage on one Direct Connect connection revealed that it takes more than a minute for traffic to fail over to the secondary Direct Connect connection. The company wants to reduce the failover time from minutes to seconds.

Which solution will provide the LARGEST reduction in the BGP failover time?

A. Reduce the BGP hold-down timer that is configured on the BGP sessions on the Direct Connect connection VIFs.

B. Configure an Amazon CloudWatch alarm for the Direct Connect connection state to invoke an AWS Lambda function to fail over the traffic.

C. Configure Bidirectional Forwarding Detection (BFD) on the Direct Connect connections on the AWS side.

D. Configure Bidirectional Forwarding Detection (BFD) on the Direct Connect connections on the on-premises router. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

Neo00 **Highly Voted** 1 year, 8 months ago

Selected Answer: D

Asynchronous BFD is automatically turned on for all AWS Direct Connect interfaces on the AWS side. You can't configure BFD settings on the AWS side. When creating a BFD session, the BFD protocol always selects the longer and slower timer.

AzureDP900 1 year, 2 months ago

Selected Answer: D

Configuring Bidirectional Forwarding Detection (BFD) on the Direct Connect connections on the on-premises router will provide the largest reduction in the BGP failover time. BFD is a protocol that enables rapid detection of link or session failures, allowing for faster convergence and faster traffic rerouting. By configuring BFD on the on-premises router, the company can reduce the failover time from minutes to seconds, improving the resiliency of their critical VPC workloads that connect to the on-premises data center through the redundant active-passive AWS Direct Connect connections.

woorkim 1 year, 3 months ago

Selected Answer: D

You can configure Bidirectional Forwarding Detection (BFD) on your network. Asynchronous BFD is automatically enabled for each AWS Direct Connect virtual interface. It's automatically enabled for Direct Connect virtual interfaces, but does not take effect until you configure it on your router.

Certified101 1 year, 7 months ago

Selected Answer: D

D is correct

ISSDoksim 1 year, 7 months ago

agreed - D

Manh 1 year, 8 months ago

it's D. https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html By enabling BFD on both sides of the Direct Connect connection, you can reduce the BGP failover time from minutes to seconds. BFD allows the BGP neighbor relationship to be quickly torn down when a failure is detected on the Direct Connect connection. Otherwise, by default, BGP waits for three keep-alives to fail at a hold-down time of 90 seconds.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #147 **Topic 1**

A European car manufacturer wants to migrate its customer-facing services and its analytics platform from two on-premises data centers to the AWS Cloud. The company has a 50-mile (80.4 km) separation between its on-premises data centers and must maintain that separation between its two locations in the cloud. The company also needs failover capabilities between the two locations in the cloud.

The company's infrastructure team creates several accounts to separate workloads and responsibilities. The company provisions resources in the eu-west-3 Region and in the eu-central-1 Region. The company selects an AWS Direct Connect Partner in each Region and requests two resilient 1 Gbps fiber connections from each provider.

The company's network engineer must establish a connection between all VPCs in the accounts and between the on-premises network and the AWS Cloud. The solution must provide access to all services in both Regions in case of network issues.

Which solution will meet these requirements?

A. Create a Direct Connect gateway. Create a private VIF on each of the Direct Connect connections. Attach the private VIFs to the Direct Connect gateway. Use equal-cost multi-path (ECMP) routing to aggregate the four connections across the two Regions. Attach the Direct Connect gateway directly to each VPC's virtual private gateway.

B. Create a Direct Connect gateway. Create a transit gateway. Attach the transit gateway to the Direct Connect gateway. Create a transit VIF on each of the Direct Connect connections. Attach the transit VIFs to the Direct Connect gateway. Use a link aggregation group (LAG) to aggregate the four connections across the two Regions. Attach the transit gateway directly to each VPC.

C. Create a Direct Connect gateway. Create a transit gateway in each Region. Attach the transit gateways to the Direct Connect gateway. Create a transit VIF on each of the Direct Connect connections. Attach the transit VIFs to the Direct Connect gateway. Peer the transit gateways. Attach the transit gateways in each Region to the VPCs in the same Region. **Most Voted**

D. Create a Direct Connect gateway. Create a private VIF on each of the Direct Connect connections. Attach the private VIFs to the Direct Connect gateway. Use a link aggregation group (LAG) to aggregate the four connections across the two Regions. Create a transit gateway. Attach the transit gateway to the Direct Connect gateway. Attach the transit gateway directly to each VPC.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Manh Highly Voted 2 years, 8 months ago

it's C To establish a connection between all VPCs in the accounts and between the on-premises network and the AWS Cloud, you need to create a Direct Connect gateway and a transit gateway in each Region. You also need to create a transit VIF on each of the Direct Connect connections and attach them to the Direct Connect gateway. Then, you need to attach the transit gateways to the Direct Connect gateway and peer them. Finally, you need to attach the transit gateways in each Region to the VPCs in the same Region.

AzureDP900 1 year, 2 months ago

Selected Answer: C

Providing access to all services in both Regions through the use of separate transit gateways in each Region, which simplifies routing and reduces the number of peering connections required. Aggregating the four 1 Gbps Direct Connect connections using a link aggregation group (LAG) to increase network resiliency and provide higher bandwidth. Ensuring redundancy by establishing connections between both data centers in the cloud through multiple Direct Connect providers. Allowing for failover capabilities by maintaining a connection between the two Regions, so if one Region experiences network issues, traffic can be redirected to the other Region without service disruption. Enabling easy management of resources and responsibilities across multiple accounts by using separate VPCs in each account.

Akshay0403 1 year, 8 months ago

Selected Answer: C

Transit gateway is regional service so need to create in each region.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

Arad 2 years, 4 months ago

Selected Answer: C

C is the right answer.

Certified101 2 years, 7 months ago

Selected Answer: C

C is correct

ISSDoksim 2 years, 7 months ago

c - https://docs.aws.amazon.com/pdfs/whitepapers/latest/hybrid-connectivity/hybrid-connectivity.pdf

https://zhangxuetu.online

[202610]

Question #148 Topic 1

A company wants to analyze TCP traffic to the internet. The traffic originates from Amazon EC2 instances in the company's VPC. The EC2 instances initiate connections through a NAT gateway. The required information includes source and destination IP addresses, ports, and the first 8 bytes of payload of TCP segments. The company needs to collect, store, and analyze all the required data points.

Which solution will meet these requirements?

A. Set up the EC2 instances as VPC traffic mirror sources. Deploy software on the traffic mirror target to forward the data to Amazon CloudWatch Logs. Analyze the data by using CloudWatch Logs Insights. **Most Voted**

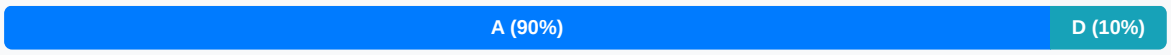
B. Set up the NAT gateway as a VPC traffic mirror source. Deploy software on the traffic mirror target to forward the data to an Amazon OpenSearch Service cluster. Analyze the data by using OpenSearch Dashboards.

C. Turn on VPC Flow Logs on the EC2 instances. Specify the default format and a log destination of Amazon CloudWatch Logs. Analyze the flow log data by using CloudWatch Logs Insights.

D. Turn on VPC Flow Logs on the EC2 instances. Specify a custom format and a log destination of Amazon S3. Analyze the flow log data by using Amazon Athena.

Correct Answer: A

Community vote distribution



Comments

Manh **Highly Voted** 2 years, 8 months ago

Selected Answer: A

VPC Flow Logs capture metadata about the network traffic, such as source and destination IP addresses, source and destination ports, protocol, packet and byte counts, start and end times of the flow, and more. This information is useful for monitoring and troubleshooting network traffic patterns, but it does not include the payload content of TCP segments. If you need to capture and analyze the payload data of TCP segments, you would need to use other monitoring and logging solutions, such as tapping into the network traffic with tools like Traffic Mirroring or using other packet capture mechanisms. These solutions can capture the actual data content for analysis, but they might require more advanced setup and configuration compared to VPC Flow Logs

Certified101 **Highly Voted** 2 years, 7 months ago

Selected Answer: A

NAT Gateways cannot be configured as a traffic mirror source, so option B is not possible.

woorkim 1 year, 3 months ago

Selected Answer: A

Even with a custom format, VPC Flow Logs capture only traffic metadata (e.g., IP addresses and ports) and not payloads. This does not meet the payload inspection requirement.
https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

Newbies 1 year, 12 months ago

D is correct

vikasj1in 2 years, 1 month ago

Selected Answer: D

VPC Flow Logs includes information about allowed and denied traffic (based on security group and network ACL rules). It also includes source and destination IP addresses, ports, the IANA protocol number, packet and byte counts, a time interval during which the flow was observed, and an action (ACCEPT or REJECT). Reference link:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

Marfee400704 2 years, 1 month ago

I think that it's correct answer is D according to SPOTO products.

Neo00 2 years, 8 months ago

Selected Answer: A

VPC flow logs do not capture the actual payload of your IP packets, rather they capture a lot of metadata such as source and destination ports, addresses, number of bytes transferred and very interestingly for us, an action

https://zhangxuetu.online

[202610]

Question #149 Topic 1

A company has three VPCs in a single AWS Region. Each VPC contains 15 Amazon EC2 instances, and no connectivity exists between the VPCs.

The company is deploying a new application across all three VPCs. The application requires high bandwidth between the nodes. A network engineer must implement connectivity between the VPCs.

Which solution will meet these requirements with the HIGHEST throughput?

A. Configure a transit gateway. Attach each VPC to the transit gateway. Configure static routing in each VPC to route traffic to the transit gateway.

B. Configure VPC peering between the three VPCs. Configure static routing to route traffic between the three VPCs. Most Voted

C. Configure a transit VPConfigure a VPN gateway in each VPCreate an AWS Site-to-Site VPN tunnel from each VPC to the transit VPUse BGP routing to route traffic between the VPCs and the transit VPC.

D. Configure AWS Site-to-Site VPN connections between each VPC. Enable route propagation for each Site-to-Site VPN connection to route traffic between the VPCs.

Correct Answer: B

Community vote distribution



Comments

sambb Highly Voted 2 years, 7 months ago

Selected Answer: B

VPC peering has no bandwidth limit unlike Transit Gateway (50Gb/s per VPC attachment) https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf "No bandwidth limits — With Transit Gateway, Maximum bandwidth (burst) per Availability Zone per VPC connection is 50 Gbps. VPC peering has no aggregate bandwidth. "

VijayKamisetty Highly Voted 2 years, 6 months ago

Selected Answer: B

VPC peering is free and also no bandwidth limit compared to 50Gbps limit for a TGW attachment

AzureDP900 1 year, 2 months ago

Selected Answer: A

The correct answer is: A. Configure a transit gateway, attach each VPC to it, and use static routing in each VPC to route traffic to the transit gateway.

woorkim 1 year, 3 months ago

Selected Answer: B

No bandwidth limits — With Transit Gateway, Maximum bandwidth (burst) per Availability Zone per VPC connection is 50 Gbps. VPC peering has no aggregate bandwidth. Individual instance network performance limits and flow limits (10 Gbps within a placement group and 5 Gbps otherwise) apply to both options. Only VPC peering supports placement groups.

46f094c 1 year, 4 months ago

Selected Answer: B

It doesn't ask about scalability or management, it asks about the HIGHEST throughput -> B

jhon648274 1 year, 7 months ago

Answer is A VPC peering does not require static routes to be setup Transit gateway peering provides connectivity to all VPCs and its high throughput

cerifyme85 1 year, 11 months ago

Selected Answer: A

Answer is A. VPC routing is non-transitive, how do you route across all VPC. This what Transit Gateways solves

seochan 1 year, 10 months ago

they only have 3 VPCs.

cerifyme85 1 year, 11 months ago

Answer is A. VPC routing is non-transitive, how do you route across all VPC. This what Transit Gateways solves

vikasj1in 2 years, 1 month ago

Selected Answer: A

In this case, configuring a transit gateway and attaching each VPC to it will provide the highest throughput. The transit gateway allows for more efficient routing of traffic between VPCs compared to VPC peering or Site-to-Site VPN connections. Option B (VPC peering) has limitations on bandwidth and does not scale as well when compared to a transit gateway. Option C (transit VPC with VPN connections) can introduce additional complexity and may not provide as high throughput as a transit gateway. Option D (AWS Site-to-Site VPN connections between each VPC) may work but can introduce additional latency and may not scale as well as a transit gateway. Therefore, option A is the preferred solution for achieving the highest throughput and efficient connectivity between the VPCs.

jorgesoma 2 years, 2 months ago

Non clear correct answer. I think it could be B, better than A.

Nyang2 2 years, 7 months ago

https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html There is no single point of failure for communication or a bandwidth bottleneck.

Manh 2 years, 8 months ago

Selected Answer: A

Transit gateways are designed for high bandwidth and low-latency communication, making them an ideal choice for scenarios where high throughput between multiple VPCs is required. Each attachment to the transit gateway can support up to 50 Gbps of bandwidth, and multiple VPCs can share the same transit gateway without any direct peering relationship between them.

ChinkSantana 2 years, 1 month ago

No bandwidth limits — With Transit Gateway, Maximum bandwidth (burst) per Availability Zone per VPC connection is 50 Gbps. VPC peering has no aggregate bandwidth. Individual instance network performance limits and flow limits (10 Gbps within a placement group and 5 Gbps otherwise) apply to both options. B: VPC peering

Neo00 2 years, 8 months ago

Selected Answer: A

Maximum bandwidth per VPC attachment, AWS Direct Connect gateway, or peered transit gateway connection, Up to 50 Gbps

https://zhangxuetu.online

[202610]

Question #150 Topic 1

A network engineer needs to deploy an AWS Network Firewall firewall into an existing AWS environment. The environment consists of the following:

• A transit gateway with all VPCs attached to it
• Several hundred application VPCs
• A centralized egress internet VPC with a NAT gateway and an internet gateway
• A centralized ingress internet VPC that hosts public Application Load Balancers
• On-premises connectivity through an AWS Direct Connect gateway attachment

The application VPCs have workloads deployed across multiple Availability Zones in private subnets with the VPC route table s default route (0.0.0.0/0) pointing to the transit gateway. The Network Firewall firewall needs to inspect east-west (VPC-to-VPC) traffic and north-south (internet-bound and on-premises network) traffic by using Suricata compatible rules.

The network engineer must deploy the firewall by using a solution that requires the least possible architectural changes to the existing production environment.

Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Deploy Network Firewall in all Availability Zones in each application VPC.

B. Deploy Network Firewall in all Availability Zones in a centralized inspection VPC. Most Voted

C. Update the HOME_NET rule group variable to include all CIDR ranges of the VPCs and on-premises networks. Most Voted

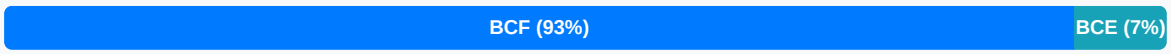
D. Update the EXTERNAL_NET rule group variable to include all CIDR ranges of the VPCs and on-premises networks.

E. Configure a single transit gateway route table. Associate all application VPCs and the centralized inspection VPC with this route table.

F. Configure two transit gateway route tables. Associate all application VPCs with one transit gateway route table. Associate the centralized inspection VPC with the other transit gateway route table. Most Voted

Correct Answer: BCF

Community vote distribution



Comments

Certified101 Highly Voted 1 year, 7 months ago

Selected Answer: BCF

Option B: A centralized inspection VPC approach would lead to a minimal architectural change and efficiently use Network Firewall resources. Option C: HOME_NET is usually defined as your local network. In this case, it would include all your VPCs and on-premises networks. Option F: Configuring two transit gateway route tables, one associated with all the application VPCs and another with the inspection VPC, will help route traffic effectively for inspection. All outbound traffic from application VPCs would be routed to the inspection VPC for firewall checks, and then the inspected traffic would be routed to its destination (internet or another VPC).

AzureDP900 1 year, 2 months ago

Selected Answer: BCF

BCF Deploy Network Firewall in a centralized location : By deploying the Network Firewall in an inspection VPC, you can easily manage and inspect traffic from all parts of your environment. Define security policies : Updating the HOME_NET rule group variable ensures that internal traffic is properly inspected and protected by the Network Firewall. Route traffic effectively : Configuring two transit gateway route tables allows for effective routing of outbound traffic to the inspection VPC for firewall checks, while also ensuring that inspected traffic reaches its destination. These three options provide a comprehensive solution for deploying an AWS Network Firewall in your environment.

woorkim 1 year, 3 months ago

Selected Answer: BCF

To inspect east-west (VPC-to-VPC) and north-south (internet-bound and on-premises) traffic using AWS Network Firewall with minimal changes to the existing environment, you need a scalable and centralized design.

ISSDoksim 1 year, 7 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/

Neo00 1 year, 8 months ago

Selected Answer: BCE

Doesn't make sense separate inspection VPC and other VPC into two TGW RT, if do so, no traffic will be able to send/receive between these

Neo00 1 year, 8 months ago

change to B,C,F https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/

https://zhangxuetu.online

[202610]

Question #151 Topic 1

A company is using a shared services VPC with two domain controllers. The domain controllers are deployed in the company's private subnets. The company is deploying a new application into a new VPC in the account. The application will be deployed onto an Amazon EC2 for Windows Server instance in the new VPC. The instance must join the existing Windows domain that is supported by the domain controllers in the shared services VPC.

A transit gateway is attached to both the shared services VPC and the new VPC. The company has updated the route tables for the transit gateway, the shared services VPC, and the new VPC. The security groups for the domain controllers and the instance are updated and allow traffic only on the ports that are necessary for domain operations. The instance is unable to join the domain that is hosted on the domain controllers.

Which combination of actions will help identify the cause of this issue with the LEAST operational overhead? (Choose two.)

A. Use AWS Network Manager to perform a route analysis for the transit gateway network. Specify the existing EC2 instance as the source. Specify the first domain controller as the destination. Repeat the route analysis for the second domain controller. Most Voted

B. Use port mirroring with the existing EC2 instance as the source and another EC2 instance as the target to obtain packet captures of the connection attempts.

C. Review the VPC flow logs on the shared services VPC and the new VPC. Most Voted

D. Issue a ping command from one of the domain controllers to the existing EC2 instance.

E. Ensure that route propagation is turned off on the shared services VPC.

Correct Answer: AC

Community vote distribution

AC (100%)

Comments

Manh Highly Voted 2 years, 1 month ago

Selected Answer: AC

To identify the cause of this issue with the least operational overhead, you can use AWS Network Manager to perform a route analysis for the transit gateway network. You can specify the existing EC2 instance as the source and one of the domain controllers as the destination. You can repeat the route analysis for the second domain controller. This will help you verify if there is any routing issue between the EC2 instance and the domain controllers through the transit gateway. You can also review the VPC flow logs on the shared services VPC and the new VPC. VPC flow logs

capture information about accepted and rejected IP traffic in your VPCs. You can use VPC flow logs to troubleshoot connectivity issues or monitor network traffic in your VPCs. You can view VPC flow logs in Amazon CloudWatch Logs or Amazon S3.

Marfee400704 1 year, 7 months ago

I think that it's correct answer is AC according to SPOTO products.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #152 Topic 1

A company has an order processing system that needs to keep credit card numbers encrypted. The company's customer-facing application runs as an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer (ALB) in the us-west-2 Region. An Amazon CloudFront distribution is configured with the ALB as the origin. The company uses a third-party trusted certificate authority to provision its certificates.

The company is using HTTPS for encryption in transit. The company needs additional field-level encryption to keep sensitive data encrypted during processing so that only certain application components can decrypt the sensitive data.

Which combination of steps will meet these requirements? (Choose two.)

A. Import the third-party certificate for the ALB. Associate the certificate with the ALB. Upload the certificate for the CloudFront distribution into AWS Certificate Manager (ACM) in us-west-2.

B. Import the third-party certificate for the ALB into AWS Certificate Manager (ACM) in us-west-2. Associate the certificate with the ALUpload the certificate for the CloudFront distribution into ACM in the us-east-1 Region. Most Voted

C. Upload the private key that handles the encryption of the sensitive data to the CloudFront distribution. Create a field-level encryption profile and specify the fields that contain sensitive information. Create a field-level encryption configuration, and choose the newly created profile. Link the configuration to the appropriate cache behavior that is associated with sensitive POST requests.

D. Upload the public key that handles the encryption of the sensitive data to the CloudFront distribution. Create a field-level encryption configuration, and specify the fields that contain sensitive information. Create a field-level encryption profile, and choose the newly created configuration. Link the profile to the appropriate cache behavior that is associated with sensitive GET requests.

E. Upload the public key that handles the encryption of the sensitive data to the CloudFront distribution. Create a field-level encryption profile and specify the fields that contain sensitive information. Create a field-level encryption configuration, and choose the newly created profile. Link the configuration to the appropriate cache behavior that is associated with sensitive POST requests. Most Voted

Correct Answer: BE

Community vote distribution

BE (92%) AE (8%)

Comments

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: BE

Option A: CloudFront does not use certificates stored in AWS Certificate Manager (ACM) in the us-west-2 region. It uses certificates stored in the us-east-1 region, making this option incorrect. Option C: This is incorrect because the private key should not be uploaded to CloudFront for field-level encryption. Instead, the public key is used. A private key must remain confidential and not exposed or uploaded to public services. Option D: This option incorrectly suggests that the field-level encryption profile should be linked to GET requests. Field-level encryption is used for encrypting sensitive information coming in POST requests (like form submissions with credit card details), not for GET requests. Therefore, this option is incorrect.

woorkim 1 year, 3 months ago

Selected Answer: BE

The answer is B and E. Rationale: B ensures proper certificate management E implements field-level encryption for sensitive data like credit card numbers Using POST requests is more secure for sending sensitive information Public key encryption ensures only authorized components can decrypt

Spaurito 1 year, 4 months ago

AE - The Cert, ALB, and CFD should all be in the same region.

JoellaLi 1 year, 12 months ago

For A and B. To use a certificate in AWS Certificate Manager (ACM) to require HTTPS between viewers and CloudFront, make sure you request (or import) the certificate in the US East (N. Virginia) Region (us-east-1). If you want to require HTTPS between CloudFront and your origin, and you're using a load balancer in Elastic Load Balancing as your origin, you can request or import the certificate in any AWS Region. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

Spaurito 1 year, 4 months ago

Not sure I understand why you would import a cert into a region not having anything provisioned. Doesn't make sense.

Spaurito 1 year, 4 months ago

Correction...adding the CFD in a region not in use.

tromyunpak 1 year, 12 months ago

Correct answer BE A is wrong due to cloudfront stores certs in us-east-1 not us-west-2 C is wrong due to the private key (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html) D is wrong because of the get requests as it should be post requests

vikasj1in 2 years, 1 month ago

Selected Answer: AE

Option B is incorrect because it suggests uploading the certificate for the CloudFront distribution into ACM in a different region, which is not necessary and can complicate management. Option A is correct as it suggests importing the third-party certificate directly into ACM in the same region where the ALB is deployed. This simplifies certificate management and allows you to associate the certificate with the ALB. Option E is the correct choice for configuring field-level encryption (FLE). It involves uploading the public key that handles encryption of the sensitive data to the CloudFront distribution, creating a field-level encryption profile to specify the fields containing sensitive information, and then creating a field-level encryption configuration and linking it to the appropriate cache behavior associated with sensitive POST requests. This ensures that sensitive data is encrypted at the field level before being sent to the application components.

ISSDoksim 2 years, 7 months ago

BE - https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #153 Topic 1

A company has deployed a multi-VPC environment in the AWS Cloud. The company uses a transit gateway to connect all the VPCs together. In the past, the company has experienced a loss of connectivity between applications after changes to security groups, network ACLs, and route tables in a VPC. When these changes occur, the company wants to automatically verify that connectivity still exists between different resources in a single VPC.

A. Create a list of paths between different resources to check in VPC Reachability Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in Amazon CloudWatch. Configure the rule to invoke an AWS Lambda function to test the different paths in Reachability Analyzer.

B. Create a list of paths between different resources to check in VPC Reachability Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in AWS. CloudTrail. Configure the rule to invoke an AWS Lambda function to test the different paths in Reachability Analyzer. **Most Voted**

C. Create a list of paths to check in AWS Transit Gateway Network Manager Route Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in Amazon CloudWatch. Configure the rule to invoke an AWS Lambda function to test the diffident paths in Route Analyzer.

D. Create a list of paths to check in AWS Transit Gateway Network Manager Route Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in AWS CloudTrail. Configure the rule to invoke an AWS Lambda function to test the different paths in Route Analyzer.

Correct Answer: B

Community vote distribution



Comments

cerifyme85 **Highly Voted** 1 year, 11 months ago

This is one of the biggest problems with AWS, way too many serivces, that could potentially be doing the same (eg monitoring), and we have know them all and their use cases? Would be a lot easier if their developer just had 2 or 3,and we dont have to remember all these nonsense

ankit_agarwal 2 months, 3 weeks ago

Selected Answer: B

B is right

AzureDP900 1 year, 2 months ago

Selected Answer: A

This solution meets the requirement of automatically verifying connectivity between resources in a single VPC after changes to security groups, network ACLs, and route tables. Here's why other options are not suitable:

woorkim 1 year, 3 months ago

Selected Answer: B

Verify connectivity within a single VPC. This suggests using VPC Reachability Analyzer, which is designed for analyzing paths between resources in a VPC. React automatically to configuration changes. Changes to security groups, NACLs, and route tables are logged in AWS CloudTrail, so monitoring CloudTrail logs is necessary. Automated path validation. Using a Lambda function to invoke the VPC Reachability Analyzer ensures the process is automated.

Spaurito 1 year, 4 months ago

B - all API calls are recorded in CloudTrail. When you make a change in the console, it is a backend API call.

seochan 1 year, 10 months ago

Selected Answer: B

I thought it was D, but it's about reachability in a single VPC. So it's B.

cerifyme85 1 year, 11 months ago

Selected Answer: B

B https://docs.aws.amazon.com/vpc/latest/reachability/logging-using-cloudtrail.html#:~:text=Reachability%20Analyzer%20is,and%20additional%20details

vikasj1in 2 years, 1 month ago

Selected Answer: A

Option B mentions CloudTrail, which is generally used for auditing AWS API calls rather than tracking changes within a VPC. Option C refers to AWS Transit Gateway Network Manager Route Analyzer, which is designed for analyzing routes in a transit gateway network, not within a single VPC. Option D is similar to Option C and is not applicable for checking connectivity within a single VPC. Therefore, Option A is the most appropriate choice for automatically verifying connectivity after changes in a single VPC.

mrt261 2 years ago

https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer

Marfee400704 2 years, 1 month ago

I think that it's correct answer is C according to SPOTO products.

sanalainen 2 years, 4 months ago

Selected Answer: B

"When a security group change is made, the change event is logged in AWS CloudTrail. CloudTrail then forwards the change event to Amazon EventBridge, which evaluates the change against a series of rules to determine if any actions must be taken. Within EventBridge, a rule will be created to forward all security group change events from CloudTrail to an AWS Lambda function. The Lambda function is responsible for determining if any EC2 instances are impacted by the security group change, and if any Reachability Analyzer paths assessing the connectivity from the internet to the instance exist. " [https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/]

Jahm 2 years, 5 months ago

Selected Answer: A

B CloudTrail?

Certified101 2 years, 7 months ago

Selected Answer: B

B https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html

ISSDoksim 2 years, 7 months ago

agreed - B, https://aws.amazon.com/blogs/aws/new-vpc-insights-analyzes-reachability-and-visibility-in-vpcs/

Neo00 2 years, 8 months ago

Selected Answer: B

B https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html

https://zhangxuetu.online

[202610]

Question #154 Topic 1

A company hosts a web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The company uses an Amazon CloudFront distribution with the ALB as an origin.

The application recently experienced an attack. In response, the company associated an AWS WAF web ACL with the CloudFront distribution. The company needs to use Amazon Athena to analyze application attacks that AWS WAF detects.

Which solution will meet this requirement?

A. Configure the ALB and the EC2 instance subnets to produce VPC flow logs. Configure the VPC flow logs to deliver logs to an Amazon S3 bucket for log analysis.

B. Create a trail in AWS CloudTrail to capture data events. Configure the trail to deliver logs to an Amazon S3 bucket for log analysis.

C. Configure the AWS WAF web ACL to deliver logs to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon S3 bucket for log analysis. **Most Voted**

D. Turn on access logging for the ALB. Configure the access logs to deliver the logs to an Amazon S3 bucket for log analysis.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Neo00 **Highly Voted** 2 years, 8 months ago

Selected Answer: C

C To send logs to Amazon Kinesis Data Firehose, you send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, AWS WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose.

JoseCC 2 years, 7 months ago

C Correct. https://aws.amazon.com/blogs/security/trimming-aws-waf-logs-with-amazon-kinesis-firehose-transformations/

woorkim 1 year, 3 months ago

Selected Answer: C

A Kinesis Data Firehose delivery stream is used to receive log records from AWS WAF. An IAM role for the Kinesis Data Firehose delivery stream, with permissions needed to invoke Lambda and write to S3. A Lambda function used to filter out WAF records matching the default action before the records are written to S3. An IAM role for the Lambda function, with the permissions needed to create CloudWatch logs (for troubleshooting). An S3 bucket where the WAF logs will be stored.

vikasj1in 2 years, 1 month ago

Selected Answer: C

Options A and D suggest using VPC flow logs and ALB access logs, respectively. While these logs are valuable for specific purposes (network analysis and access patterns), they do not capture the detailed information about web requests and attacks that are logged by AWS WAF. Option B involves AWS CloudTrail, which is more focused on auditing API calls rather than capturing detailed web request information. Therefore, for analyzing application attacks detected by AWS WAF, configuring AWS WAF logs to be delivered to an Amazon Kinesis Data Firehose stream is the recommended approach.

ISSDoksim 2 years, 7 months ago

agreed - C

https://zhangxuetu.online

[202610]

Question #155 Topic 1

A real estate company is using Amazon Workspaces to provide corporate managed desktop service to its real estate agents around the world. These Workspaces are deployed in seven VPCs. Each VPC is in a different AWS Region.

According to a new requirement, the company's cloud-hosted security information and events management (SIEM) system needs to analyze DNS queries generated by the Workspaces to identify the target domains that are connected to the Workspaces. The SIEM system supports poll and push methods for data and log collection.

Which solution should a network engineer implement to meet these requirements MOST cost-effectively?

A. Create VPC flow logs in each VPC that is connected to the Workspaces instances. Publish the log data to a central Amazon S3 bucket. Configure the SIEM system to poll the S3 bucket periodically.

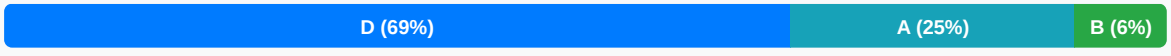
B. Configure an Amazon CloudWatch agent to log all DNS requests in Amazon CloudWatch Logs. Configure a subscription filter in CloudWatch Logs. Push the logs to the SIEM system by using Amazon Kinesis Data Firehose.

C. Configure VPC Traffic Mirroring to copy network traffic from each Workspace and to send the traffic to the SIEM system probes for analysis.

D. Configure Amazon Route 53 query logging. Set the destination as an Amazon Kinesis Data Firehose delivery stream that is configured to push data to the SIEM system. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

Neo00 **Highly Voted** 2 years, 8 months ago

Selected Answer: D

D https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-query-logs-choosing-target-resource.html

46f094c 1 year, 4 months ago

Selected Answer: D

A- no, flow logs does not capture the DNS query itself B- no, do you imagine setting up the agent in ALL workspace instances? C- no, traffic mirror just to analyze DNS queries is an overkill D- YES, native Route53 product functionality

vikasj1in 2 years, 1 month ago

Selected Answer: A

Option B suggests using CloudWatch Logs, but it might result in higher costs compared to VPC Flow Logs, and the push method might introduce additional complexities and costs. Option C (Traffic Mirroring) is a powerful feature, but it may introduce additional costs and complexity, especially when considering the number of Workspaces in different VPCs and Regions. Option D involves Route 53 query logging, which may not capture all DNS queries for Workspaces, especially if they are using different DNS servers. Therefore, option A using VPC Flow Logs is the most cost-effective and straightforward solution for the given scenario.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is B according to SPOTO products.

Arad 2 years, 4 months ago

Shouldn't it be B? The question doesn't talk about using Route53 as resolver, instead it needs to log all DNS queries made by Workspace Desktops. Maybe these Desktops are using a DNS resolver other than Route53 one. So it doesn't make more sense to configure a CloudWatch agent on desktops to gather DNS queries and send them to CloudWatch?

Adzz 2 years, 3 months ago

Just like route 53 is not mentioned, it is nowhere mentioned that Workspace is using any custom DNS server. So it is good to assume the AmazonProvidedDNS.

unclehou 2 years, 6 months ago

Selected Answer: A

A is the correct answer. it says the most cost effective. S3 would be the most cost effective. While option D might work, it's not the most cost-effective or straightforward solution for capturing DNS query logs generated by Amazon Workspaces in multiple VPCs across different AWS Regions.

Becklang 2 years, 5 months ago

you can't configure the vpc log only to log DNS querying , it would be a huge cost to enable logging for 7 vpcs while Kinesis Data Firehose First 500 TB / month $0.036 per GB

BasselBuzz 2 years ago

YES DNS traffic to Amazon DNS is not logged. but DNS traffic to other DNS servers is logged. according to the link provided by zendeveloper

zendevloper 2 years, 4 months ago

DNS traffic is not logged by flow logs https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#flow-logs-limitations

near22 1 year, 2 months ago

The answer is A. AWS workspaces not use route53 DNS directly but the MSAD or Simple AD as result the DNS query will be logged in VPC flow log

Certified101 2 years, 7 months ago

Selected Answer: B

Wouldn't option D log all Route53 query logs from all other servers? We need to only monitor Workspaces in the this scenario - would B be correct?

Certified101 2 years, 7 months ago

Changing to D as you can filter the resource after

掌学兔
ZHANGXUETU

[202610]

Question #156 Topic 1

A network engineer needs to design the architecture for a high performance computing (HPC) workload. Amazon EC2 instances will require 10 Gbps flows and an aggregate throughput of up to 100 Gbps across many instances with low-latency communication.

Which architecture solution will optimize this workload?

A. Place nodes in a single subnet of a VPC. Configure a cluster placement group. Ensure that the latest Elastic Fabric Adapter (EFA) drivers are installed on the EC2 instances with a supported operating system. **Most Voted**

B. Place nodes in multiple subnets in a single VPC. Configure a spread placement group. Ensure that the EC2 instances support Elastic Network Adapters (ENAs) and that the drivers are updated on each instance operating system.

C. Place nodes in multiple VPCs Use AWS Transit Gateway to route traffic between the VPCs. Ensure that the latest Elastic Fabric Adapter (EFA) drivers are installed on the EC2 instances with a supported operating system.

D. Place nodes in multiple subnets in multiple Availability Zones. Configure a cluster placement group. Ensure that the EC2 instances support Elastic Network Adapters (ENAs) and that the drivers are updated on each instance operating system.

Correct Answer: A

Community vote distribution

A (100%)

Comments

Manh Highly Voted 2 years, 1 month ago

Selected Answer: A

Option A is the most suitable solution for the high-performance computing workload: Cluster Placement Group: A cluster placement group ensures that EC2 instances are placed close together within the same Availability Zone to minimize network latency and provide high-bandwidth, low-latency communication between instances. This is crucial for an HPC workload where low-latency communication is essential. Single Subnet of a VPC: Placing nodes in a single subnet of a VPC ensures that the EC2 instances are closely located within the same subnet, further reducing network latency. Elastic Fabric Adapter (EFA): EFA is a network interface designed specifically for HPC workloads that require low-latency and high-bandwidth communication. Using EFA drivers on EC2 instances ensures optimal performance for communication between instances.

Hoversteng 1 year, 8 months ago

Selected Answer: A

A is correct

Certified101 2 years, 1 month ago

Selected Answer: A

A indeed correct

ISSDoksim 2 years, 1 month ago

A https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-limitations-spread

https://zhangxuetu.online

[202610]

Question #157 Topic 1

A company uses multiple AWS accounts and VPCs in a single AWS Region. The company must log all network traffic for Amazon EC2 instances and Amazon RDS databases. The company will use the log information to monitor and identify traffic flows in the event of a security incident. The information must be retained for 12 months but will be accessed infrequently after the first 90 days. The company must be able to view metadata that includes the vpc-id, subnet-id: and tcp-flags fields.

Which solution will meet these requirements at the LOWEST cost?

A. Configure VPC flow logs with the default fields Store the logs in Amazon CloudWatch Logs.

B. Configure Traffic Mirroring on all AWS resources to point to a Network Load Balancer that will send the mirrored traffic to monitoring instances.

C. Configure VPC flow logs with additional custom format fields Store the logs in Amazon S3. **Most Voted**

D. Configure VPC flow logs with additional custom format fields Store the logs in Amazon CloudWatch Logs.

Correct Answer: C

Community vote distribution



Comments

Certified101 **Highly Voted** 1 year, 7 months ago

Selected Answer: C

The other options are less cost-effective: Option A does not allow you to capture the custom fields you need (vpc-id, subnet-id, and tcp-flags). Option B, Traffic Mirroring, would involve a considerable overhead in terms of infrastructure and cost. Traffic Mirroring copies all traffic (not just metadata), which can be massive, and it requires additional resources to capture and process that traffic. Option D is less cost-effective for long-term, infrequently accessed storage because Amazon CloudWatch Logs is more expensive than Amazon S3 for these use cases.

AzureDP900 1 year, 2 months ago

Option C is actually the most cost-effective solution. By configuring VPC flow logs with additional custom format fields, the logs will be stored in Amazon S3, which has a lower storage cost compared to Amazon CloudWatch Logs. This option also allows for more flexibility and control over the log data, as well as the ability to easily access and filter the logs using AWS CLI or SDKs.

woorkim 1 year, 3 months ago

Selected Answer: C

S3 is more cost effective!

ISSDoksim 1 year, 8 months ago

C. https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#flow-logs-custom

https://zhangxuetu.online

[202610]

Question #158 Topic 1

A network engineer is evaluating a network setup for a global retail company. The company has an AWS Direct Connect connection between its on-premises data center and the AWS Cloud. The company has AWS resources in the eu-west-2 Region. These resources consist of multiple VPCs that are attached to a transit gateway.

The company recently provisioned a few AWS resources in the eu-central-1. Region in a single VPC close to its users in this area. The network engineer must connect the resources in eu-central-1 with the on-premises data center and the resources in eu-west-2. The solution must minimize changes to the Direct Connect connection.

What should the network engineer do to meet these requirements?

A. Create a new virtual private gateway. Attach the new virtual private gateway to the VPC in eu-central-1. Use a transit VIF to connect the VPC and the Direct Connect router.

B. Create a new transit gateway in eu-central-1. Create a peering attachment request to the transit gateway in eu-west-2. Add a static route in the transit gateway route table in eu-central-1 to point to the transit gateway peering attachment. Accept the peering request. Add a static route in the transit gateway route table in eu-west-2 to point to the new transit gateway peering attachment. Most Voted

C. Create a new transit gateway in eu-central-1. Use an AWS Site-to-Site VPN connection to peer both transit gateways. Add a static route in the transit gateway route table in eu-central-1 to point to the transit gateway VPN attachment. Add a static route in the transit gateway route table in eu-west-2 to point to the new transit gateway peering attachment.

D. Create a new virtual private gateway. Attach the new virtual private gateway to the VPC in eu-central-1. Use a public VIF to connect the VPC and the Direct Connect router.

Correct Answer: B

Community vote distribution

B (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: B

This option allows for the minimum number of changes to the existing Direct Connect connection while still providing connectivity between the resources in eu-central-1 and eu-west-2.

woorkim 1 year, 3 months ago

Selected Answer: B

The best solution is B. Reasoning: Meets requirement of minimizing changes to Direct Connect Leverages existing transit gateway infrastructure Provides direct connectivity between regions Uses transit gateway peering for efficient routing Minimal additional configuration Maintains network segmentation and security Scales well with future expansion

WherecanIstart 2 years ago

Selected Answer: B

B is the right answer. VPCs in different regions can't attach to the same Transit Gateway. You need to create a Transit Gateway in each region and peer the TGWs.

michele_scar 2 years ago

Selected Answer: B

A, C, D wrong definitions

Certified101 2 years, 7 months ago

Selected Answer: B

B seems correct

ISSDoksim 2 years, 7 months ago

B - https://aws.amazon.com/blogs/networking-and-content-delivery/building-a-global-network-using-aws-transit-gateway-inter-region-peering/

https://zhangxuetu.online

[202610]

Question #159 Topic 1

A company has a 2 Gbps AWS Direct Connect hosted connection from the company's office to a VPC in the ap-southeast-2 Region. A network engineer adds a 5 Gbps Direct Connect hosted connection from a different Direct Connect location in the same Region. The hosted connections are connected to different routers from the office with an iBGP session running in between the routers.

The network engineer wants to ensure that the VPC uses the 5 Gbps hosted connection to route traffic to the office. Failover to the 2 Gbps hosted connection must occur when the 5 Gbps hosted connection is down.

Which solution will meet these requirements?

A. Configure an outbound BGP policy from the router that is connected to the 2 Gbps connection. Advertise routes with a longer AS_PATH attribute to AWS. **Most Voted**

B. Advertise a longer prefix route from the router that is connected to the 2 Gbps connection.

C. Advertise a less specific route from the router that is connected to the 5 Gbps connection.

D. Configure an outbound BGP policy from the router that is connected to the 5 Gbps connection. Advertise routes with a longer AS_PATH attribute to AWS.

Correct Answer: A

Community vote distribution

A (100%)

Comments

Manh **Highly Voted** 2 years, 8 months ago

Selected Answer: A

BGP prefers routes with a shorter AS_PATH over routes with a longer AS_PATH. By advertising routes with a longer AS_PATH attribute from the 2 Gbps connection, you can make those routes less preferable than the routes advertised from the 5 Gbps connection. This way, the VPC will use the 5 Gbps connection to route traffic to the office, as long as it is available. If the 5 Gbps connection goes down, BGP will fail over to the 2 Gbps connection.

ISSDoksim **Highly Voted** 2 years, 7 months ago

A - agreed, shorter AS_PATH is preferred

AzureDP900 1 year, 2 months ago

Selected Answer: A

This option ensures that the VPC uses the 5 Gbps hosted connection to route traffic to the office, while also allowing failover to the 2 Gbps hosted connection when the 5 Gbps hosted connection is down.

woorkim 1 year, 3 months ago

Selected Answer: A

bgp prefer shortest AS-PATH, lowest MED for inbound TE, higher LP, Weight for outbound TE.

Newbies 1 year, 12 months ago

A -This configures the wrong router and doesn't leverage BGP policy effectively.

Vogd 2 years, 2 months ago

Selected Answer: A

Option B is wrong, since advertises the longest prefix to least preferred route. check
https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

https://zhangxuetu.online

[202610]

Question #160 Topic 1

An ecommerce company needs to implement additional security controls on all its domain names that are hosted in Amazon Route 53. The company's new policy requires data authentication and data integrity verification for all queries to the company's domain names. The current Route 53 architecture has four public hosted zones.

A network engineer needs to implement DNS Security Extensions (DNSSEC) signing and validation on the hosted zones. The solution must include an alert capability.

Which combination of steps will meet these requirements? (Choose three.)

A. Enable DNSSEC signing for Route 53 Request that Route 53 create a key-signing key (KSK) based on a customer managed key in AWS Key Management Service (AWS KMS). Most Voted

B. Enable DNSSEC signing for Route 53 Request that Route 53 create a zone-signing key (ZSK) based on a customer managed key in AWS Key Management Service (AWS KMS).

C. Create a chain of trust for the hosted zones by adding a Delegation Signer (DS) record for each subdomain

D. Create a chain of trust for the hosted zones by adding a Delegation Signer (DS) record to the parent zone. Most Voted

E. Set up an Amazon CloudWatch alarm that provides an alert whenever a DNSSECInternalFailure error or DNSSECKeySigningKeysNeedingAction error is detected. Most Voted

F. Set up an AWS CloudTrail alarm that provides an alert whenever a DNSSECInternalFailure error or DNSSECKeySigningKeysNeedingAction error is detected.

Correct Answer: ADE

Community vote distribution

ADE (100%)

Comments

woorkim 1 year, 3 months ago

Selected Answer: ADE

B. Issue: Route 53 manages the ZSK automatically. The user only needs to manage the KSK (key-signing key). There is no need to explicitly request a ZSK. C. DNSSEC works at the zone level. A DS record is added to the parent zone,

not for each subdomain, to create the chain of trust. F: CloudTrail logs API calls but does not natively monitor DNSSEC-related errors. CloudWatch is the correct service for monitoring DNSSEC issues.

Certified101 1 year, 7 months ago

Selected Answer: ADE

Option B: While it is true that DNSSEC uses zone-signing keys (ZSKs) in addition to KSKs, AWS Key Management Service (KMS) is not involved in creating ZSKs for DNSSEC in Route 53. Option C: Delegation Signer (DS) records are used to establish a chain of trust from a parent zone to a child zone, not between subdomains within a zone.

Neo00 1 year, 8 months ago

Selected Answer: ADE

ADE https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-configuring-dnssec-ksk.html

https://zhangxuetu.online

[202610]

Question #161 Topic 1

A financial company that is located in the us-east-1 Region needs to establish secure connectivity to AWS. The company has two on-premises data centers, each located within the same Region. The company's network team needs to establish hybrid connectivity to its AWS environment with reliable and consistent connectivity.

The connection must provide access to the company's private resources inside its AWS environment. The resources are located in the us-east-1 and us-west-2 Regions. The connection must allow resources from the corporate networks to send large amounts of data to Amazon S3 over the same connection. To meet compliance requirements, the connection must be highly available and must provide encryption for all packets that are sent between the on-premises location and any services on AWS.

Which combination of steps should the network team take to meet these requirements? (Choose two.)

A. Set up a private VIF to send data to Amazon S3. Use an AWS Site-to-Site VPN connection over the private VIF to encrypt data in transit to the VPCs in us-east-1 and us-west-2.

B. Set up an AWS Direct Connect connection to each of the company's data centers. Most Voted

C. Set up an AWS Direct Connect connection from one of the company's data centers to us-east-1 and us-west-2.

D. Set up a public VIF to send data to Amazon S3. Use an AWS Site-to-Site VPN connection over the public VIF to encrypt data in transit to the VPCs in us-east-1 and us-west-2. Most Voted

E. Set up a transit VIF for an AWS Direct Connect gateway to send data to Amazon S3. Create a transit gateway. Associate the transit gateway with the Direct Connect gateway to provide secure communications from the company's data centers to the VPCs in us-east-1 and us-west-2.

Correct Answer: BD

Community vote distribution



Comments

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: BD

Option B: Establishing an AWS Direct Connect connection to each of the company's data centers ensures a reliable, consistent connection. This setup also addresses the requirement for high availability. If there are problems with one connection, the other connection can maintain the data flow. Option D: A public VIF can provide direct access to AWS services, including Amazon S3, across the Direct Connect link. By using an AWS Site-to-Site VPN connection over the

public VIF, you can encrypt data in transit between the on-premises location and the VPCs in us-east-1 and us-west-2, thereby meeting the company's compliance requirements.

1a17d1e 7 months, 1 week ago

Selected Answer: BE

To use the public VIF you'd have to configure AWS Site-to-Site VPN over a Transit Gateway. The Q doesn't mention a TG so option D is out.

hedglin 1 year, 9 months ago

Option B & E is correct. Why the other options are incorrect: A and D: These options suggest using Site-to-Site VPN over Direct Connect, which is not necessary when using a Transit Gateway and Direct Connect gateway. The Transit Gateway provides the required encryption. C: This option only sets up a Direct Connect connection from one data center, which doesn't meet the high availability requirement.

vikasj1in 2 years, 1 month ago

Selected Answer: BE

B: This ensures reliable, consistent, and highly available connectivity. E: The transit gateway provides a centralized hub for connectivity, simplifying network architecture and allowing the flow of data securely. A: is incorrect because using a private VIF and an AWS Site-to-Site VPN connection is not necessary when there is a dedicated AWS Direct Connect connection to each data center. C: is not optimal because it suggests a separate Direct Connect connection for each AWS Region, which can lead to additional complexity and cost. D: is not recommended because using a public VIF for sending data to Amazon S3 might involve traffic going over the public internet, potentially impacting security and compliance requirements.

sambb 2 years, 7 months ago

Selected Answer: BD

E - does not mention any type of encryption (no MACsec, no IPsec S2S VPN) A - S2S VPN is not available a private VIF as far as i know D - provides encryption and connection to S3 is possible with an interface endpoint. A single connection has 2 VPN tunnels, so we have redundancy, but it's not very highly available.

ISSDoksim 2 years, 7 months ago

BD - https://docs.aws.amazon.com/vpn/latest/s2svpn/Examples.html

johnconnor 2 years, 7 months ago

I agree with B, wouldn't both D and E work as well?

johnconnor 2 years, 7 months ago

My concern with D is the HA part

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #162 Topic 1

A global company is designing a hybrid architecture to privately access AWS resources in the us-west-2 Region. The company's existing architecture includes a VPC that uses RFC 1918 IP address space. The VPC is connected to an on-premises data center over AWS Direct Connect Amazon Route 53 provides name resolution within the VPC. Locally managed DNS servers in the data center provide DNS services to the on-premises hosts.

The company has applications in the data center that need to download objects from an Amazon S3 bucket in us-west-2.

Which solution can the company use to access Amazon S3 without using the public IP address space?

A. Create an S3 interface endpoint in the VPC. Update the on-premises application configuration to use the Regional VPC endpoint DNS hostname that is mapped to the S3 interface endpoint.

B. Create an S3 interface endpoint in the VPC. Configure a Route 53 Resolver inbound endpoint in the VPC. Set up the data center DNS servers to forward DNS queries for the S3 domain from on premises to the inbound endpoint. Most Voted

C. Create an S3 gateway endpoint in the VPUpdate the on-premises application configuration to use the hostname that is mapped to the S3 gateway endpoint.

D. Create an S3 gateway endpoint in the VPC. Configure a Route 53 Resolver inbound endpoint in the VPC. Set up the data center DNS servers to forward DNS queries for the S3 domain from on premises to the inbound endpoint.

Correct Answer: B

Community vote distribution



Comments

sanalainen Highly Voted 2 years, 4 months ago

Selected Answer: A

Actually both A and B would work. https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/ With B, you would need to set up PHZ as well.

sanalainen 2 years, 4 months ago

A = Option 1 B = Option 3 in https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/

luisgu 1 year, 6 months ago

For option 3 (B) you would need to create a PHZ --> correct answer is A

AikAWS 6 months, 2 weeks ago

Selected Answer: D

Why D Works Create an S3 gateway endpoint Traffic from the VPC (and routed via Direct Connect) goes to S3 over private IPs, never touching the public internet. Set up Route 53 Resolver inbound endpoint On-premises DNS servers forward queries for *.s3.amazonaws.com to the inbound endpoint. Applications resolve the private IP of S3 endpoint. On-premises traffic flows privately With Direct Connect and private DNS, S3 is accessed without using public IPs.

matanasov 10 months, 2 weeks ago

Selected Answer: D

S3 Gateway endpoint supports private IP space (RFC 1918) It works over Direct Connect It does not require public IPs or NAT Route 53 Resolver inbound endpoint allows on-prem DNS servers to resolve s3.amazonaws.com to private IPs Most cost-effective and AWS-recommended hybrid pattern

Spaurito 1 year, 4 months ago

A - the key to this configuration is "...to privately access AWS resources". This would remove option B as it is setting up for a public IP addressing use. This link shows using Public and Private IP Address configurations For the Private, it is using a VPC Interface Endpoint and doesn't require the inbound Resolver endpoint.

Sailor 1 year, 11 months ago

Selected Answer: B

When you configure an interface VPC endpoint, an elastic network interface (ENI) with a private IP address is deployed in your subnet. An Amazon EC2 instance in the VPC can communicate with an Amazon S3 bucket through the ENI and AWS network. Using the interface endpoint, applications in your on-premises data center can easily query S3 buckets over AWS Direct Connect or Site-to-Site VPN. Interface endpoint supports a growing list of AWS services. Consult our documentation to find AWS services compatible with interface endpoints powered by AWS PrivateLink. https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

Newbies 1 year, 12 months ago

Ans: A S3 Interface Endpoint: By creating an S3 interface endpoint within the VPC, the company can establish a private connection to S3 buckets without traversing the public internet. Route 53 Resolver (Implicit): VPC endpoint DNS names inherently resolve through Route 53 Resolver within the VPC. No explicit configuration for a separate Route 53 Resolver inbound endpoint is required. On-premises Application Update: Updating the application configuration to utilize the Regional VPC endpoint DNS hostname mapped to the S3 interface endpoint allows the application to connect to S3 through the private connection. B. Route 53 Resolver Inbound Endpoint (Unnecessary): While Route 53 Resolver can be used for DNS resolution within a VPC, in this case, the VPC endpoint DNS name itself resolves through Route 53 Resolver implicitly. Setting up an additional inbound endpoint is not required.

AzureDP900 1 year, 2 months ago

yes, A is right. • Option B: While creating an S3 interface endpoint is a good starting point, configuring a Route 53 Resolver inbound endpoint in the VPC isn't necessary. The on-premises DNS servers will still need to forward requests to the S3 interface endpoint.

psou7 2 years ago

D. S3 uses GW endpoint. So between B and D -> D

WherecanIstart 2 years ago

Selected Answer: B

Correct answer is B. The question says "..... without using the public IP address space? " Use a private IP address over Direct Connect (with an interface VPC endpoint)

BasselBuzz 2 years ago

Selected Answer: A

https://repost.aws/knowledge-center/s3-bucket-access-direct-connect No need to inbound resolver. it is enough with the interface DNS hostname

michele_scar 2 years, 1 month ago

Selected Answer: B

A it's not correct because if you configure your local DNS to forward s3 dns queries to S3 VPC Endpoints you will not reach the private vpc endpoints without tells to your dns server how to reach it

vikasj1in 2 years, 1 month ago

Selected Answer: B

This solution maintains the use of private IP address space and avoids the need for public IP addresses. It ensures that the on-premises applications can securely access Amazon S3 in the us-west-2 Region without relying on public internet connectivity. Options A and D are incorrect because they refer to S3 interface endpoints without involving Route 53 Resolver, which is necessary for DNS resolution. Option C mentions an S3 gateway endpoint, but S3 gateway endpoints are used for accessing S3 from on-premises environments, not for VPC-to-S3 communication.

ogrefighter 2 years ago

Agree answer is B. But the reason Gateway Endpoint is wrong is that can only be set up in routing table using the pl-xxxxxxxx prefix list route. Interface endpint uses more flexible privatelink/ENI and is the only one that works with on-premises.

Isaias 2 years, 1 month ago

Selected Answer: A

You dont need an inbound endpoint, it can be resolved on any public dns resolving to the private IP of the endpoint, that because the endpoint domain name is Public (*vpce.amazonaws.com)

mike5656 2 years, 3 months ago

The answer is A. You don't need to have an inbound endpoint in order to resolve the DNS. The endpoint DNS names can be resolved from anywhere but they will resolve to the private IPs. You can try to create an endpoint and resolve it from your PC ;)

sambb 2 years, 7 months ago

Selected Answer: B

B - https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/

ISSDoksim 2 years, 7 months ago

B - agreed, gateway endpoint is available within the VPC

Manh 2 years, 8 months ago

Selected Answer: B

https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html

KittensGutters 2 years, 8 months ago

Selected Answer: B

https://repost.aws/knowledge-center/s3-bucket-access-direct-connect

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #163 Topic 1

A company is migrating critical applications to AWS. The company has multiple accounts and VPCs that are connected by a transit gateway.

A network engineer must design a solution that performs deep packet inspection for any traffic that leaves a VPC network boundary. All inspected traffic and the actions that are taken on the traffic must be logged in a central log account.

Which solution will meet these requirements with the LEAST administrative overhead?

A. Create a central network VPC that includes an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the new attachment. Deploy an AWS Gateway Load Balancer that is backed by third-party, next-generation firewall appliances to the central network VPC. Create a policy that contains the rules for deep packet inspection. Attach the policy to the firewall appliances. Create an Amazon S3 bucket in the central log account. Configure the firewall appliances to capture and save the network flow logs to the S3 bucket. **Most Voted**

B. Create a central network VPC that includes an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the new attachment. Deploy an AWS Application Load Balancer that is backed by third-party, next-generation firewall appliances to the central network VPC. Create a policy that contains the rules for deep packet inspection. Attach the policy to the firewall appliances. Create a syslog server in the central log account. Configure the firewall appliances to capture and save the network flow logs to the syslog server.

C. Deploy network ACLs and security groups to each VPAttach the security groups to active network interfaces. Associate the network ACLs with VPC subnets. Create rules for the network ACLs and security groups to allow only the required traffic flows between subnets and network interfaces. Create an Amazon S3 bucket in the central log account. Configure a VPC flow log that captures and saves all traffic flows to the S3 bucket.

D. Create a central log VPC and an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the new attachment. Deploy an AWS Network Load Balancer (NLB) that is backed by third-party, next-generation intrusion detection system (IDS) security appliances to the central VPC. Activate rules on the security appliances to monitor for intrusion signatures. For each network interface, create a VPC Traffic Mirroring session that sends the traffic to the central VPC's NLB.

Correct Answer: A

Community vote distribution



Comments

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: A

A is correct as sambb said. GWLB is perfect for traffic inspection

trap 2 years, 6 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-gateway-load-balancer-supported-architecture-patterns/

Spaurito 1 year, 4 months ago

A - For high availability, we recommend that you use a Network Load Balancer or a Gateway Load Balancer endpoint as a mirror target. You might experience out-of-order delivery of mirrored packets when you use a Network Load Balancer or Gateway Load Balancer endpoint as your traffic mirror target. If your monitoring appliance can't handle out-of-order packets, we recommend using a network interface as your traffic mirror target.

Blitz1 1 year, 8 months ago

Selected Answer: A

It's A just because of D is saying: "For each network interface, create a VPC Traffic Mirroring session that sends the traffic to the central VPC's NLB. " Mirroring each interface in "multiple accounts and VPCs" is definitly NOT the " LEAST administrative overhead".

Blitz1 1 year, 8 months ago

Selected Answer: A

For sure A. It cannot be D because it is saying "All inspected traffic and the actions that are taken on the traffic must be logged in a central log account." Since we are talking about mirroring there is no ACTION that can be taken on the traffic since is not INLINE but a mirror.

Newbies 1 year, 12 months ago

A & B GLB/ALB with FW: These options require additional configuration and policy mgmt for the FW in the central VPC, complex and time-consuming to maintain across multiple VPCs. Answer is D - no changes req on TGW config

Vogd 2 years, 2 months ago

Selected Answer: A

I do not see any word "mirroring" in the question. If you route traffic through GWLB you dont need mirroring at all. Also D offers to store Logs in different VPC than Central where Firewall is deployed. It does not make sense and incur additional complication.

nuzz 2 years, 2 months ago

Selected Answer: A

A is the correct answer. do not get confused between mirroring and inspection

Becklang 2 years, 5 months ago

Selected Answer: D

NFGW is also a router, it drops packets when there is no route entry on its routing table, IDS will accept the packets arriving at its interface no matter what the src/dst is.

Cheam 2 years, 5 months ago

Selected Answer: D

Again, people still get it wrong as to what is a valid mirror target. GWLB Endpoint is a valid mirror target, but not the GWLB itself. Ref: https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html Also, the question provides a good hint on which is the appropriate answer, "All inspected traffic... must be logged in a central log account". All the best.

aws_god 2 years, 4 months ago

Nowhere in the question is a mirror target mentioned

zendevloper 2 years, 4 months ago

It's A. D does not mention where the traffic is logged

sambb 2 years, 7 months ago

Selected Answer: A

D asks for creating a mirroring session for each ENI, this is operationally inefficient. A provides a solution that monitors all IP traffic that reaches the transit gateway.

Becklang 2 years, 5 months ago

No need for create mirroring session for each ENI , just create it on TGW ENI in each VPC

ISSDoksim 2 years, 7 months ago

D - https://aws.amazon.com/blogs/networking-and-content-delivery/using-vpc-traffic-mirroring-to-monitor-and-secure-your-aws-infrastructure/

johnconnor 2 years, 7 months ago

Agreed, deep traffic inspection and mirroring go like jelly and peanut butter

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #164 Topic 1

A company has an on-premises data center in the United States. The data center is connected to AWS by an AWS Direct Connect connection. The data center has a private VIF that is connected to a Direct Connect gateway.

Recently, the company opened a new data center in Europe and established a new Direct Connect connection between the Europe data center and AWS. A new private VIF connects to the existing Direct Connect gateway.

The company wants to use Direct Connect SiteLink to set up a private network between the data center in the United States and the data center in Europe.

Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create a new public VIF from each data center. Enable SiteLink on the new public VIFs.

B. Create a new transit VIF from each data center. Enable SiteLink on the new transit VIFs.

C. Use the existing VIF from each data center. Enable SiteLink on the existing private VIFs. **Most Voted**

D. Create a new AWS Site-to-Site VPN connection between the data centers. Configure the new connection to use SiteLink.

Correct Answer: C

Community vote distribution

C (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: C

Option C (existing private VIFs) can be a more operationally efficient solution for setting up a SiteLink between the two data centers.

woorkim 1 year, 3 months ago

Selected Answer: C

You make this change on an existing or a new Transit or Private virtual interface (VIF) (regular or hosted VIF) attached to a DXGW. The requirements for creating and configuring a SiteLink-enabled VIF are the same as a regular DX Private or Transit VIF.

vikasj1in 2 years, 1 month ago

Selected Answer: C

Direct Connect SiteLink is a feature that allows you to establish private virtual interfaces (VIFs) between Direct Connect gateways in different geographic locations. It enables you to create a private network connection between your on-premises data centers connected via Direct Connect. In this scenario, the company already has private VIFs connecting its on-premises data centers (in the United States and Europe) to the existing Direct Connect gateway. To set up a private network between these data centers using Direct Connect SiteLink, you can enable SiteLink on the existing private VIFs. This is operationally efficient, as it utilizes the existing connections and configurations.

Marfee400704 2 years, 1 month ago

I think that it's correct answer is B.

Certified101 2 years, 7 months ago

Selected Answer: C

C is correct

Certified101 2 years, 7 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-direct-connect-sitelink/

johnconnor 2 years, 7 months ago

It is C "If you are using Direct Connect now, either through a direct or hosted connection, you have everything you need to use SiteLink. No new connections are required. "

ISSDoksim 2 years, 7 months ago

C - https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-direct-connect-sitelink/

https://zhangxuetu.online

[202610]

Question #165 Topic 1

A company has a new AWS Direct Connect connection between its on-premises data center and the AWS Cloud. The company has created a new private VIF on this connection. However, the VIF status is DOWN.

A network engineer verifies that the physical connection status is UP and RUNNING based on information from the AWS Management Console. The network engineer checks the customer Direct Connect router and can see the ARP entry for the VLAN interface created for the private VIF at AWS.

What could be causing the private VIF to have a DOWN status?

A. ICMP is blocked on the customer Direct Connect router.

B. TCP port 179 is blocked on the customer Direct Connect router. Most Voted

C. The IEEE 802.1Q VLAN identifier is misconfigured on the customer Direct Connect router.

D. The company has configured IEEE 802.1ad instead of 802.1Q on the customer Direct Connect router.

Correct Answer: B

Community vote distribution

B (61%) C (39%)

Comments

ISSDoksim Highly Voted 2 years, 8 months ago

C - https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html#ts-layer-2

KidPags 1 year, 4 months ago

That doc says as part of troubleshooting to "Verify if the router has a MAC address entry from the AWS endpoint in your address resolution protocol (ARP) table." In this Q the ARP entry exists, so the q-tag must be configured correctly.

AzureDP900 1 year, 2 months ago

C is correct here's why: Down Status : The private VIF has a DOWN status, which indicates that there is an issue with the communication between the two ends of the AWS Direct Connect connection. Physical Connection Status : The physical connection status is UP and RUNNING based on information from the AWS Management Console. This means that there is no problem with the physical link itself. ARP Entry : The network engineer can see the ARP entry for the VLAN interface created for the private VIF at AWS, which indicates that the IP address mapping is correct. Given these facts, we can rule out options A and B because ICMP (Internet Control Message Protocol) and TCP port 179 are not directly related to the IEEE 802.1Q VLAN identifier or the communication between the two ends of the AWS Direct Connect connection.

Certified101 Highly Voted 2 years, 7 months ago

Selected Answer: B

Changed to B as the entry is visible for the VLAN interface created for the private VIF at AWS, which means that the Layer 2 connectivity appears to be functioning correctly. BGP is the issue

woorkim 1 year, 3 months ago

Selected Answer: B

Your virtual interface on Direct Connect can go down for multiple reasons: Physical connection is down or flapping OSI layer 2 configuration issues Border Gateway Protocol (BGP) configuration issues Bidirectional Forwarding Detection (BFD) configuration issues https://repost.aws/knowledge-center/direct-connect-down-virtual-interface

APTAPT 1 year, 4 months ago

Selected Answer: C

The ARP entry is for private VIF's VLAN interface at AWS, not is for on-premise router. Therefore, the connection at layer 2 cannot be considered normal. Option C is a layer2 problem.

APTAPT 1 year, 4 months ago

The ARP entry is for private VIF's VLAN interface at AWS, not is for on-premise router. Therefore, the connection at layer 2 cannot be considered normal. Option C is a layer2 problem.

APTAPT 1 year, 4 months ago

Selected Answer: C

The ARP entry is for private VIF's VLAN interface at AWS, not is for on-premise router. Therefore, the connection at layer 2 cannot be considered normal.

erima21 1 year, 5 months ago

Selected Answer: C

However, even if BGP is blocked or misconfigured, this would not cause the VIF status to be "DOWN." The VIF status depends on layer 2 (Ethernet) connectivity, not layer 3. Even if the BGP session is not working, the VIF should be "UP" at layer 2 if the Ethernet frames are being transmitted and tagged correctly.

Spaurito 1 year, 4 months ago

If Layer 2 is fine...just walk up the OSI Model...layer 3 is next. Option B

Newbies 1 year, 12 months ago

ISSDoksim is correct. Ans C, DXCON uses VLAN tagging (IEEE 802.1Q) to separate customer traffic on the shared physical connection

tromyunpak 1 year, 12 months ago

Answer is B - since the VIF uses BGP A is not relevant CD are wrong due to the fact the ARP entry is visible

psou7 2 years ago

Answer C

vikasj1in 2 years, 1 month ago

Selected Answer: C

The most likely reason for a private VIF (Virtual Interface) to have a DOWN status is a misconfiguration of the VLAN identifier. When setting up a private VIF, you need to configure the correct IEEE 802.1Q VLAN identifier on both ends, matching the VLAN ID associated with the VIF. If there's a mismatch in VLAN configuration, it can lead to the VIF being down. Option A and Option B are less likely to cause the private VIF to be DOWN. ICMP and TCP port 179 are related to specific networking protocols (ping and BGP, respectively), but the DOWN status is more likely associated

with VLAN configuration issues. Option D refers to IEEE 802.1ad (Provider Bridging or Q-in-Q), which is not typically used for AWS Direct Connect connections. Misconfiguration of the VLAN identifier (802.1Q) is a more common issue leading to a DOWN status.

WherecanIstart 2 years, 1 month ago

Seeing the arp entries on the vlan interface points to the fact that 802.1q is configured correctly.

Becklang 2 years, 5 months ago

Selected Answer: B

As the arp entry can be seen on the customer side which means the dot1.q is correctly configured , so C is wrong

unclehou 2 years, 6 months ago

C is correct. TCP port 179 is associated with the Border Gateway Protocol (BGP), which is used for routing updates between the customer's router and the AWS Direct Connect router. Blocking port 179 would prevent BGP from establishing a connection, but it would usually result in a BGP DOWN status, not necessarily a DOWN status for the entire private VIF.

Certified101 2 years, 7 months ago

Selected Answer: C

If it was B it would show BGP as DOWN not VIF - this is a layer 2 issue Given the ARP entry visibility and physical connection's UP state, it indicates that the Layer 2 configuration (VLAN) might be correct on the Direct Connect router. However, if the VIF status is still showing as DOWN, it can be related to incorrect 802.1Q VLAN configuration, which might have been performed correctly on the customer end, but misconfigured on the AWS side or vice versa. So, the correct answer would be: C. The IEEE 802.1Q VLAN identifier is misconfigured on the customer Direct Connect router.

Manh 2 years, 8 months ago

Selected Answer: B

https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html#ts-layer-2 Ensure that there are no firewall or ACL rules that are blocking TCP port 179 or any high-numbered ephemeral TCP ports. These ports are necessary for BGP to establish a TCP connection between the peers.

https://zhangxuetu.online

[202610]

Question #166 Topic 1

AnyCompany has acquired Example Corp. AnyCompany's infrastructure is all on premises, and Example Corp's infrastructure is completely in the AWS Cloud. The companies are using AWS Direct Connect with AWS Transit Gateway to establish connectivity between each other.

Example Corp has deployed a new application across two Availability Zones in a VPC with no internet gateway. The CIDR range for the VPC is 10.0.0.0/16. Example Corp needs to access an application that is deployed on premises by AnyCompany. Because of compliance requirements, Example Corp must access the application through a limited contiguous block of approved IP addresses (10.1.0.0/24).

A network engineer needs to implement a highly available solution to achieve this goal. The network engineer starts by updating the VPC to add a new CIDR range of 10.1.0.0/24.

What should the network engineer do next to meet the requirements?

A. In each Availability Zone in the VPC, create a subnet that uses part of the allowed IP address range. Create a public NAT gateway in each of the new subnets. Update the route tables that are associated with other subnets to route application traffic to the public NAT gateway in the corresponding Availability Zone. Add a route to the route table that is associated with the subnets of the public NAT gateways to send traffic destined for the application to the transit gateway.

B. In each Availability Zone in the VPC, create a subnet that uses part of the allowed IP address range. Create a private NAT gateway in each of the new subnets. Update the route tables that are associated with other subnets to route application traffic to the private NAT gateway in the corresponding Availability Zone. Add a route to the route table that is associated with the subnets of the private NAT gateways to send traffic destined for the application to the transit gateway. Most Voted

C. In the VPC, create a subnet that uses the allowed IP address range. Create a private NAT gateway in the new subnet. Update the route tables that are associated with other subnets to route application traffic to the private NAT gateway. Add a route to the route table that is associated with the subnet of the private NAT gateway to send traffic destined for the application to the transit gateway.

D. In the VPC, create a subnet that uses the allowed IP address range. Create a public NAT gateway in the new subnet. Update the route tables that are associated with other subnets to route application traffic to the public NAT gateway. Add a route to the route table that is associated with the subnet of the public NAT gateway to send traffic destined for the application to the transit gateway.

Correct Answer: B

Community vote distribution



Comments

matanasov 10 months, 2 weeks ago

Selected Answer: B

Subnets should be in each AZ No IGW = Private NAT

AzureDP900 1 year, 2 months ago

Selected Answer: B

By using private NAT gateways, you can allow Example Corp's traffic to access the on-premises application through the limited contiguous block of approved IP addresses (10.1.0.0/24) while still maintaining the security and isolation of the AWS Direct Connect connection.

woorkim 1 year, 3 months ago

Selected Answer: B

Private NAT to solve IP exhaustion problem and enable communication between two Amazon Virtual Private Clouds (VPCs) with overlapping CIDR ranges.

tyh391 1 year, 11 months ago

B. needs to implement a highly available solution

Certified101 2 years, 7 months ago

Selected Answer: B

Also the VPC uses the subnet 10.1.0.0/24 already. You cannot create a single subnet in that VPC range. Needs to be split up into multiple subnets. "The network engineer starts by updating the VPC to add a new CIDR range of 10.1.0.0/24"

Certified101 2 years, 7 months ago

Selected Answer: B

B is correct - Needs to be highly available so multiple AZ's required one in each of the 2 AZ's "Example Corp has deployed a new application across two Availability Zones in a VPC with no internet gateway"

sambb 2 years, 7 months ago

Selected Answer: B

A and D - public NAT gateway has nothing to do here. B provides an multi-az solution, compared to C

ISSDoksim 2 years, 7 months ago

https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-solve-private-ip-exhaustion-with-private-nat-solution/

payelix795 2 years, 7 months ago

I've been going through the docs for info.I take it it works like a regular NAT gateway where I would need one per AZ for HA ? Is B a possible option ?

Manh 2 years, 8 months ago

Selected Answer: C

Create 3 NATs in each subnet is crazy. therefore, the choice is C. The network engineer should create a private NAT gateway in the VPC and update the route tables that are associated with other subnets to route application traffic to

the private NAT gateway. This will allow Example Corp to access the application on premises through the allowed IP address range, while also maintaining compliance requirements.

johnconnor 2 years, 7 months ago

It would be a lot easier to manage, but isn't the limitation of "A subnet must reside within a single Availability Zone." an issue for C?

https://zhangxuetu.online

[202610]

Question #167 Topic 1

A company recently experienced an IP address exhaustion event in its VPCs. The event affected service capacity. The VPCs hold two or more subnets in different Availability Zones.

A network engineer needs to develop a solution that monitors IP address usage across resources in the VPCs. The company needs to receive notification about possible issues so that the company can act before an incident happens.

Which solution will meet these requirements with the LEAST operational overhead?

A. Set up Amazon VPC IP Address Manager (IPAM) with a new top-level pool. In the top-level pool, create a pool for each VPC. In each VPC pool, create a pool for each subnet in that VPC. Turn on the auto-import option for the VPC pools and the subnet pools. Configure an Amazon CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold is reached. **Most Voted**

B. Set up a log group in Amazon CloudWatch Logs for each subnet. Create an AWS Lambda function that reads each subnet's IP address usage and publishes metrics to the log group. Configure an Amazon CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold is reached.

C. Set up a custom Amazon CloudWatch metric for IP address usage for each subnet. Create an AWS Lambda function that reads each subnet's IP address usage and publishes a CloudWatch metric dimension. Schedule the Lambda function to run every 5 minutes. Configure a CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold is reached.

D. Set up Amazon VPC IP Address Manager (IPAM) with a new top-level pool. In the top-level pool, create a pool for each VPC. In each VPC pool, create a pool for each subnet in that VPC. Turn on the auto-import option for the VPC pools and the subnet pools. Configure an Amazon EventBridge rule that monitors each pool availability limit threshold and sends an Amazon Simple Notification Service (Amazon SNS) notification if the limit threshold is reached.

Correct Answer: A

Community vote distribution

A (100%)

Comments

Certified101 Highly Voted 2 years, 1 month ago

Selected Answer: A

A is correct - no need for eventbridge as it integrates with cloudwatch already

AzureDP900 1 year, 2 months ago

Selected Answer: A

Option A is indeed the correct answer because it utilizes Amazon VPC IP Address Manager (IPAM), which provides automatic monitoring and alerts for IP address usage across resources in the VPCs. By setting up a new top-level pool with auto-import option enabled, you can monitor IP address availability limits for each subnet without having to write custom code or manage additional infrastructure.

GaryQian 1 year, 7 months ago

Selected Answer: A

Yes it must be A

Marfee400704 1 year, 7 months ago

I think that it's correct answer is C.

ISSDoksim 2 years, 1 month ago

A https://docs.aws.amazon.com/vpc/latest/ipam/cloudwatch-ipam.html

https://zhangxuetu.online

[202610]

Question #168 Topic 1

A company has a hybrid IT setup that includes services that run in an on-premises data center and in the AWS Cloud. The company is using AWS Direct Connect to connect its data center to AWS. The company is using one AWS Site-to-Site VPN connection as backup and requires a backup connectivity option to always be present. The company is transitioning to IPv6 by implementing dual-stack architectures.

Which combination of steps will transition the data center's connectivity to AWS in the LEAST amount of time? (Choose two.)

A. Create a new Site-to-Site VPN tunnel for the IPv6 traffic. Most Voted

B. Create a new dual-stack Site-to-Site VPN connection between the data center and AWS. Provision routing. Delete the original Site-to-Site VPN connection.

C. Associate a new dual-stack public VIF with the Direct Connect connection. Migrate the Direct Connect traffic to the new VIF.

D. Add a new IPv6 peer in the existing VIF. Use the IPv6 address provided by Amazon on the peer router. Most Voted

E. Send IPv6 traffic between the data center and AWS in a tunnel inside the existing IPv4 tunnels.

Correct Answer: AD

Community vote distribution



Comments

tromyunpak Highly Voted 1 year, 12 months ago

AD are correct since a new vpn is needed and a new IPv6 peer can be added to the existing vif BE are wrong - since you cannot add iPv6 to an existing s2s and a s2s cannot be dual stack (https://docs.aws.amazon.com/vpn/latest/s2svpn/ipv4-ipv6.html) C is good but not fulfil the least amount of time requirement

Rollizo 1 year, 1 month ago

Selected Answer: AD

The following rules apply: IPv6 addresses are only supported for the inside IP addresses of the VPN tunnels. The outside tunnel IP addresses for the AWS endpoints are IPv4 addresses, and the public IP address of your customer gateway must be an IPv4 address. Site-to-Site VPN connections on a virtual private gateway do not support IPv6. You cannot enable IPv6 support for an existing Site-to-Site VPN connection. A Site-to-Site VPN connection cannot support both IPv4 and IPv6 traffic. Cannot be B

secdaddy 1 year, 1 month ago

Selected Answer: BD

Not sure why people are saying A as A has only ipv6 and the requirement is for dual-stack. Need B for new dual-stack VPN + D for adding ipv6 to the existing DX vif.

AzureDP900 1 year, 2 months ago

Selected Answer: AD

• Option A: Creating a new Site-to-Site VPN tunnel for IPv6 traffic allows you to gradually transition your connectivity to AWS while still using the existing Direct Connect connection. • Option D: Adding an IPv6 peer to the existing VIF enables you to start sending IPv6 traffic over the existing connection, allowing you to test your dual-stack architecture without disrupting the existing connectivity.

woorkim 1 year, 3 months ago

Selected Answer: AD

cannot enable IPv6 support for an existing Site-to-Site VPN connection.

cas_tori 1 year, 7 months ago

Selected Answer: AD

A and D

cerifyme85 1 year, 11 months ago

Selected Answer: AD

A D is correct.

JoellaLi 1 year, 12 months ago

Selected Answer: AD

A D is correct. Agree with tromyunpak.

Kayceetalks 2 years ago

B and C

jinu 2 years ago

A and E

https://zhangxuetu.online

[202610]

Question #169 Topic 1

A company is developing a new application that is deployed in multiple VPCs across multiple AWS Regions. The VPCs are connected through AWS Transit Gateway. The VPCs contain private subnets and public subnets.

All outbound internet traffic in the private subnets must be audited and logged. The company's network engineer plans to use AWS Network Firewall and must ensure that all traffic through Network Firewall is completely logged for auditing and alerting.

How should the network engineer configure Network Firewall logging to meet these requirements?

A. Configure Network Firewall logging in Amazon CloudWatch to capture all alerts. Send the logs to a log group in Amazon CloudWatch Logs.

B. Configure Network Firewall logging in Network Firewall to capture all alerts and flow logs. **Most Voted**

C. Configure Network Firewall logging by configuring VPC Flow Logs for the firewall endpoint. Send the logs to a log group in Amazon CloudWatch Logs.

D. Configure Network Firewall logging by configuring AWS CloudTrail to capture data events.

Correct Answer: B

Community vote distribution



Comments

bluz **Highly Voted** 2 years ago

Selected Answer: B

"to capture all alerts and flow logs"

jinu **Highly Voted** 2 years ago

A- https://docs.aws.amazon.com/network-firewall/latest/developerguide/logging-cw-logs.html

secdaddy 1 year, 1 month ago

A actions alerts but does not meet the flow logs requirement. B does both.

qomtodie 1 year, 7 months ago

Selected Answer: A Only 3 systems can have AWS Network Firewall Log. Amazon Simple Storage Service, Amazon CloudWatch Logs, Amazon Data Firehose.

Spaurito 1 year, 4 months ago

Option A is saying configure in CloudWatch. You have to configure on the Network Firewall which would suggest Option B. If it said "Configure Network Firewall logging to Amazon CloudWatch..." it may be more accurate.

kupo777 1 year, 7 months ago

Selected Answer: B A: Since only all alerts are captured, the requirement to capture all traffic logs cannot be met. B: The Network Firewall log settings are configured for logging from the Network Firewall's Firewall Details screen. When configuring the logging settings, select either the alert log or the traffic log, or both, and configure the output settings. C: The requirement is not met because alerts cannot be captured. D: Network Firewall alerts and traffic logs cannot be captured by CloudTrail.

KobDragoon 1 year, 11 months ago

Selected Answer: B

B - is the only Answer that correctly mentions both alert logs and flowlogs which are 2 different log types the network firewall can be configured to log. A - seems like a good answer as it mentions sending the logs to a cloudwatch log group, but where the logs are sent is not part of the question and so as A only mentions alert logs, it's incorrect.

JoellaLi 1 year, 12 months ago

Selected Answer: D

AWS Network Firewall is integrated with AWS CloudTrail, a service that provides a record of API calls to Network Firewall by a user, role, or an AWS service. CloudTrail captures all API calls for Network Firewall as events. The calls captured include calls from the Network Firewall console and code calls to the Network Firewall API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Network Firewall. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine information including the request that was made to Network Firewall, the IP address from which the request was made, who made the request, and when the request was made.

Spaurito 1 year, 4 months ago

CloudTrail won't do this.

daemon101 1 year, 12 months ago

Selected Answer: A

logging destinations are s3, cloudwatch, or data firehose https://docs.aws.amazon.com/network-firewall/latest/developerguide/firewall-logging-destinations.html

JoellaLi 1 year, 12 months ago

D is correct

Spaurito 1 year, 4 months ago

CloudTrail won't do this.

https://zhangxuetu.online

[202610]

Question #170 Topic 1

A company has set up a NAT gateway in a single Availability Zone (AZ1) in a VPC (VPC1) to access the internet from Amazon EC2 workloads in the VPC. The EC2 workloads are running in private subnets in three Availability Zones (AZ1, AZ2, AZ3). The route table for each subnet is configured to use the NAT gateway to access the internet.

Recently during an outage, internet access stopped working for the EC2 workloads because of the NAT gateway's unavailability. A network engineer must implement a solution to remove the single point of failure from the architecture and provide built-in redundancy.

Which solution will meet these requirements?

A. Set up two NAT gateways. Place each NAT gateway in a different public subnet in separate Availability Zones (AZ2 and AZ3). Configure a route table for private subnets to route traffic to the virtual IP addresses of the two NAT gateways.

B. Set up two NAT gateways. Place each NAT gateway in a different public subnet in separate Availability Zones (AZ2 and AZ3). Configure a route table to point the AZ2 private subnets to the NAT gateway in AZ2. Configure the same route table to point the AZ3 private subnets to the NAT gateway in AZ3.

C. Create a second VPC (VPC2). Set up two NAT gateways. Place each NAT gateway in a different VPC (VPC1 and VPC2) and in the same Availability Zone (AZ2). Configure a route table in VPC1 to point the AZ2 private subnets to one NAT gateway. Configure a route table in VPC2 to point the AZ2 private subnets to the second NAT gateway.

D. Set up two NAT gateways. Place each NAT gateway in a different public subnet in separate Availability Zones (AZ2 and AZ3). Configure a route table to point the AZ2 private subnets to the NAT gateway in AZ2. Configure a second route table to point the AZ3 private subnets to the NAT gateway in AZ3. Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Comments

backspace0900 Highly Voted 2 years ago

Selected Answer: D

D NAT2-AZ2 NAT3-AZ3

woorkim 1 year, 3 months ago

D is correct. no VIP in NAT GW!

tromyunpak 1 year, 12 months ago

D is correct - as you will have 1 NAT per AZ with each subnet has its own route table A is wrong since you cannot use virtual IP of the NAT gateway (feature not available) C is wrong due to the fact that a new vpc is not required B is wrong since AZ2 & AZ3 are sharing the same nat gatweway

https://zhangxuetu.online

[202610]

Question #171 Topic 1

A company has a total of 30 VPCs. Three AWS Regions each contain 10 VPCs. The company has attached the VPCs in each Region to a transit gateway in that Region. The company also has set up inter-Region peering connections between the transit gateways.

The company wants to use AWS Direct Connect to provide access from its on-premises location for only four VPCs across the three Regions. The company has provisioned four Direct Connect connections at two Direct Connect locations.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

A. Create four virtual private gateways. Attach the virtual private gateways to the four VPCs. **Most Voted**

B. Create a Direct Connect gateway. Associate the four virtual private gateways with the Direct Connect gateway. **Most Voted**

C. Create four transit VIFs on each Direct Connect connection. Associate the transit VIFs with the Direct Connect gateway.

D. Create four transit VIFs on each Direct Connect connection. Associate the transit VIFs with the four virtual private gateways.

E. Create four private VIFs on each Direct Connect connection to the Direct Connect gateway. **Most Voted**

F. Create an association between the Direct Connect gateway and the transit gateways.

Correct Answer: ABE

Community vote distribution



Comments

psou7 **Highly Voted** 2 years ago

ABE TGW for inter VPC peering within AWS. From on-prem access to only 4 VPCs is required. Hence DXGW and VGW via private VIF. Peering TGW with DXGW would be possible for on-prem connectivity but is more costly. https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-vgw-multi-regions-and-aws-public-peering.html

Nouwara 10 months, 4 weeks ago

Selected Answer: BCF

as there is already a TGW, why nor use it

Hubabi 1 year ago

Selected Answer: ABE

From the options presented, it's clear that you need to use DXGW. The only option where "Create a Direct Connect gateway" is stated is option (B). Option (B) also states "Associate the four virtual private gateways with the Direct Connect gateway", thus you need to pick the other two remaining options that make sense with VGW - (A) and (E). Regardless what the cost is, this is the only valid answer that you can select.

woorkim 1 year, 3 months ago

Selected Answer: ABE

TGW is asking more cost!

MO_SAM 1 year, 5 months ago

Selected Answer: BCF

Since there already and exciting TWG there is no need to create VGW and private VIFs, instead just create 4 transit VIF along with DXGW and association to connect things together and hence COST is the main factor!

VerRi 1 year, 5 months ago

Selected Answer: ABE

BCF is a good practice but ABE is cheaper.

AlirezaNetWorld 1 year, 6 months ago

BCF based on the current setup on AWS.

cerifyme85 1 year, 11 months ago

Selected Answer: ABE

TGW for inter VPC peering within AWS. From on-prem access to only 4 VPCs is required. Hence DXGW and VGW via private VIF. Peering TGW with DXGW would be possible for on-prem connectivity but is more costly.

cerifyme85 1 year, 11 months ago

Also only need one TGW per region .. we have 3 regions, question does not give the split per region.... so not 4 TGW

cerifyme85 1 year, 11 months ago

Sorry guys just an adjustment in understanding : connecting to VPC directly ==> PVIF + DXG + VPG

cerifyme85 1 year, 11 months ago

If the option was to use TGW, they would have provided an option in the answer to connect DX Gateway to TGW. Also the conectivity to "only" for VPCs does not affect the architecture design as Psou7 said, and given the above, both VPG and TG would work, it is just which one is less expensive.. OR which combination of answers helps. VPG ==> VPG +DXG + PVIF TGW ==> TGW + DXG + TVIF The above options ==> so ABE

victian 1 year ago

if use TGW ==> TGW + DXG + TVIF solution，option C and F are enough？

KobDragoon 1 year, 11 months ago

Selected Answer: ABE

As there is no answer that allows us to configure specific route tables in the TGW to make the DataCenters really only have access to 4 of the 30 VPCs. The most logical solution is ABE, as the other options would allow access to more VPCs than intended.

tromyunpak 2 years ago

ABE are the correct answer as these are required to build the VPG setup. CD are wrong due to the fact all the VPC will access the onpremises (you need to configure the 4 specific VPC prefixes in the DX gateway to TGW association or use different routing tables within the TGW to limit the routes to only the 4 VPCs required to access the on-premises) F is not needed since VPG will be used

backspace0900 2 years ago

Selected Answer: BCF

BCF DirectConnectGateway TransitVIF TransitGateway

https://zhangxuetu.online

[202610]

Question #172 Topic 1

A company needs to manage Amazon EC2 instances through command line interfaces for Linux hosts and Windows hosts. The EC2 instances are deployed in an environment in which there is no route to the internet. The company must implement role-based access control for management of the instances. The company has a standalone on-premises environment.

Which approach will meet these requirements with the LEAST maintenance overhead?

A. Set up an AWS Direct Connect connection between the on-premises environment and the VPC where the instances are deployed. Configure routing, security groups, and ACLs. Connect to the instances by using the Direct Connect connection.

B. Deploy and configure AWS Systems Manager Agent (SSM Agent) on each instance. Deploy VPC endpoints for Systems Manager Session Manager. Connect to the instances by using Session Manager. **Most Voted**

C. Establish an AWS Site-to-Site VPN connection between the on-premises environment and the VPC where the instances are deployed. Configure routing, security groups, and ACLs. Connect to the instances by using the Site-to-Site VPN connection.

D. Deploy an appliance to the VPC where the instances are deployed. Assign a public IP address to the appliance. Configure security groups and ACLs. Connect to the instances by using the appliance as an intermediary.

Correct Answer: B

Community vote distribution

B (100%)

Comments

KobDragoon Highly Voted 1 year, 5 months ago

Selected Answer: B

Only option that references Role-Based Access Control: AWS Systems Manager integrates with AWS Identity and Access Management (IAM), allowing you to define granular access permissions based on roles.

AzureDP900 1 year, 2 months ago

Selected Answer: B

Option B is right, other options have higher maintenance overhead:

https://zhangxuetu.online

[202610]

Question #173 Topic 1

A network engineer needs to improve the network security of an existing AWS environment by adding an AWS Network Firewall firewall to control internet-bound traffic. The AWS environment consists of five VPCs. Each VPC has an internet gateway, NAT gateways, public Application Load Balancers (ALBs), and Amazon EC2 instances. The EC2 instances are deployed in private subnets. The architecture is deployed across two Availability Zones.

The network engineer must be able to configure rules for the public IP addresses in the environment, regardless of the direction of traffic. The network engineer must add the firewall by implementing a solution that minimizes changes to the existing production environment. The solution also must ensure high availability.

Which combination of steps should the network engineer take to meet these requirements? (Choose two.)

A. Create a centralized inspection VPC with subnets in two Availability Zones. Deploy Network Firewall in this inspection VPC with an endpoint in each Availability Zone.

B. Configure new subnets in two Availability Zones in each VPC. Deploy Network Firewall in each VPC with an endpoint in each Availability Zone. **Most Voted**

C. Deploy Network Firewall in each VPUse existing subnets in each of the two Availability Zones to deploy Network Firewall endpoints.

D. Update the route tables that are associated with the private subnets that host the EC2 instances. Add routes to the Network Firewall endpoints.

E. Update the route tables that are associated with the public subnets that host the NAT gateways and the ALBs. Add routes to the Network Firewall endpoints. **Most Voted**

Correct Answer: BE

Community vote distribution



Comments

backspace0900 **Highly Voted** 2 years ago

Selected Answer: BE

BE New Firewall subnet Public subnet Routetable change

daemon101 1 year, 12 months ago

B would create 10 subnets with 10 network firewall and wouldn't meet the requirement of minimizing changes to the existing production. I would go for A and E instead.

JoellaLi 1 year, 12 months ago

I choose C and E.

JoellaLi 1 year, 12 months ago

Change to A D

JoellaLi 1 year, 12 months ago

But there is no Transit Gateway now. For centralized deployment model, AWS Transit Gateway is a prerequisite. AWS Transit Gateway acts as a network hub and simplifies the connectivity between VPCs as well as on-premises networks. AWS Transit Gateway also provides inter-region peering capabilities to other Transit Gateways to establish a global network using AWS backbone. Another key characteristic of the centralized deployment is a dedicated inspection VPC. Inspection VPC consists of two subnets in each AZs. One subnet is a dedicated firewall endpoint subnet and second is dedicated to AWS Transit Gateway attachment.

percolate792 1 year ago

Selected Answer: AE

Comparing this to Option A (centralized inspection VPC), which creates a single new VPC without touching the existing VPCs' structure, Option B introduces more changes to the production environment by adding new subnets to each VPC. In terms of "minimizing changes to existing production environment," Option A (centralized model) would generally be considered less intrusive than Option B (distributed model) because: It leaves the structure of existing VPCs unchanged It requires only one Network Firewall deployment instead of five It centralizes security management rather than distributing it

hughnguyen 1 year, 1 month ago

Selected Answer: AE

It's easier to create a single VPC than it is to add 2 subnets two five VPCs

MO_SAM 1 year, 5 months ago

Selected Answer: BE

ALL options are valid **___but___** you need to look at the requirements aka the criteria! which means min changes/interruption to the existing PROD env so definitely BE

Blitz1 1 year, 8 months ago

Selected Answer: BE

It took me some time to understand the infra and what is requested. It's indeed about decentralized env because you need transit gateway for centralized one. Plus it is saying that each vpc is completely independent and we need to provide a " solution that minimizes changes". OK , so we have B until now. But were we put the routes: in private subnet or in public subnet. Here is comes the trick saying that we have ALB. So we will put route in public subnet to protect also ALB. So we have E. please read carefully: https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/

acloudguru 1 year, 10 months ago

Selected Answer: AE

The combination of these two steps meets the requirements of adding an AWS Network Firewall firewall to control internet-bound traffic, minimizing changes to the existing production environment, ensuring high availability, and allowing the configuration of rules for public IP addresses in both directions. Options B and C involve deploying Network Firewall in each VPC, which may not be necessary and could lead to increased complexity and management

overhead. Option D alone is not sufficient, as it only covers traffic from the private EC2 instances but not the public ALBs.

Sailor 1 year, 10 months ago

to choose A, you need connectivity between the new inspection VPC and the VPC either by VPC peering or transit gateway (both are not mentioned) , so the only way to direct traffic to the network firewall is new subnet

Spaurito 1 year, 4 months ago

Great point on the VPC connectivity. It does not mention if the 5 VPCs are all connected. If they were, "A" would be a definite.

cerifyme85 1 year, 11 months ago

Selected Answer: BE

It is not a centralised setup. It is a distributed setup. Five seperate VPCs Each VPC : ALB + NAT + EC2 Question says architecture should not be changed. So just deploy ANF endpoints in a sep subnet in each AZ. https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/#:~:text=AWS%C2%A0Network%C2%A0Firewall%20is%20deployed%20to%20protect%20traffic%20between%20a%20workload%20public%20subnet%20and%20IGW Also question is concenred about about inbound traffic so E To use centralised we need a TGW

Spaurito 1 year, 4 months ago

The question states minimal changes. The central may seem to be out of line, but it meets the minimal changes to the existing environments and ensures high availability.

cerifyme85 1 year, 11 months ago

Selected Answer: AD

Ans is AD

Sailor 1 year, 11 months ago

D talks about private subnets and the question says: The network engineer must be able to configure rules for the public IP addresses in the environment, regardless of the direction of traffic., so it is A, E

xTrayusx 1 year, 11 months ago

Selected Answer: AE

'The network engineer must add the firewall by implementing a solution that minimizes changes to the existing production environment'

JoellaLi 1 year, 12 months ago

Selected Answer: AD

The Network Firewall acts as a "filter" for traffic between the subnets and locations outside the VPC. To enable this filtering, route tables need to be modified so traffic passes through the firewall endpoints. Private subnets contain the EC2 instances, so their route tables should be updated to send outbound traffic to the firewall. The firewall then allows or denies the traffic before sending it to its final destination like internet gateway or NAT gateway. Route tables for public subnets hosting NAT/ALB do not need changes as instances are not present there. Traffic originating from private subnets is what needs inspection.

JoellaLi 1 year, 11 months ago

Filter traffic going to and from the EC2 instances in the private subnets. This will ensure traffic from the instances is directed through the Network Firewall endpoints before reaching its destination (such as the internet gateway or NAT gateway).]

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #174 Topic 1

A company is planning to migrate an internal application to the AWS Cloud. The application will run on Amazon EC2 instances in one VPC. Users will access the application from the company's on-premises data center through AWS VPN or AWS Direct Connect. Users will use private domain names for the application endpoint from a domain name that is reserved explicitly for use in the AWS Cloud.

Each EC2 instance must have automatic failover to another EC2 instance in the same AWS account and the same VPC. A network engineer must design a DNS solution that will not expose the application to the internet.

Which solution will meet these requirements?

A. Assign public IP addresses to the EC2 instances. Create an Amazon Route 53 private hosted zone for the AWS reserved domain name. Associate the private hosted zone with the VPC. Create a Route 53 Resolver outbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the outbound endpoint IP address for Route 53 Resolver. In the private hosted zone, configure primary and failover records that point to the public IP addresses of the EC2 instances. Create an Amazon CloudWatch metric and alarm to monitor the application's health. Set up a health check on the alarm for the primary application endpoint.

B. Place the EC2 instances in private subnets. Create an Amazon Route 53 public hosted zone for the AWS reserved domain name. Associate the public hosted zone with the VPC. Create a Route 53 Resolver inbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the inbound endpoint IP address for Route 53 Resolver. In the public hosted zone, configure primary and failover records that point to the IP addresses of the EC2 instances. Create an Amazon CloudWatch metric and alarm to monitor the application's health. Set up a health check on the alarm for the primary application endpoint.

C. Place the EC2 instances in private subnets. Create an Amazon Route 53 private hosted zone for the AWS reserved domain name. Associate the private hosted zone with the VPCreate a Route 53 Resolver inbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the inbound endpoint IP address for Route 53 Resolver. In the private hosted zone, configure primary and failover records that point to the IP addresses of the EC2 instances. Create an Amazon CloudWatch metric and alarm to monitor the application's health. Set up a health check on the alarm for the primary application endpoint. **Most Voted**

D. Place the EC2 instances in private subnets. Create an Amazon Route 53 private hosted zone for the AWS reserved domain name. Associate the private hosted zone with the VPC. Create a Route 53 Resolver inbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the inbound endpoint IP address for Route 53 Resolver. In the private hosted

zone, configure primary and failover records that point to the IP addresses of the EC2 instances. Set up Route 53 health checks on the private IP addresses of the EC2 instances.

Correct Answer: C

Community vote distribution



Comments

backspace0900 Highly Voted 2 years ago

C Route53 healthchecker need publicIP

psou7 2 years ago

Agree. C

Spaurito 1 year, 4 months ago

C - as per documentation - To set up Route 53 health checks on the private IP addresses of EC2 instances, you need to assign a public IP address to the EC2 instance as Route 53 health checkers can only access resources with publicly routable IP addresses; then, configure the health check in Route 53 to point to that public IP, allowing you to monitor the health of your private resource within the VPC; you can use a private hosted zone to associate the health check with your internal domain names This would expose to the internet. Monitoring the applications endpoint is the next solution.

khaanikahttak 1 year, 7 months ago

D is correct answer. Coz route53 health check is design for end points fail over. route 53 redirect traffic to the healthy end point in case one is failed.

cerifyme85 1 year, 11 months ago

Selected Answer: C

Can only be done using cloudwatch for private IPS https://aws.amazon.com/blogs/networking-and-content-delivery/performing-route-53-health-checks-on-private-resources-in-a-vpc-with-aws-lambda-and-amazon-cloudwatch/ R53 cannot monitor pHz https://repost.aws/questions/QUVcLK5gUqSxKGondJkrzw0Q/private-zone-route53-health-checks#:~:text=If%20you%20mean,private%20hosted%20zone

KobDragoon 1 year, 11 months ago

Selected Answer: D

I vote for D instead of C, because Route53 health checks are necessary for the implementation of Route53 failover records. R53 health checks can be done directly to the instances or to the cloudwatch alarms, but why use cloudwatch alarm configuration when you can go the more direct route and there is no requirement to get any metrics from the EC2s from cloudwatch.

JoellaLi 1 year, 11 months ago

but Route53 healthchecker need publicIP

AzureDP900 1 year, 2 months ago

D is right Route 53 health checks do not necessarily require a public IP address. According to Amazon Web Services (AWS), you can configure Route 53 health checks to use private IP addresses, such as those assigned to an Elastic IP or a NAT gateway. This allows you to monitor the availability of your application without exposing it to the internet.

backspace0900 1 year, 12 months ago

Selected Answer: C

supplement the vote

https://zhangxuetu.online

[202610]

Question #175 Topic 1

A company uses Amazon Route 53 for its DNS needs. The company's security team wants to update the DNS infrastructure to provide the most recent security posture.

The security team has configured DNS Security Extensions (DNSSEC) for the domain. The security team wants a network engineer to explain who is responsible for the rotation of DNSSEC keys.

Which explanation should the network administrator provide to the security team?

A. AWS rotates the zone-signing key (ZSK). The company rotates the key-signing key (KSK). **Most Voted**

B. The company rotates the zone-signing key (ZSK) and the key-signing key (KSK).

C. AWS rotates the AWS Key Management Service (AWS KMS) key and the key-signing key (KSK).

D. The company rotates the AWS Key Management Service (AWS KMS) key. AWS rotates the key-signing key (KSK).

Correct Answer: A

Community vote distribution

A (100%)

Comments

backspace0900 **Highly Voted** 2 years ago

Selected Answer: A

customer KSK AWS ZSK

Kayceetalks 2 years ago

Agreed A, You are responsible for KSK management, which includes rotating it if needed. ZSK management is performed by Route 53. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-configuring-dnssec.html

a0e6696 7 months ago

Selected Answer: A

There are two kinds of keys in DNSSEC: a key-signing key (KSK) and a zone-signing key (ZSK). In Route 53 DNSSEC signing, each KSK is based on an asymmetric customer managed key in AWS KMS that you own. You are responsible for KSK management, which includes rotating it if needed. ZSK management is performed by Route 53.

AzureDP900 1 year, 2 months ago

Selected Answer: A

In DNSSEC, Amazon Route 53 handles the rotation of the Zone Signaling Key (ZSK). The ZSK is used to sign the DNS records in a zone and is typically rotated by AWS every 90 days. This ensures that any man-in-the-middle

attacks are quickly identified and mitigated. On the other hand, the company's Key Signing Key (KSK) should be rotated regularly, but not automatically by AWS. The KSK is used to sign the ZSKs themselves, and its rotation is typically performed by the company itself, either manually or through automation scripts.

woorkim 1 year, 3 months ago

A is answer! There are two kinds of keys in DNSSEC: a key-signing key (KSK) and a zone-signing key (ZSK). In Route 53 DNSSEC signing, each KSK is based on an asymmetric customer managed key in AWS KMS that you own. You are responsible for KSK management, which includes rotating it if needed. ZSK management is performed by Route 53.

Nodin 2 years ago

Selected Answer: A

AWS rotates ZSK and customer rotates KSK (self managed)

https://zhangxuetu.online

[202610]

Question #176 Topic 1

A company has agreed to collaborate with a partner for a research project. The company has multiple VPCs in the us-east-1 Region that use CIDR blocks within 10.10.0.0/16. The VPCs are connected by a transit gateway that is named TGW-C in us-east-1. TGW-C has an Autonomous System Number (ASN) configuration value of 64520.

The partner has multiple VPCs in us-east-1 that use CIDR blocks within 172.16.0.0/16. The VPCs are connected by a transit gateway that is named TGW-P in us-east-1. TGW-P has an ASN configuration value of 64530.

A network engineer needs to establish network connectivity between the company's VPCs and the partner's VPCs in us-east-1.

Which solution will meet these requirements with MINIMUM changes to both networks?

A. Create a new VPC in a new account. Deploy a router from AWS Marketplace. Share TGW-C and TGW-P with the new account by using AWS Resource Access Manager (AWS RAM). Associate TGW-C and TGW-P with the new VPC. Configure the router in the new VPC to route between TGW-C and TGW-P.

B. Create an IPsec VPN connection between TGW-C and TGW-P. Configure the routing between the transit gateways to use the IPsec VPN connection.

C. Configure a cross-account transit gateway peering attachment between TGW-C and TGW-P. Configure the routing between the transit gateways to use the peering attachment. Most Voted

D. Share TGW-C with the partner account by using AWS Resource Access Manager (AWS RAM). Associate the partner VPCs with TGW-C. Configure routing in the partner VPCs and TGW-C.

Correct Answer: C

Community vote distribution



Comments

psou7 Highly Voted 2 years ago

I vote for C https://repost.aws/questions/QUbU0rsbkYTPKWHqYT0nIAEA/transit-gateway-peering-cross-accounts-not-sharing-payer-id

Spaurito 1 year, 4 months ago

C - You can peer into an opt-in Region as long as the account that accepts the peering attachment has opted into that Region.

Spaurito 1 year, 4 months ago

C - The task is to establish connectivity between the 2 companies and their VPC's. Option D - Although you could use (RAM), it doesn't define they would be sharing resources.

cas_tori 1 year, 6 months ago

Selected Answer: C

this is C

amamatsumoto9 1 year, 7 months ago

I think it's D. Because transit gateways are not normally peered within a region, but rather peered across regions.

rdiaz 1 year, 9 months ago

Selected Answer: C

c transit gw cross account sharing

https://zhangxuetu.online

[202610]

Question #177 Topic 1

A company has a public application. The application uses an Application Load Balancer (ALB) that has a target group of Amazon EC2 instances.

The company wants to protect the application from security issues in web requests. The traffic to the application must have end-to-end encryption.

Which solution will meet these requirements?

A. Configure a Network Load Balancer (NLB) that has a target group of the existing EC2 instances. Configure TLS connections to terminate on the EC2 instances that use a public certificate. Configure an AWS WAF web ACL. Associate the web ACL with the NLB.

B. Configure TLS connections to terminate at the ALB that uses a public certificate. Configure AWS Certificate Manager (ACM) certificates for the communication between the ALB and the EC2 instances. Configure an AWS WAF web ACL. Associate the web ACL with the ALB.

C. Configure a Network Load Balancer (NLB) that has a target group of the existing EC2 instances. Configure TLS connections to terminate at the EC2 instances by creating a TLS listener. Configure self-signed certificates on the EC2 instances for the communication between the NLB and the EC2 instances. Configure an AWS WAF web ACL. Associate the web ACL with the NLB.

D. Configure a third-party certificate on the EC2 instances for the communication between the ALB and the EC2 instances. Import the third-party certificate into AWS Certificate Manager (ACM). Associate the imported certificate with the ALB. Configure TLS connections to terminate at the ALB. Configure an AWS WAF web ACL. Associate the web ACL with the ALB. **Most Voted**

Correct Answer: D

Community vote distribution

D (72%) B (28%)

Comments

JoellaLi **Highly Voted** 1 year, 11 months ago

Selected Answer: D

ACM certificates are supported by the following services: • Elastic Load Balancing To serve secure content over SSL/TLS, load balancers require that SSL/TLS certificates be installed on either the load balancer or the back-end Amazon EC2 instance. ACM is integrated with Elastic Load Balancing to deploy ACM certificates on the load balancer. • Amazon CloudFront To use an ACM certificate with CloudFront, make sure you request (or import) the certificate in

the US East Region (us-east-1). • Amazon API Gateway With the proliferation of mobile devices and growth of the Internet of Things (IoT), it has become increasingly common to create APIs that can be used to access data and interact with back-end systems on AWS. • AWS Nitro Enclaves EC2 instances connected to Nitro Enclaves support ACM certificates. You cannot associate ACM certificates with an EC2 instance that is not connected to a Nitro Enclave.

Blitz1 Highly Voted 1 year, 8 months ago

Selected Answer: D

The debate is between B and D ...(because the question is actually saying that ALB is already used -> NLB is excluded from the beginning) Even if ACM is more easier to use (i mean you don't need to go to a third party provider) when reading B answer it is saying : "Configure AWS Certificate Manager (ACM) certificates for the communication between the ALB and the EC2 instances." You cannot use ACM for communication between ALB and EC2. Actually in the target group you can specify protocol and port and the instances associated but there is no field where to specify which certificate to use. Also in (B) it is not saying to configure the certificates in EC2 which is wrong as well. The ACM is used for ALB and in the listener part you have the default certificate and the SNIs under certificates tab. Therefore D is the correct answer.

yismail 2 months, 3 weeks ago

Selected Answer: B

the solution must include WAF ACL to "protect the application from security issues in web requests" WAF ACL can't be associated with NLB

Nouwara 10 months, 4 weeks ago

Selected Answer: D

between B or D.

Spaurito 1 year, 4 months ago

D - You can import a certificate for use with ALB, CF, etc. If you need on your EC2 instances, you will need to import to them as well, but they can be used. Do this on a regular basis it seems.

VerRi 1 year, 5 months ago

Selected Answer: D

You cannot use ACM's cert between EC2 and ALB.

Spaurito 1 year, 4 months ago

You can get a Public cert, install on EC2 instances, import into ACM, and associate it to other resources. It's just not an AWS provided certificate.

hedglin 1 year, 8 months ago

B is correct. D is wrong, because this option involves using a third-party certificate, which adds complexity without providing any clear benefits over using ACM directly for certificate management. Terminating TLS at the ALB and applying the WAF ACL at the ALB level is correct, but the ALB's integration with ACM simplifies the process.

hedglin 1 year, 6 months ago

Sorry, D is correct. You cannot directly use AWS ACM (Certificate Manager) for communication between an Application Load Balancer (ALB) and an EC2 instance.

KobDragoon 1 year, 11 months ago

Selected Answer: B

WAF for security and ACM managed certificate for TLS encryptions. B looks fine to me

掌学兔
ZHANGXUETU

[202610]

Question #178 Topic 1

A company has an application that hosts personally identifiable information (PII) of users. All connections to the application must be secured by HTTPS with TLS certificates that implement Elliptic Curve Cryptography (ECC).

The application uses stateful connections between the web tier and the end users. Multiple instances host the application. A network engineer must implement a solution that offloads TLS connections to a load balancer.

Which load-balancing solution will meet these requirements?

A. Provision a Network Load Balancer. Configure a TLS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS identity and Access Management (IAM). Turn on health checks to monitor the web hosts that connect to the end users.

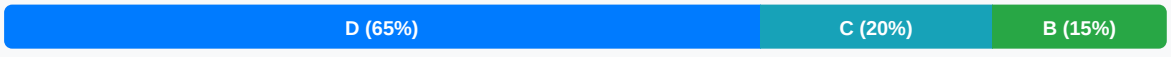
B. Provision an Application Load Balancer. Configure an HTTPS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS Certificate Manager (ACM). Configure a default action to redirect to the URL for the application. Turn on health checks to monitor the web hosts that connect to the end users.

C. Provision a Network Load Balancer. Configure a TLS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS Certificate Manager (ACM). Turn on application-based session affinity (sticky sessions). Turn on health checks to monitor the web hosts that connect to the end users.

D. Provision an Application Load Balancer. Configure an HTTPS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS Identity and Access Management (IAM). Configure a default action to redirect to the URL for the application. Turn on application-based session affinity (sticky sessions). **Most Voted**

Correct Answer: D

Community vote distribution



Comments

yismail 2 months, 3 weeks ago

Selected Answer: D

I agree, D is the correct answer

DSExam 1 year, 2 months ago

Selected Answer: D

You can upload certificate to IAM via aws cli. ACM did not support ECC-SSL at the time exam question were written, but they do now, for the purpose of this question you need to use IAM. https://repost.aws/knowledge-center/import-ssl-

certificate-to-iam

woorkim 1 year, 3 months ago

Selected Answer: D

A. Network Load Balancer with ECC SSL certificate in IAM: Network Load Balancers (NLBs) support TLS listeners but are designed for layer 4 (TCP) traffic. They lack features like session affinity and application-specific health checks. NLBs are not suitable for applications requiring sticky sessions or application-layer processing. B. ALB with health checks but no session affinity: This option misses the requirement for maintaining stateful connections. Without session affinity, the ALB may route user requests to different backend instances, breaking stateful communication. C. NLB with ECC SSL certificate in ACM and session affinity: NLB does not natively support application-based session affinity or sticky sessions. NLB is a layer 4 load balancer and is not optimal for this use case, which requires application-layer capabilities.

Christina666 1 year, 3 months ago

Selected Answer: B

weird question, C and D both incorrect

imymoco 1 year, 3 months ago

Selected Answer: C

c why use iam

MO_SAM 1 year, 5 months ago

Selected Answer: D

Network load balancer does not the stickiness!! because stateful means you have to enable the sessions sickness which application layer 7

Spaurito 1 year, 4 months ago

You can set sticky sessions with Target groups on the NLB now. In the past was not supported.

Spaurito 1 year, 4 months ago

and to further define...not for application support.

KobDragoon 1 year, 11 months ago

Selected Answer: D

Considering the importance of sticky sessions for stateful connections in conjunction with the other requirements (end-to-end encryption, use of ECC certificates), Option D works better, even if managing the certificate with IAM instead of ACM feels weird, it is possible.

bluz 2 years ago

Selected Answer: D

NLB does not use application-based stickiness. For certificates in a Region supported by AWS Certificate Manager (ACM), we recommend that you use ACM to provision, manage, and deploy your server certificates. In unsupported Regions, you must use IAM as a certificate manager.

daemon101 1 year, 12 months ago

i would for B if the ALB is using cookie-based affinity but it is not mentioned so I agree with you. I would also go for D. i think C is incorrect because when NLB is using a TLS listener, the session stickiness feature will longer available. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_server-certs.html

psou7 2 years ago

i Vote C

KobDragoon 1 year, 11 months ago

Wrong - NLBs do not inherently manage application-level session affinity ("sticky sessions") based on cookies.

backspace0900 2 years ago

Selected Answer: C

C ssl certificate managed acm

KobDragoon 1 year, 11 months ago

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#sticky-sessions

"Sticky sessions are not supported for TLS listeners."

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #179 Topic 1

A company hosts infrastructure services in multiple VPCs across multiple accounts in the us-west-2 Region. The VPC CIDR blocks do not overlap. The company wants to connect the VPCs to its data centers by using AWS Site-to-Site VPN tunnels.

The connections must be encrypted in transit. Additionally, the connection from each data center must route to the closest AWS edge location. The connections must be highly available and must accommodate automatic failover.

Which solution will meet these requirements?

A. Deploy a transit gateway. Share the transit gateway with each of the other accounts by using AWS Resource Access Manager (AWS RAM). Create VPC attachments to the transit gateway from each service account. Add routes to the on-premises subnet in each of the service VPC route tables by using the attachment as the gateway. Create Site-to-Site VPN tunnel attachments with dynamic routing to the transit gateway. Enable the acceleration feature for the Site-to-Site VPN connection. Configure the VPN tunnels on the on-premises equipment. Configure BGP peering. **Most Voted**

B. Deploy VPN gateways to each account. Enable the acceleration feature for VPN gateways on each account. Add routes to the on-premises subnet in each of the service VPC route tables. Use the VPNs as the gateway. Configure the VPN tunnels on the on-premises equipment. Configure BGP peering.

C. Deploy a transit gateway. Share the transit gateway with each of the other accounts by using AWS Resource Access Manager (AWS RAM). Create VPC attachments to the transit gateway from each service account. Add routes to the on-premises subnet in each of the service VPC route tables by using the attachment as the gateway. Create Site-to-Site VPN tunnel attachments with dynamic routing to the transit gateway. Enable the acceleration feature for the Site-to-Site VPN connection. Configure the VPN tunnels on the on-premises equipment. Configure static routing.

D. Deploy VPN gateways to each account. Enable the acceleration feature for VPN gateways on each account. Add routes to the on-premises subnet in each of the service VPC route tables. Use the VPNs as the gateway. Configure the VPN tunnels on the on-premises equipment. Configure static routing.

Correct Answer: A

Community vote distribution

A (100%)

Comments

Blitz1 Highly Voted 1 year, 8 months ago

Selected Answer: A

automatic failover = BGP -> so we exclude static acceleration is not possible in Virtual private gateway -> and this is how we remain with (A)

KobDragoon 1 year, 11 months ago

Selected Answer: A

Looks good, A over C just due to dynamic routing with BGP peering instead of static routing.

Kayceetalks 2 years ago

A - correct

psou7 2 years ago

I agree with A

https://zhangxuetu.online

[202610]

Question #180 Topic 1

A company has a transit gateway in AWS Account A. The company uses AWS Resource Access Manager (AWS RAM) to share the transit gateway so that users in other accounts can connect to multiple VPCs in the same AWS Region. AWS Account B contains a VPC (10.0.0.0/16) with subnet 10.0.0.0/24 in the us-west-2a Availability Zone and subnet 10.0.1.0/24 in the us-west-2b Availability Zone. Resources in these subnets can communicate with other VPCs.

A network engineer creates two new subnets: 10.0.2.0/24 in the us-west-2b Availability Zone and 10.0.3.0/24 in the us-west-2c Availability Zone. All the subnets share one route table. The default route 0.0.0.0/0 is pointing to the transit gateway. Resources in subnet 10.0.2.0/24 can communicate with other VPCs, but resources in subnet 10.0.3.0/24 cannot communicate with other VPCs.

What should the network engineer do so that resources in subnet 10.0.3.0/24 can communicate with other VPCs?

A. In Account B, add 10.0.2.0/24 and 10.0.3.0/24 as the destinations to the route table. Use the transit gateway as the target.

B. In Account B, update the transit gateway attachment. Attach the new subnet ID that is associated with us-west-2c to Account B's VPC. **Most Voted**

C. In Account A, create a static route for 10.0.3.0/24 in the transit gateway route tables.

D. In Account A, recreate propagation for 10.0.0.0/16 in the transit gateway route tables.

Correct Answer: B

Community vote distribution



Comments

acloudguru Highly Voted 1 year, 10 months ago

Selected Answer: B

Option C is incorrect because the transit gateway route tables are managed by Account A, which owns the transit gateway. Account B cannot modify the route tables in Account A's transit gateway. Option D is incorrect because propagation is not relevant in this scenario. Propagation is used when you have multiple transit gateways in different AWS Regions, and you want to propagate routes between them.

KobDragoon Highly Voted 1 year, 11 months ago

Selected Answer: C

If all subnets share one route table then new subnet in AZ C should also have a route to the TGW, and we don't need necessarily a TGW attachment associated with the new subnet C, it should be able to route to the existing TGW attachments inside the VPC. Only answer that makes sense to me then is C if we assume that Account B doesn't have route propagation enabled by default and the TGW route tables are using instead static routes. This would explain why traffic can't reach the new subnet but can reach the others.

6e5b127 1 year, 8 months ago

Resources that reside in Availability Zones where there is no transit gateway attachment cannot reach the transit gateway even though route table is set up. You need to assciate at least one subnet in even AZ. So the answer is B.

Spaurito 1 year, 4 months ago

B - The new subnet is in a new AZ. If not associated to the TGW, then it won't communicate. The new AZ is key here.

siheom 1 year, 7 months ago

Selected Answer: B

vote B

kajiyatta 1 year, 8 months ago

When you attach a VPC to a transit gateway, you must specify one subnet from each Availability Zone to be used by the transit gateway to route traffic. Specifying one subnet from an Availability Zone enables traffic to reach resources in every subnet in that Availability Zone. https://docs.aws.amazon.com/vpc/latest/tgw/tgw-vpc-attachments.html

hedglin 1 year, 8 months ago

The correct answer is B: In Account B, update the transit gateway attachment. Attach the new subnet ID that is associated with us-west-2c to Account B's VPC. C is wrong. Creating a static route in Account A's transit gateway route tables is not necessary and wouldn't solve the issue, as the problem is with the attachment, not routing.

seochan 1 year, 10 months ago

Selected Answer: C

There’s no such thing as ‘Attach the new subnet ID’ in TGW attachments.

Kupaloid 1 year, 10 months ago

Selected Answer: B

The most likely cause is that the new subnet has not been attached to the transit gateway.

https://zhangxuetu.online

[202610]

Question #181 Topic 1

A company has started using AWS Cloud WAN with one edge location in the us-east-1 Region. The company has a production segment and a security segment in AWS Cloud WAN. The company also has a default core network policy.

The company has created a production VPC for the production workload. The company has created an outbound inspection VPC to inspect internet-bound traffic from the production VPC. The company has attached the production VPC to the production segment and has attached the outbound inspection VPC to the security segment. The company has also created an AWS Network Firewall firewall in the outbound inspection VPC to inspect internet-based traffic.

The company has updated a route table for the production VPC to send all internet-bound traffic to the AWS Cloud WAN core network. The company has updated a route table for the outbound inspection VPC to ensure that Network Firewall inspects any outgoing traffic and incoming traffic.

During testing, an Amazon EC2 instance in the production VPC cannot reach the internet. The company checks the Network Firewall rules and confirms that the rules are not blocking the traffic.

Which combination of steps will meet these requirements? (Choose two.)

A. Update the core network policy to configure segment sharing. Share the production segment with the security segment. **Most Voted**

B. Update the core network policy to create a static route for the security segment. Specify 0.0.0.0/0 as the destination CIDR block. Specify the outbound inspection VPC as an attachment.

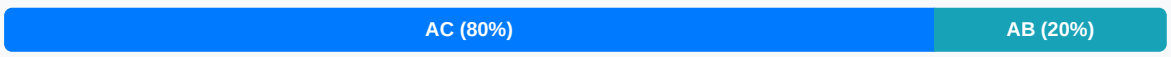
C. Update the core network policy to create a static route for the production segment. Specify 0.0.0.0/0 as the destination CIDR block. Specify the outbound inspection VPC as an attachment. **Most Voted**

D. Update the core network policy to create a static route for the production segment. Specify 10.2.0.0/16 as the destination CIDR block. Specify the outbound inspection VPC as an attachment.

E. Create an attachment to attach the outbound inspection VPC to the production segment. Update the core network policy to turn on isolated attachment for the production segment.

Correct Answer: AC

Community vote distribution



Comments

Rollizo 1 year ago

Selected Answer: AC

It is C because of this sentence: "The company has updated a route table for the production VPC to send all internet-bound traffic to the AWS Cloud WAN core network." Then you need to configure the CORE route policy with a static route in production segment to send the traffic to inspection

secdaddy 1 year, 1 month ago

Selected Answer: AB

"Segment sharing is bidirectional by default." so A handles routing between security and production. https://docs.aws.amazon.com/network-manager/latest/cloudwan/cloudwan-policy-network-actions-routes.html B is required to enable the security segment to route traffic to the inspection VPC

woorkim 1 year, 3 months ago

Selected Answer: AC

Option B is not correct because a static route for the security segment targeting 0.0.0.0/0 does not directly solve the issue for production traffic routing. Option D is incorrect because it involves a route with a CIDR block that does not represent internet-bound traffic (10.2.0.0/16 is a private IP range). Option E is incorrect because attaching the outbound inspection VPC directly to the production segment and enabling isolated attachment conflicts with the requirement to inspect traffic through the security segment.

Blitz1 1 year, 8 months ago

Selected Answer: AC

A. When traffic is returning from internet to inspection segment a route is needed to pass the traffic to correct segment. https://docs.aws.amazon.com/network-manager/latest/cloudwan/cloudwan-policy-network-actions-routes.html C. is pushing all the traffic (internet) to outbound inspection

973b658 1 year, 11 months ago

Selected Answer: AC

A&C is OK.

Stants 1 year, 11 months ago

Option C: Update the core network policy to create a static route for the production segment. Specify 0.0.0.0/0 as the destination CIDR block. Specify the outbound inspection VPC as an attachment. Explanation: By creating a static route for the production segment with a destination of 0.0.0.0/0 (which covers all internet-bound traffic), and attaching it to the outbound inspection VPC, you ensure that traffic from the production VPC is directed to the Network Firewall in the outbound inspection VPC. Option D: Update the core network policy to create a static route for the production segment. Specify 10.2.0.0/16 as the destination CIDR block. Specify the outbound inspection VPC as an attachment. Explanation: Creating a static route for the production segment with a specific destination CIDR block (10.2.0.0/16) ensures that traffic from the production VPC is routed to the outbound inspection VPC.

https://zhangxuetu.online

[202610]

Question #182 Topic 1

A company has two business units (BUs). The company operates in the us-east-1 Region and the us-west-1 Region. The company plans to extend to more Regions in the future. Each BU has a VPC in each Region. Each Region has a transit gateway with the BU VPCs attached. The transit gateways in both Regions are peered.

The company will create several more BUs in the future and will need to isolate some of the BUs from the other BUs. The company wants to migrate to an architecture to incorporate more Regions and BUs.

Which solution will meet these requirements with the MOST operational efficiency?

A. Create a new transit gateway for each new BU in each Region. Peer the new transit gateways with the existing transit gateways. Update the route tables to control traffic between BUs.

B. Create an AWS Cloud WAN core network with an edge location in both Regions. Configure a segment for each BU with VPC attachments to the new BU VPCs. Use segment actions to control traffic between segments. **Most Voted**

C. Create an AWS Cloud WAN core network with an edge location in both Regions. Configure a segment for each BU with VPC attachments to the new BU VPCs. Configure the segments to isolate attachments to control traffic between segments.

D. Attach new VPCs to the existing transit gateways. Update route tables to control traffic between BUs.

Correct Answer: B

Community vote distribution



Comments

973b658 **Highly Voted** 1 year, 11 months ago

Selected Answer: B

it is B.

secdaddy 1 year, 1 month ago

Selected Answer: C

Stated goal is to isolate some BUs from other BUs with the most operational efficiency so I am going with isolate attachements.

AzureDP900 1 year, 2 months ago

Selected Answer: B

Option B: This solution involves creating an AWS Cloud WAN core network with an edge location in both Regions, configuring a segment for each BU with VPC attachments to the new BU VPCs. Segment-based routing : Segment actions can control traffic between segments and provide a more isolated environment, which is necessary when dealing with multiple BUs. This makes it easier to isolate certain BUs from others while maintaining connectivity between others. Option B also provides flexibility and scalability as new Regions can be added, and new segments can be created without requiring additional changes to existing transit gateways or VPCs.

woorkim 1 year, 3 months ago

Selected Answer: B

Option A requires creating and peering multiple transit gateways, which increases complexity. Option C is similar to B but lacks the explicit segment action specification. Option D lacks the scalability and isolation capabilities needed for future expansion.

https://zhangxuetu.online

[202610]

Question #183 Topic 1

A company has an AWS Site-to-Site VPN connection between AWS and its branch office. A network engineer is troubleshooting connectivity issues that the connection is experiencing. The VPN connection terminates at a transit gateway and is statically routed. In the transit gateway route table, there are several static route entries that target specific subnets at the branch office.

The network engineer determines that the root cause of the issues was the expansion of underlying subnet ranges in the branch office during routine maintenance.

Which solution will solve this problem with the LEAST administrative overhead for future expansion efforts?

A. Determine a supernet for the branch office. In the transit gateway route table, add an aggregate route that targets the VPN attachment. Replace the specific subnet routes in the transit gateway route table with the new supernet route.

B. Create an AWS Direct Connect gateway and a transit VIF. Associate the Direct Connect gateway with the transit gateway. Create a propagation for the Direct Connect attachment to the transit gateway route table.

C. Create a dynamically routed VPN connection on the transit gateway. Connect the dynamically routed VPN connection to the branch office. Create a propagation for the VPN attachment to the transit gateway route table. Remove the existing static VPN connection. **Most Voted**

D. Create a prefix list that contains the new subnets and the old subnets for the branch office. Remove the specific subnet routes in the transit gateway route table. Create a prefix list reference in the transit gateway route table.

Correct Answer: C

Community vote distribution



Comments

Kupaloid **Highly Voted** 1 year, 10 months ago

Selected Answer: C

Move from static to dynamic routing to remove administrative overhead

TechAwesome 1 year ago

Selected Answer: D

D is correct. A for sure is wrong. The on-premises could expand it's network with a different RFC1918 subnet. For C, you need to build another connection.

AzureDP900 1 year, 2 months ago

Selected Answer: C

Here's why: Option C: This solution involves creating a dynamically routed VPN connection on the transit gateway and connecting it to the branch office. It then creates a propagation for the VPN attachment to the transit gateway route table. After that, it removes the existing static VPN connection.

woorkim 1 year, 3 months ago

Selected Answer: C

A: Using a supernet (aggregate route) can work if the branch office subnets fit neatly within a single supernet. However, if future expansions include subnets outside the supernet, manual updates will still be required. This does not fully solve the problem of minimizing administrative overhead. B: While AWS Direct Connect offers high bandwidth and low latency, it is unnecessary for addressing the root cause (static route updates). It also involves additional costs and complexity. D: A prefix list simplifies management compared to individual static routes, but it still requires manual updates whenever new subnets are added or existing ones change. This does not eliminate administrative overhead as effectively as dynamic routing.

Spaurito 1 year, 4 months ago

C - Let dynamic routing do the work. Static routes are operational overhead.

6cae226 1 year, 6 months ago

Selected Answer: A

The solution that provides the LEAST administrative overhead for future expansion efforts is Option A. By determining a supernet and using an aggregate route, you can significantly reduce the need for future updates to the Transit Gateway route table as the branch office network expands. This approach ensures that as long as the expansion stays within the defined supernet, no further route updates will be necessary.

rltk8029 1 year, 11 months ago

Why not C? Site-to-Site VPN config lets use BGP. As a traditional network engineer I'd always prefer dynamic routing.

973b658 1 year, 11 months ago

Selected Answer: A

it is A.

JoellaLi 1 year, 11 months ago

Selected Answer: D

You can reference a prefix list in your transit gateway route table. A prefix list is a set of one or more CIDR block entries that you define and manage. You can use a prefix list to simplify the management of the IP addresses that you reference in your resources to route network traffic. For example, if you frequently specify the same destination CIDRs across multiple transit gateway route tables, you can manage those CIDRs in a single prefix list, instead of repeatedly referencing the same CIDRs in each route table. If you need to remove a destination CIDR block, you can remove its entry from the prefix list instead of removing the route from every affected route table. When you create a prefix list reference in your transit gateway route table, each entry in the prefix list is represented as a route in your transit gateway route table.

Kayceetalks 2 years ago

A - Correct

psou7 2 years ago

I vote C

https://zhangxuetu.online

[202610]

Question #184 Topic 1

An education agency is preparing for its annual competition between schools. In the competition, students at schools from around the country solve math problems, complete puzzles, and write essays.

The IP addressing plan of all the schools is well-known and is administered centrally. The competition is hosted in the AWS Cloud and is not publicly available. All competition traffic must be encrypted in transit. Only authorized endpoints can access the competition. All the schools have firewall policies that block ICMP traffic.

A network engineer builds a solution in which all the schools access the competition through AWS Site-to-Site VPN connections. The network engineer uses BGP as the routing protocol. The network engineer must implement a solution that notifies schools when they lose connectivity and need to take action on their premises to address the issue.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

A. Monitor the state of the VPN tunnels by using Amazon CloudWatch. Create a CloudWatch alarm that uses Amazon Simple Notification Service (Amazon SNS) to notify people at the affected school if the tunnels are down. **Most Voted**

B. Create a scheduled AWS Lambda function that pings each school's on-premises customer gateway device. Configure the Lambda function to send an Amazon Simple Notification Service (Amazon SNS) notification to people at the affected school if the ping fails.

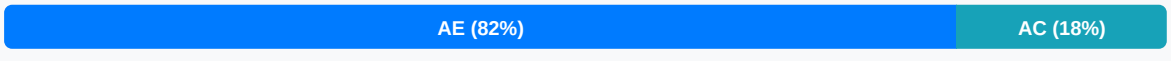
C. Create a scheduled AWS Lambda function that uses the VPC Reachability Analyzer API to verify the connectivity. Configure the Lambda function to send an Amazon Simple Notification Service (Amazon SNS) notification to people at the affected school if failure occurs.

D. Create an Amazon CloudWatch dashboard for each school to show all CloudWatch metrics for each school's Site-to-Site VPN connection. Share each dashboard with the appropriate school.

E. Create a scheduled AWS Lambda function to monitor the existence of each school's routes in the VPC route table where VPN routes are propagated. Configure the Lambda function to send an Amazon Simple Notification Service (Amazon SNS) notification to people at the affected school if failure occurs. **Most Voted**

Correct Answer: AE

Community vote distribution



Comments

seochan Highly Voted 1 year, 10 months ago

Selected Answer: AE

I think it's AE. Option B is not possible because the clients are blocking ICMP protocol. Option C is not cost-effective option because the VPC reachability analyzer has per-invoke cost. Option D is not a requirement in this scenario.

woorkim 1 year, 3 months ago

Selected Answer: AE

B: Pinging customer gateway devices is not viable since the schools block ICMP traffic. This option would fail due to the schools' firewall policies. C: While VPC Reachability Analyzer is a powerful tool, using it for frequent connectivity checks is more complex and potentially costlier than leveraging existing metrics and route table monitoring. D: CloudWatch dashboards are useful for monitoring but do not provide proactive notifications. They require someone to manually review the data, which does not align with the requirement for automated notifications.

Spaurito 1 year, 4 months ago

AE - This seems to be the best answer. You could use option C but the cost would add up. Monitoring the Route Table and having a CloudWatch monitor makes the most sense.

cas_tori 1 year, 6 months ago

Selected Answer: AE

this is AE

973b658 1 year, 11 months ago

Selected Answer: AC

A&C is OK.

https://zhangxuetu.online

[202610]

Question #185 Topic 1

A company securely connects resources that are in its VPC to a software as a service (SaaS) solution from a SaaS provider. The SaaS solution is hosted in the AWS Cloud and is powered by AWS PrivateLink. The company uses a PrivateLink endpoint to access the SaaS solution behind the SaaS provider's Network Load Balancer (NLB).

The company recently added a new Availability Zone and new subnets to its VPC. A network engineer is unable to deploy a new interface VPC endpoint for the SaaS solution in the new Availability Zone.

What is the cause of this problem?

A. The CIDR block of the new subnets conflicts with the SaaS provider's CIDR block.

B. The enableDnsHostnames attribute and enableDnsSupport attribute were not configured on the new subnets in the new Availability Zone.

C. The SaaS provider does not offer the solution in the new Availability Zone and has not configured cross-zone load balancing for the NLB. **Most Voted**

D. The new subnets are missing a route to the VPC internet gateway.

Correct Answer: C

Community vote distribution

C (100%)

Comments

woorkim 1 year, 3 months ago

C is right! A: CIDR block conflicts are not relevant here, as PrivateLink operates at the network interface level and is independent of the CIDR block configuration of the VPC. B: The enableDnsHostnames and enableDnsSupport attributes are required for DNS resolution of private endpoints, but their absence would not block the creation of an endpoint in a specific Availability Zone. D: The new subnets do not need a route to an internet gateway to use AWS PrivateLink, as it operates within the AWS network and does not rely on public internet routing.

cas_tori 1 year, 6 months ago

Selected Answer: C

this is C

Akshay0403 1 year, 8 months ago

Selected Answer: C

AWS PrivateLink endpoints require the service to be available in the Availability Zone where the endpoint is being created. If the SaaS provider does not offer the service in the new Availability Zone and cross-zone load balancing is not configured for the NLB, the endpoint cannot be deployed in that Availability Zone. This is a likely cause of the problem because the endpoint creation depends on the service being present and accessible in the desired Availability Zone.

rdiaz 1 year, 9 months ago

Selected Answer: C

https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/creating-highly-available-endpoint-services.html

https://zhangxuetu.online

[202610]

Question #186 Topic 1

A company wants to use an AWS Network Firewall firewall to secure its workloads in the cloud through network traffic inspection. The company must record complete metadata information, such as source/destination IP addresses and protocol type. The company must also record all network traffic flows and any DROP or ALERT actions that the firewall takes for traffic that the firewall processes. The Network Firewall endpoints are placed in the correct subnets, and the VPC route tables direct traffic to the Network Firewall endpoints on the path to and from the internet.

How should a network engineer configure the firewall to meet these requirements?

A. Create a firewall policy to ensure that traffic is processed by stateless or stateful rules according to needs. Select Amazon CloudWatch Logs as the destination for the flow logs.

B. Create a firewall policy to ensure that traffic is processed by stateless or stateful rules according to needs. Configure Network Firewall logging for alert logs and flow logs.
Select a destination for logs separately for stateful and stateless engines.

C. Create a firewall policy to ensure that a stateful engine processes all the traffic. Configure Network Firewall logging for alert logs and flow logs. Select a destination for alert logs and flow logs. Most Voted

D. Create a firewall policy to ensure that a stateful engine processes all the traffic. Configure VPC flow logs for the subnets that the firewall protects. Select a destination for the flow logs.

Correct Answer: C

Community vote distribution



Comments

c1193d4 Highly Voted 1 year, 2 months ago

Selected Answer: C

Firewall logging is only available for traffic that you forward to the stateful rules engine.

46f094c 1 year, 4 months ago

Selected Answer: C

B doesn't mention the "engine". "...Firewall logging is only available for traffic that you forward to the stateful rules engine..." so no engine, no logging

Spaurito 1 year, 4 months ago

B - You can configure AWS Network Firewall logging for your firewall's stateful engine. Logging gives you detailed information about network traffic, including the time that the stateful engine received a packet, detailed information

about the packet, and any stateful rule action taken against the packet. The logs are published to the log destination that you've configured, where you can retrieve and view them. This meets the requirements best.

Spaurito 1 year, 4 months ago

Here is a demo of the Network Firewall Dashboard. Defines the separate logging for Stateful and Stateless.

seongheon 1 year, 6 months ago

Selected Answer: C

C : Firewall logging is only available for traffic that you forward to the stateful rules engine. You forward traffic to the stateful engine through stateless rule actions and stateless default actions in the firewall policy.

arturogomezb 1 year, 9 months ago

Firewall logging is only available for traffic that you forward to the stateful rules engine. You forward traffic to the stateful engine through stateless rule actions and stateless default actions in the firewall policy. For information about these actions settings, https://docs.aws.amazon.com/network-firewall/latest/developerguide/firewall-logging.html

luisgu 1 year, 6 months ago

so, correct answer is C; option B cannot guarantee the traffic is processed by the stateful engine

acloudguru 1 year, 10 months ago

Selected Answer: B

Option D: Using VPC Flow Logs would capture network traffic flows, but it would not capture the specific DROP or ALERT actions taken by the AWS Network Firewall. Additionally, VPC Flow Logs do not provide the same level of detail and metadata as the Network Firewall flow logs

JoellaLi 1 year, 11 months ago

Selected Answer: B

You can configure AWS Network Firewall logging for your firewall's stateful engine. Logging gives you detailed information about network traffic, including the time that the stateful engine received a packet, detailed information about the packet, and any stateful rule action taken against the packet. The logs are published to the log destination that you've configured, where you can retrieve and view them.

JoellaLi 1 year, 11 months ago

You can record flow logs and alert logs from your Network Firewall stateful engine. • Flow logs are standard network traffic flow logs. Each flow log record captures the network flow for a specific standard stateless rule group. • Alert logs report traffic that matches your stateful rules that have an action that sends an alert. A stateful rule sends alerts for the rule actions DROP, ALERT, and REJECT.

KobDragoon 1 year, 11 months ago

Selected Answer: B

B is the right answer, not all traffic needs to be processed by the stateful engine like C suggests

Spaurito 1 year, 4 months ago

Actually, the requirement states, "record all network traffic flows". This would lead to need both Stateful and Stateless engines.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #187 Topic 1

A company is building a new workload on AWS that uses an Application Load Balancer (ALB). The company has configured a new ALB target group that uses slow start mode. A team begins registering Amazon EC2 instances as targets in the new target group. During testing, the team observes that the targets did not enter slow start mode.

What caused the targets to not enter slow start mode?

A. The ALB configuration uses the round robin routing algorithm for traffic.

B. The target group did not contain at least one healthy target configured in slow start mode. Most Voted

C. The target group must contain EC2 instances that are all the same instance type.

D. The ALB configuration uses the 5-tuple criteria for traffic.

Correct Answer: B

Community vote distribution

B (100%)

Comments

billgoldberg14 Highly Voted 1 year, 11 months ago

Selected Answer: B

Looks like the answer is B according to this link: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#slow-start-mode " When you enable slow start for an empty target group and then register targets using a single registration operation, these targets do not enter slow start mode. Newly registered targets enter slow start mode only when there is at least one healthy target that is not in slow start mode."

woorkim 1 year, 3 months ago

Selected Answer: B

When you enable slow start for an empty target group and then register targets using a single registration operation, these targets do not enter slow start mode. Newly registered targets enter slow start mode only when there is at least one healthy target that is not in slow start mode.

cas_tori 1 year, 6 months ago

Selected Answer: B

this is B

https://zhangxuetu.online

[202610]

Question #188 Topic 1

A network engineer is using AWS Direct Connect connections and MACsec to encrypt data from a corporate data center to the Direct Connect location. The network engineer learns that the MACsec secret key might have been compromised. The network engineer needs to update the connection with an uncompromised secure key.

Which solution will meet this requirement?

A. Create a new MACsec secret key that uses an AWS Key Management Service (AWS KMS) AWS managed key. Associate the new pre-shared key, Connection Key Name (CKN), and Connectivity Association Key (CAK) with the connection.

B. Create a new MACsec secret key that uses an AWS Key Management Service (AWS KMS) customer managed key. Associate the new pre-shared key, Connection Key Name (CKN), and Connectivity Association Key (CAK) with the connection. **Most Voted**

C. Modify the existing MACsec secret key. Re-associate the existing pre-shared key, Connection Key Name (CKN), and Connectivity Association Key (CAK) with the connection.

D. Modify the existing MACsec secret key. Associate the new pre-shared key, Connection Key Name (CKN), and Connectivity Association Key (CAK) with the connection.

Correct Answer: B

Community vote distribution

B (100%)

Comments

KobDragoon Highly Voted 1 year, 11 months ago

Selected Answer: B

You cannot modify a MACsec secret key after you associate it with a connection. If you need to modify the key, disassociate the key from the connection, and then associate a new key with the connection.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/associate-key-connection.html

cas_tori 1 year, 6 months ago

Selected Answer: B

this is B

veyisceylan 1 year, 9 months ago

MACsec pre-shared CKN/CAK key considerations AWS Direct Connect uses AWS managed CMKs for the pre-shared keys that you associate with connections or LAGs. Secrets Manager stores your pre-shared CKN and CAK pairs as a

secret that the Secrets Manager’s root key encrypts. For more information, see AWS managed CMKs in the AWS Key Management Service Developer Guide.

94b9222 7 months ago

Exactly, its says AWS Managed CMKs, thats why it should be the option A, not B.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #189 Topic 1

A network engineer configures a second AWS Direct Connect connection to an existing network. The network engineer runs a test in the AWS Direct Connect Resiliency Toolkit on the connections. The test produces a failure. During the failover event, the network engineer observes a 90-second interruption before traffic shifts to the failover connection.

Which solution will reduce the time for failover?

A. Decrease the BGP hello timer to 5 seconds.

B. Add a VPN connection to the connectivity solution. Implement fast failover.

C. Configure Bidirectional Forwarding Detection (BFD) on the on-premises router. **Most Voted**

D. Decrease the BGP hold-down timer to 5 seconds.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Akshay0403 **Highly Voted** 1 year, 8 months ago

Selected Answer: C

The most effective solution to reduce the failover time in this scenario is option C, configuring Bidirectional Forwarding Detection (BFD) on the on-premises router. BFD provides rapid failure detection and is commonly used in conjunction with BGP to achieve faster failover times in network connections like AWS Direct Connect.

KobDragoon 1 year, 11 months ago

Selected Answer: C

C is the right answer for quicker failover

https://zhangxuetu.online

[202610]

Question #190 Topic 1

A company is building an API-based application on AWS and is using a microservices architecture for the design. The company is using a multi-account AWS environment that includes a separate AWS account for each microservice development team. Each team hosts its microservice in its own VPC that contains Amazon EC2 instances behind a Network Load Balancer (NLB).

A network engineer needs to use Amazon API Gateway in a shared services account to create an HTTP API to expose these microservices to external applications. The network engineer must ensure that access to the microservices can occur only over a private network. Additionally, the company must be able to control which entities from its internal network can connect to the microservices. In the future, the company will create more microservices that the company must be able to integrate with the application.

What is the MOST secure solution that meets these requirements?

A. Create an Application Load Balancer (ALB) in a VPC in the shared services account. Configure the integration to the API Gateway API by using a VPC link. Associate the VPC link with the ALB. Create a VPC endpoint service in each microservice account. Create an AWS PrivateLink endpoint for those services in the shared services account. Add the elastic network interface IP addresses of the VPC endpoint as targets for the target group of the ALB. **Most Voted**

B. Create an Application Load Balancer (ALB) in a VPC in the shared services account. Configure the integration to the API Gateway API by using a VPC link. Associate the VPC link with the ALConnect all the VPCs to each other by using a central transit gateway. Add the IP addresses of the NLB as IP-based targets in the ALB target group.

C. Configure the integration to the API Gateway API by using HTTP-based integration. Connect all the VPCs to each other by using a central transit gateway. Create a separate HTTP integration to each NLB for each microservice. Add the HTTP endpoint of the NLB as the endpoint URL in the HTTP integration.

D. Configure the integration to the API Gateway API by using VPC link integration. Connect all the VPCs to each other by using a central transit gateway. Create a separate VPC link to each NLB for each microservice. Add the HTTP endpoint of the NLB as the endpoint URL in the VPC link integration.

Correct Answer: A

Community vote distribution



Comments

seochan Highly Voted 1 year, 9 months ago

Selected Answer: A

I think it's A VPC link - ensure using private network VPC endpoint service - scalable and secure (TGW need non-overlapping CIDR, hence no scalable, and you can access control using ENI SG)

c1193d4 1 year, 2 months ago

Selected Answer: A

D: incorrect because the API Gateway won't be able to reach the NLBs located in microservices accounts through the VPC Link created in the shared VPC account "To create a private integration, all resources must be owned by the same AWS account (including the load balancer or AWS Cloud Map service, VPC link and HTTP API)." in https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-develop-integrations-private.html

46f094c 1 year, 2 months ago

If using PrivateLink there is no need for a TGW

luisgu 1 year, 6 months ago

Selected Answer: A

See "Private integration cross-account" on this link: https://docs.aws.amazon.com/whitepapers/latest/best-practices-api-gateway-private-apis-integration/http-api.html

Spaurito 1 year, 4 months ago

I see your thought here but the environment already has NLB's in place for the EC2 instances.

Ravan 1 year, 7 months ago

Selected Answer: A

D. Incorrect VPC link configuration: The VPC link should be associated with the ALB, not the NLB.

siheom 1 year, 7 months ago

Selected Answer: D

VOTE D

kupo777 1 year, 7 months ago

D is correct. A, B: HTTP API does not require ALB creation on the shared account side because the communication is to ENI. C: HTTP-based integration does not exist.

Akshay0403 1 year, 8 months ago

Selected Answer: D

Option D is the most secure and scalable solution. It provides private network communication using VPC link integration and leverages a transit gateway for efficient VPC management. This approach ensures that traffic remains secure within the AWS network while offering the flexibility to control access and easily integrate new microservices in the future.

jfedotov 1 year, 1 month ago

it's not, "Connect all the VPCs to each other by using a central transit gateway". There is no requirement to connect whole VPCs, it is not secure.

yeahaya 1 year, 9 months ago

Selected Answer: D

D. i choice

yeahaya 1 year, 9 months ago

D. i choice

rdiaz 1 year, 9 months ago

Selected Answer: B

TGW required.

https://zhangxuetu.online

[202610]

Question #191 Topic 1

A company's VPC has Amazon EC2 instances that are communicating with AWS services over the public internet. The company needs to change the connectivity so that the communication does not occur over the public internet.

The company deploys AWS PrivateLink endpoints in the VPC. After the deployment of the PrivateLink endpoints, the EC2 instances can no longer communicate at all with the required AWS services.

Which combination of steps should a network engineer take to restore communication with the AWS services? (Choose two.)

A. In the VPC route table, add a route that has the PrivateLink endpoints as the destination.

B. Ensure that the enableDnsSupport attribute is set to True for the VPC. Ensure that each VPC endpoint has DNS support enabled. Most Voted

C. Ensure that the VPC endpoint policy allows communication. Most Voted

D. Create an Amazon Route 53 public hosted zone for all services.

E. Create an Amazon Route 53 private hosted zone that includes a custom name for each service.

Correct Answer: BC

Community vote distribution

BC (100%)

Comments

woorkim 1 year, 3 months ago

Selected Answer: BC

A is incorrect: Adding routes to the PrivateLink endpoints in the route table is not necessary for endpoint communication D is incorrect: Creating a public hosted zone is not the right approach for private connectivity E is incorrect: While private hosted zones can be useful, they are not directly required to restore PrivateLink endpoint communication

Akshay0403 1 year, 8 months ago

Selected Answer: BC

The most effective steps are B and C. Ensuring that DNS support is enabled for both the VPC and the PrivateLink endpoints, along with verifying that the VPC endpoint policy permits the required access, will restore the necessary communication between the EC2 instances and the AWS services over the private network. These steps ensure that the services are correctly resolved and accessible while maintaining security and privacy through the AWS network.

seochan 1 year, 9 months ago

Selected Answer: BC

A. This is not a VPC Gateway Endpoint. B. You need to use AmazonProvidedDNS, so this is doable option. C. VPC endpoint policy might block the connection, so possible cause. D & E. You don't need to use the R53 Hosted Zone for this scenario.

https://zhangxuetu.online

[202610]

Question #192 Topic 1

An international company wants to implement a multi-site hybrid infrastructure. The company wants to deploy its cloud computing resources on AWS in the us-east-1 Region and in the eu-west-2 Region, and in on-premises data centers in the United States (US) and in the United Kingdom (UK). The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through BGP. The company wants to have two AWS Direct Connect connections, one each in the US and the UK.

The company expects to have 15 VPCs in each Region with CIDR blocks that do not overlap with each other or with CIDR blocks of the on-premises environment. The VPC CIDR blocks are planned so that the prefix aggregation can be performed both on a Regional level and across the entire AWS environment. The company will deploy a transit gateway in each Region to connect the VPCs. A network engineer plans to use a Direct Connect gateway in each Region. A transit VIF will attach the Direct Connect gateway in each Region to the transit gateway in that Region. The transit gateways will be peered with each other.

The network engineer wants to ensure that traffic follows the shortest geographical path from source to destination. Traffic between the on-premises data centers and AWS must travel across a local Direct Connect connection. Traffic between the US data center and eu-west-2 and traffic between the UK data center and us-east-1 must use the private WAN connection to reach the Direct Connect connection to the appropriate Region when the Direct Connect connection is available. The network must be resilient to failures in either the private WAN connection or with the Direct Connect connections. The network also must reroute traffic automatically in the event of any failure.

How should the network engineer configure the transit VIF associations on the Direct Connect gateways to meet these requirements?

A. Advertise only the aggregate route for the company's entire AWS environment.

B. Advertise VPC-specific CIDR prefixes from only the local Region. Additionally, advertise the aggregate route for the company's entire AWS environment. **Most Voted**

C. Advertise all the specific VPC CIDR blocks from both Regions.

D. Advertise both Regional aggregate prefixes. Configure custom BGP communities on the routes advertised toward the data center.

Correct Answer: B

Community vote distribution



Comments

strike3test Highly Voted 1 year, 9 months ago

Selected Answer: B

To meet the requirements of ensuring traffic follows the shortest geographical path, using the private WAN connection when Direct Connect is unavailable, and ensuring resilience to failures, the network engineer should configure the transit VIF associations on the Direct Connect gateways as follows: B. Advertise VPC-specific CIDR prefixes from only the local Region. Additionally, advertise the aggregate route for the company's entire AWS environment. This option allows for the most efficient routing by advertising VPC-specific CIDR prefixes from the local Region, ensuring traffic takes the shortest path within the AWS network. Additionally, advertising the aggregate route for the entire AWS environment ensures that in case of any failures or unavailability of Direct Connect connections, traffic can still reach its destination via other available paths, such as the private WAN connection.

steli0 5 months, 2 weeks ago

Selected Answer: B

Another reason on why D is wrong is that just advertising the communities in the DCs routers it won't affect traffic and routing decissions. Further configuration at on-prem (route-maps and actions to modify weight or local preference) is needed.

youonebe 1 year ago

Selected Answer: D

Answer is D

woorkim 1 year, 3 months ago

Selected Answer: B

The other options have drawbacks: Option A: Too limited, doesn't provide granular routing information Option C: Too verbose, increases routing complexity Option D: While it uses BGP communities, it doesn't optimize routing as effectively as

cas_tori 1 year, 6 months ago

Selected Answer: B

this is B

siheom 1 year, 7 months ago

Selected Answer: D

VOTE D

https://zhangxuetu.online

[202610]

Question #193 Topic 1

A company's AWS infrastructure is spread across more than 50 accounts and across five AWS Regions. The company needs to manage its security posture with simplified administration and maintenance for all the AWS accounts. The company wants to use AWS Firewall Manager to manage the firewall rules and requirements.

The company creates an organization with all features enabled in AWS Organizations.

Which combination of steps should the company take next to meet the requirements? (Choose three.)

A. Configure only the Firewall Manager administrator account to join the organization.

B. Configure all the accounts to join the organization. Most Voted

C. Set an account as the Firewall Manager administrator account. Most Voted

D. Set an account as the Firewall Manager child account.

E. Set up AWS Config for all the accounts and all the Regions where the company has resources. Most Voted

F. Set up AWS Config for only the organization's management account.

Correct Answer: BCE

Community vote distribution

BCE (100%)

Comments

rdiaz Highly Voted 1 year, 9 months ago

Selected Answer: BCE

All accounts, firewall parent and aws config in all accounts.

AzureDP900 1 year, 2 months ago

Selected Answer: BCE

Option B ensures that all 50+ AWS accounts are under the same management, making it easier to manage security posture. Option C sets up an administrator account within one of these accounts, which can manage all Firewall Manager configurations across the organization. Option E enables centralized monitoring and compliance for resources across all Regions, allowing the company to maintain consistency in their AWS security posture.

woorkim 1 year, 3 months ago

Selected Answer: BCE

Pre-requisites for Firewall Manager • Enable AWS Organization (full features) • Enable AWS Config • Enable AWS Resource Access Manager (RAM)

cas_tori 1 year, 6 months ago

Selected Answer: BCE

this is BCE

https://zhangxuetu.online

[202610]

Question #194 Topic 1

A company is using an Amazon CloudFront distribution that is configured with an Application Load Balancer (ALB) as an origin. A network engineer needs to implement a solution that requires all inbound traffic to the ALB to come from CloudFront. The network engineer must implement the solution at the network layer rather than in the application.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Add an inbound rule to the ALB's security group to allow the AWS managed prefix list for CloudFront. **Most Voted**

B. Add an inbound rule to the network ACLs that are associated with the ALB's subnets. Use the AWS managed prefix list for CloudFront as the source in the rule.

C. Configure CloudFront to add a custom HTTP header to the requests that CloudFront sends to the ALB.

D. Associate an AWS WAF web ACL with the ALB. Configure the AWS WAF rules to allow traffic from the CloudFront IP set. Automatically update the CloudFront IP set by using an AWS Lambda function.

Correct Answer: A

Community vote distribution



Comments

veyisceylan **Highly Voted** 1 year, 9 months ago

It is asking a solution at network layer rather than application layer. Therefore it is A in my opinion. A managed prefix list is a set of one or more CIDR blocks. You can use prefix lists to make it easier to configure and maintain your security groups and route tables.

AzureDP900 1 year, 2 months ago

Selected Answer: A

A is right Adding an inbound rule to the ALB's security group to allow the AWS managed prefix list for CloudFront ensures that only traffic coming from CloudFront is allowed to reach the ALB. This meets the requirement of having all inbound traffic to the ALB come from CloudFront.

woorkim 1 year, 3 months ago

Selected Answer: A

AWS Managed Prefix List for CloudFront: AWS provides a managed prefix list that includes the IP ranges for CloudFront edge locations. By using this list in the ALB's security group, the network engineer can restrict access to only traffic originating from CloudFront without manually managing IP ranges. Operational Efficiency: This approach is

operationally efficient because: The managed prefix list is automatically updated by AWS whenever CloudFront's IP ranges change. Security groups are simple to configure and maintain compared to other options like network ACLs or AWS WAF.

Spaurito 1 year, 4 months ago

C - This defines the solution https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html

Spaurito 1 year, 4 months ago

Have to change my answer to "A". A defined for the network layer requirement.

Akshay0403 1 year, 8 months ago

Selected Answer: A

Option A is the most operationally efficient solution as it leverages AWS managed prefix lists, ensuring up-to-date and secure traffic management to the ALB from CloudFront. Security groups provide a straightforward way to enforce network layer restrictions without additional administrative overhead or application changes. This aligns well with the requirement to implement a solution strictly at the network layer.

Blitz1 1 year, 8 months ago

Selected Answer: A

A because is saying at network layer. https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/

rdiaz 1 year, 9 months ago

Selected Answer: C

cloudfront header and alb condition

AXH 1 year, 9 months ago

Voting for C.

https://zhangxuetu.online

[202610]

Question #195 Topic 1

A company has AWS accounts in an organization in AWS Organizations. The company has implemented Amazon VPC IP Address Manager (IPAM) in its networking AWS account. The company is using AWS Resource Access Manager (AWS RAM) to share IPAM pools with other AWS accounts. The company has created a top-level pool with a CIDR block of 10.0.0.0/8. For each AWS account, the company has created an IPAM pool within the top-level pool.

A network engineer needs to implement a solution to ensure that users in each AWS account cannot create new VPCs. The solution also must prevent users from associating a CIDR block with existing VPCs unless the CIDR block is from the IPAM pool for that account.

Which solution will meet these requirements?

A. Create a new AWS Config rule to find all VPCs that are not configured to allocate their CIDR block from an IPAM pool. Invoke an AWS Lambda function to delete these VPCs.

B. Create a new SCP in Organizations. Add a condition that denies the CreateVpc and AssociateVpcCidrBlock Amazon EC2 actions if the Ipv4IpamPoolId context key value is not the ID of an IPAM pool. **Most Voted**

C. Create an AWS Lambda function to check for and delete all VPCs that are not configured to allocate their CIDR block from an IPAM pool. Invoke the Lambda function at regular intervals.

D. Create an Amazon EventBridge rule to check for AWS CloudTrail events for the CreateVpc and AssociateVpcCidrBlock Amazon EC2 actions. Use the rule to invoke an AWS Lambda function to delete all VPCs that are not configured to allocate their CIDR block from an IPAM pool.

Correct Answer: B

Community vote distribution



Comments

AzureDP900 1 year, 2 months ago

Selected Answer: B

Option B meets all of the requirements with least operational overhead: It creates a new SCP in Organizations that denies the CreateVpc and AssociateVpcCidrBlock Amazon EC2 actions if the Ipv4IpamPoolId context key value is not the ID of an IPAM pool. The SCP will prevent users from creating VPCs without the correct CIDR block. It prevents users from associating a CIDR block with existing VPCs unless the CIDR block is from the IPAM pool for that account.

woorkim 1 year, 3 months ago

Selected Answer: B

AWS Organization Service control policy (SCP) to enforce CIDR allocation through IPAM while creating VPCs • Enforce using specific IPAM pools • Enforce specific IPAM pools to specific OUs

Spaurito 1 year, 4 months ago

B - This meets the requirements, although option A would as well. Only issue with option A, is the deletion of VPC's. Doesn't mention removing or reclaiming existing IP's.

Akshay0403 1 year, 8 months ago

Selected Answer: B

Option B is the most effective and efficient solution because it proactively prevents non-compliant actions at the organization level, enforcing a strict policy that ensures VPC creation and CIDR block associations are limited to IPAM pools. By leveraging SCPs, you can maintain control over your network architecture, ensuring all resources comply with predefined security and operational guidelines.

strike3test 1 year, 9 months ago

Selected Answer: B

The most suitable option for enforcing the policy at the point of action (creating or associating CIDR blocks) across all AWS accounts in the organization is option B. Therefore, the correct answer is: B. Create a new SCP in Organizations. Add a condition that denies the CreateVpc and AssociateVpcCidrBlock Amazon EC2 actions if the Ipv4IpamPoolId context key value is not the ID of an IPAM pool.

rdiaz 1 year, 9 months ago

Selected Answer: A

aws config

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #196 Topic 1

A company has an application that runs on premises. The application needs to communicate with an application that runs in a VPC on AWS. The communication between the applications must be encrypted and must use private IP addresses. The communication cannot travel across the public internet.

The company has established a 1 Gbps AWS Direct Connect connection between the on-premises location and AWS.

Which solution will meet the connectivity requirements with the LEAST operational overhead?

A. Configure a private VIF on the Direct Connect connection. Associate the private VIF with the VPC's virtual private gateway. Set up an AWS Site-to-Site VPN private IP VPN connection to the virtual private gateway.

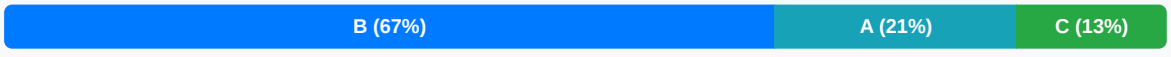
B. Create a transit gateway. Configure a transit VIF on the Direct Connect connection. Associate the transit VIF with a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway. Set up an AWS Site-to-Site VPN private IP VPN connection to the transit gateway. **Most Voted**

C. Configure a public VIF on the Direct Connect connection. Associate the public VIF with a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway. Set up an AWS Site-to-Site VPN private IP VPN connection to the transit gateway.

D. Create a transit gateway. Configure a transit VIF on the Direct Connect connection. Associate the transit VIF with a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway. Set up a third-party firewall in a new VPC that is attached to the transit gateway. Set up a VPN connection to the third-party firewall.

Correct Answer: B

Community vote distribution



Comments

vic614 **Highly Voted** 1 year, 9 months ago

Selected Answer: A

Least operational overhead. No need for a transit gateway since just 1 vpc. Use Site-to-site to make sure encryption. No public VIF.

chang4li 1 year, 2 months ago

Private VIF good enough when u have Direct Connect connection

ankit_agarwal 2 months, 3 weeks ago

It is should be private vif because questions says LEAST operational overhead. using Transit Gateway and Direct Connect gateway and VPN is lot of overheads

ankit_agarwal 2 months, 3 weeks ago

Scratch that, B is appropriate because S2S VPN can't be established on Private vif

AzureDP900 1 year, 2 months ago

Selected Answer: B

Option B meets all of the requirements with least operational overhead: It uses a transit gateway and a transit VIF on the Direct Connect connection. Associating the transit VIF with a Direct Connect gateway ensures that communication between the Direct Connect connection and the AWS infrastructure is secure. The transit gateway can be associated with a new transit gateway, which allows data to flow between sites while maintaining security and meeting requirements. It sets up an AWS Site-to-Site VPN private IP VPN connection to the transit gateway.

Nel07 1 year, 5 months ago

Selected Answer: B

https://docs.aws.amazon.com/vpn/latest/s2svpn/private-ip-dx.html

AlirezaNetWorld 1 year, 6 months ago

C is the correct answer. Establishing IPsec is only permitted over the Public VIF, but this doesn't mean traffic is transmitted over the public Internet as all traffic will be sent and received between the on-prem and AWS across the DX line which is considered as a private link.

Akshay0403 1 year, 8 months ago

Selected Answer: B

Option B is the most operationally efficient solution that meets all requirements: Encrypted Communication: The AWS Site-to-Site VPN connection provides encryption. Private IP Addresses: The transit VIF and Direct Connect gateway ensure private IP connectivity. Least Operational Overhead: By using the transit gateway and Direct Connect's transit VIF, the solution simplifies network management and minimizes operational complexity.

Blitz1 1 year, 8 months ago

Selected Answer: B

A - you cannot have s2s vpn with private vif. You need public -> A fail C - can you can have 2s2 vpn with public vif but you cannot have in the same time trasit vif(because is mentioning transit gateway) and public vif associated with direct connect gateway -> C fail D - third party vpn -> not LEAST operational overhead -> D fail

chrootxxx 1 year, 3 months ago

https://docs.aws.amazon.com/vpn/latest/s2svpn/private-ip-dx.html

veyisceylan 1 year, 9 months ago

To build Site-to-Site VPN over Direct Connect to Amazon VPC, use a public virtual interface. To build Site-to-Site VPN between on-premises equipment and AWS Transit Gateway, choose a public or a transit virtual interface. It should be B with Transit Gateway and Private IP VPN

tsangckl 1 year, 9 months ago

Selected Answer: C

Site-to-site VPN have to be created over public VIF

kajiyatta 1 year, 8 months ago

The communication between the applications must be encrypted and must use private IP addresses.So,public vif can not used.

strike3test 1 year, 9 months ago

Selected Answer: B

Private VIFs are used to establish private connectivity between your on-premises network and your VPCs in AWS without traversing the public internet. They are typically used for scenarios where you need dedicated, private communication between your on-premises infrastructure and your AWS resources. However, to establish a Site-to-Site VPN connection, you need to configure a virtual private gateway (VGW) in your VPC. The VGW acts as the VPN endpoint in the AWS cloud. Site-to-Site VPN connections are established between the VGW and your on-premises VPN device or network. Option B is correct

AXH 1 year, 9 months ago

Agree, A is least overhead to implement.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #197 Topic 1

A company has established connectivity between its on-premises data center in Paris. France, and the AWS Cloud by using an AWS Direct Connect connection. The company uses a transit VIF that connects the Direct Connect connection with a transit gateway that is hosted in the Europe (Paris) Region. The company hosts workloads in private subnets in several VPCs that are attached to the transit gateway.

The company recently acquired another corporation that hosts workloads on premises in an office building in Tokyo, Japan. The company needs to migrate the workloads from the Tokyo office to AWS. These workloads must have access to the company's existing workloads in Paris. The company also must establish connectivity between the Tokyo office building and the Paris data center.

In the Asia Pacific (Tokyo) Region, the company creates a new VPC with private subnets for migration of the workloads. The workload migration must be completed in 5 days. The workloads cannot be directly accessible from the internet.

Which set of steps should a network engineer take to meet these requirements?

A. 1. Create public subnets in the Tokyo VPC to migrate the workloads into.
2. Configure an internet gateway for the Tokyo office to reach the Tokyo VPC.
3. Configure security groups on the Tokyo workloads to only allow traffic from the Tokyo office and the Paris workloads.
4. Create peering connections between the Tokyo VPC and the Paris VPCs.
5. Configure a VPN connection between the Paris data center and the Tokyo office by using existing routers.

B. 1. Configure a transit gateway in the Asia Pacific (Tokyo) Region. Associate this transit gateway with the Tokyo VPC.
2. Create peering connections between the Tokyo transit gateway and the Paris transit gateway.
3. Set up a new Direct Connect connection from the Tokyo office to the Tokyo transit gateway.
4. Configure routing on both transit gateways to allow data to flow between sites and the VPCs.

C. 1. Configure a transit gateway in the Asia Pacific (Tokyo) Region. Associate this transit gateway with the Tokyo VPC.
2. Create peering connections between the Tokyo transit gateway and the Paris transit gateway.
3. Configure an AWS Site-to-Site VPN connection from the Tokyo office. Set the Tokyo transit gateway as the target.
4. Configure routing on both transit gateways to allow data to flow between sites and the VPCs. **Most Voted**

D. 1. Configure an AWS Site-to-Site VPN connection from the Tokyo office to the Paris transit gateway.
2. Create an association between the Paris transit gateway and the Tokyo VPC.

3. Configure routing on the Paris transit gateway to allow data to flow between sites and the VPC.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Akshay0403 Highly Voted 1 year, 8 months ago

Selected Answer: C

5 days so VPN needs to be used over Direct connect

kajiyatta 1 year, 8 months ago

You mean ANS.B,right?

Akshay0403 1 year, 8 months ago

Option C offers the best solution by efficiently integrating Tokyo and Paris regions through transit gateways and a VPN connection while adhering to the requirement of avoiding direct internet access. This approach is both secure and operationally efficient, ensuring private and encrypted communication between on-premises and AWS resources.

AzureDP900 1 year, 2 months ago

Using a transit gateway that connects both regions, ensuring secure connectivity between workloads in Paris and Tokyo. Configuring peering connections between the Tokyo transit gateway and the Paris transit gateway for further security. Setting up an AWS Site-to-Site VPN connection to establish encrypted tunneling between the Tokyo office and the Paris transit gateway. This solution ensures that workloads can be migrated within 5 days, are not directly accessible from the internet, and maintain connectivity between sites while securely accessing each other's resources.

intp75 1 year ago

Why bother with TGW? Why not just Site-To-Site VPN that is Answer D?

Nouwara 10 months, 4 weeks ago

Selected Answer: C

it is between B or C but as the solution should be in 5 days so C as we can't have a DX in 5 days

woorkim 1 year, 3 months ago

C is answer! Provisioning a new Direct Connect connection for the Tokyo office would take weeks, making it infeasible for a 5-day migration timeline.

cas_tori 1 year, 6 months ago

Selected Answer: C

this is C

https://zhangxuetu.online

[202610]

Question #198 Topic 1

Company A recently acquired Company B. Company A has a hybrid AWS and on-premises environment that uses a hosted AWS Direct Connect connection, a Direct Connect gateway, and a transit gateway. Company A has a transit VIF to access the resources in its production environment in the us-east-1 Region.

Company B has applications that run across multiple VPCs in the us-west-2 Region in a single AWS account. A transit gateway connects all Company B's application VPCs. The CIDR blocks for both companies do not overlap.

Company A needs to use the existing Direct Connect connection to access Company B's applications from the on-premises environment.

Which solution will meet these requirements?

A. Create a new Direct Connect gateway in the Company B account. Associate the Company B transit gateway with the new Direct Connect gateway. Create a transit VIF on the existing hosted connection for Company B.

B. Create an association proposal from the Company B account to associate the Company B transit gateway with the Company A Direct Connect gateway. Accept the transit gateway association proposal by logging into the Company A account. **Most Voted**

C. Create multiple virtual private gateways. Attach the virtual private gateways to each of Company B's application VPCs. Create a hosted private VIF for each virtual private gateway.

D. Create a new Direct Connect gateway in the Company B account. Associate the Company B transit gateway with the new Direct Connect gateway. Create a hosted private VIF for Company B.

Correct Answer: B

Community vote distribution

B (100%)

Comments

AzureDP900 1 year, 2 months ago

B is right Both companies have different AWS accounts, making it impossible for them to directly share a transit gateway. The existing hosted connection is in the us-east-1 Region, while Company B's applications are located in the us-west-2 Region, and they do not overlap with each other. Therefore, using the same transit VIF would not be viable without some sort of shared resource between them.

woorkim 1 year, 3 months ago

B is right! In Company B's account, create an association proposal to link the transit gateway in us-west-2 to Company A's Direct Connect gateway. In Company A's account, accept the association proposal. Update routing configurations to allow traffic from Company A's on-premises environment to reach Company B's applications via the Direct Connect gateway and transit gateway.

Akshay0403 1 year, 8 months ago

Selected Answer: B

Option B is the most efficient solution for connecting Company A's on-premises environment to Company B's applications. It leverages the existing Direct Connect infrastructure, minimizing the need for additional hardware and configuration, and uses Direct Connect gateway and transit gateway association for seamless integration between the two companies' environments.

Blitz1 1 year, 8 months ago

Selected Answer: B

https://docs.aws.amazon.com/directconnect/latest/UserGuide/multi-account-associate-tgw.html

veyisceylan 1 year, 9 months ago

it is B. Hosted connection allows only one VIF(transit, public or private)

https://zhangxuetu.online

[202610]

Question #199 Topic 1

A company has developed a web service for language translation. The web service's application runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The instances run behind an Application Load Balancer (ALB) and are deployed in a private subnet. The web service can process requests that contain hundreds of megabytes of data.

The company needs to give some customers the ability to access the web service. Each customer has its own AWS account. The company must make the web service accessible to approved customers without making the web service accessible to all customers.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Create VPC peering connections with the approved customers only.

B. Create an AWS PrivateLink endpoint service. Configure the endpoint service to require acceptance that will be granted to approved customers only. **Most Voted**

C. Configure an authentication action for the endpoint service's load balancer to allow customers to log in by using their AWS credentials. Provide only approved customers with the URL.

D. Configure a Network Load Balancer (NLB) and a listener with the ALB as a target. Associate the NLB with the endpoint service. **Most Voted**

E. Associate the ALB with the endpoint service.

Correct Answer: BD

Community vote distribution

BD (100%)

Comments

AzureDP900 1 year, 2 months ago

B and D Both options provide a secure connection between your EC2 instances behind an ALB and approved customers' AWS accounts, ensuring that only authorized users have access to your web service.

cas_tori 1 year, 6 months ago

Selected Answer: BD

this is BD

rdiaz 1 year, 9 months ago

Selected Answer: BD

BD are ok

Akshay0403 1 year, 8 months ago

While using a Network Load Balancer (NLB) is a valid approach, it adds unnecessary complexity if you are already using an ALB. AWS PrivateLink supports integration directly with ALB, and using an NLB introduces additional configuration steps that are not needed in this scenario. I will go with B and E

kupo777 1 year, 7 months ago

DB is correct. ALB cannot be specified as the target of an endpoint service.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #200 Topic 1

A company is migrating an application to the AWS Cloud. The company has successfully provisioned and tested connectivity between AWS Direct Connect and the company's on-premises data center. The application runs on Amazon EC2 instances across multiple Availability Zones. The instances are in an Auto Scaling group.

The application communicates through HTTPS to a third-party vendor's data service that is hosted at the company's data center. The data service implements a static ACL through explicit allow listing of client IP addresses.

A network engineer must design a network solution so that the migrated application can continue to access the vendor's data service as the application scales.

Which solution will meet these requirements with the LEAST amount of ongoing change to the vendor's allow list?

A. Configure a private NAT gateway in the subnets for each Availability Zone that the application runs in. Configure the application to target the NAT gateways instead of the data service directly. Update the data service's allow list to include the IP addresses of the NAT gateways. **Most Voted**

B. Configure an elastic network interface in the subnets for each Availability Zone that the application runs in. Associate the elastic network interfaces with the Auto Scaling group for the application. Update the data service's allow list to include the IP addresses of the elastic network interfaces.

C. Configure an elastic network interface in the subnets for each Availability Zone that the application runs in. Launch an EC2 instance into each subnet. Attach the respective elastic network interfaces to the new EC2 instances. In the application subnet route tables, configure the new EC2 instances as the next destination for the data service. Update the data service's allow list to include the IP addresses of the elastic network interfaces.

D. Configure an Application Load Balancer (ALB) in the subnets for each Availability Zone that the application runs in. Configure an ALB-associated target group that contains a target that uses the IP address for the data service. Configure the application to target the ALB instead of the data service directly. Update the data service's allow list to include the IP addresses of the ALBs.

Correct Answer: A

Community vote distribution



Comments

c1193d4 1 year, 2 months ago

Selected Answer: A

A ... but I'm not ok with "Configure the application to target the NAT gateways instead of the data service directly." => the subnet route tables should be modified ... NOT the application itself.

woorkim 1 year, 3 months ago

Selected Answer: A

By using a private NAT gateway, the solution ensures that the vendor's data service always sees the same IP address, minimizing the need for ongoing updates to the allow list while allowing the application to scale.

cas_tori 1 year, 7 months ago

Selected Answer: A

this is A

siheom 1 year, 7 months ago

Selected Answer: A

VOTE A

yama_chan 1 year, 8 months ago

The correct answer is D. Considering the simplicity of managing the allow list and the automation of load balancing, option D, using an Application Load Balancer (ALB), is the optimal solution. However, if managing the allow list is not an issue or if direct communication is required due to specific requirements, option B, using an Elastic Network Interface (ENI), is also a strong choice.

jhon648274 1 year, 7 months ago

Application load balancer ip is not static and it can change thus why is not an optimal solution

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #201 Topic 1

A company has a highly available application that is hosted in multiple VPCs and in two on-premises data centers. All the VPCs reside in the same AWS Region. All the VPCs require access to each other and to the on-premises data centers for the transfer of files that are multiple gigabytes in size.

A network engineer is designing an AWS Direct Connect solution to connect the on-premises data centers to each VPC.

Which architecture will meet the company's requirements with the LEAST operational overhead?

A. Configure a virtual private gateway and a private VIF in each VPC in the Region. Configure a Direct Connect gateway. Associate the VIF of every VPC with the Direct Connect gateway. Create a new private VIF that connects the Direct Connect gateway to each on-premises data center. Configure the new private VIF to exchange BGP routes with the on-premises data centers and to have an MTU of 9001. Use VPC peering between each VPC. Configure static routing in each VPC to provide inter-VPC routing.

B. Configure a virtual private gateway and a private VIF in each VPC in the Region. Configure a Direct Connect gateway. Associate the VIF of every VPC with the Direct Connect gateway. Create a new private VIF that connects the Direct Connect gateway to each on-premises data center. Configure the new private VIF to exchange BGP routes with the on-premises data centers and to have an MTU of 8500. Use VPC peering between each VPC. Configure static routing in each VPC to provide inter-VPC routing.

C. Configure a transit gateway in the same Region of each VPAttach each VPC to the transit gateway. Configure a Direct Connect gateway. Associate the Direct Connect gateway with the transit gateway. Associate a new transit VIF with each Direct Connect connection. Configure the new transit VIF to exchange BGP routes and to have an MTU of 9001. Configure route propagation between each VPC and the transit gateway.

D. Configure a transit gateway in the same Region of each VPC. Attach each VPC to the transit gateway. Configure a Direct Connect gateway. Associate the Direct Connect gateway with the transit gateway. Associate a new transit VIF with each Direct Connect connection. Configure the new transit VIF to exchange BGP routes and to have an MTU of 8500. Configure route propagation between each VPC and the transit gateway. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

woorkim 1 year, 3 months ago

D is answer! The MTU of a transit virtual interface can be either 1500 or 8500 (jumbo frames).

chiaseed 1 year, 5 months ago

Selected Answer: D

"Jumbo frames will apply only to propagated routes via AWS Direct Connect and static routes via transit gateways. Jumbo frames on transit gateways support only 8500 bytes."

chiaseed 1 year, 5 months ago

https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html#set-jumbo-frames-vif I attached the link to the above but somehow it is not showing. So I am attaching it here again.

cas_tori 1 year, 6 months ago

Selected Answer: D

this is D

strike3test 1 year, 9 months ago

Selected Answer: D

Jumbo frames will apply only to propagated routes via AWS Direct Connect and static routes via transit gateways. Jumbo frames on transit gateways support only 8500 bytes.

rdiaz 1 year, 9 months ago

Selected Answer: D

8500 mtu of transit vif https://docs.aws.amazon.com/directconnect/latest/UserGuide/set-jumbo-frames-vif.html

https://zhangxuetu.online

[202610]

Question #202 Topic 1

A company has a data center in the us-west-1 Region with a 10 Gbps AWS Direct Connect dedicated connection to a Direct Connect gateway. There are two private VIFs from the same data center location in us-west-1 that are attached to the same Direct Connect gateway.

VIF 1 advertises 172.16.0.0/16 with an AS_PATH attribute value of 65000. VIF 2 advertises 172.16.1.0/24 with an AS PATH attribute value of 65000 65000 65000.

How will AWS route traffic to the data center for traffic that has a destination address within the 172.16.1.0/24 network range?

A. AWS will route all traffic by using VIF 1.

B. AWS will route all traffic by using VIF 2. **Most Voted**

C. AWS will use both VIFs for routing by using a round-robin policy.

D. AWS will use flow control to balance the traffic between the two VIFs.

Correct Answer: B

Community vote distribution

B (100%)

Comments

Akshay0403 **Highly Voted** 1 year, 8 months ago

Selected Answer: B

AWS will route traffic to the data center for addresses within the 172.16.1.0/24 network range using VIF 2 because it provides a more specific route, despite having a longer AS_PATH. Therefore, the correct answer is: B. AWS will route all traffic by using VIF 2.

tushar321 10 months, 3 weeks ago

Selected Answer: B

Priority wins. More specific match / precise route / in same region is always a better choice

AzureDP900 1 year, 2 months ago

Selected Answer: B

B is right, here is why AS_PATH Attribute : The AS_PATH attribute of a private IP address indicates the path that packets must take from the internet source to their destination. In this case, both VIFs have an AS_PATH value of 65000. Priority : Since both VIFs have the same AS_PATH value, AWS will use the AS_PATH value of VIF 2 (65000 65000 65000) as a priority for routing traffic to destinations in the 172.16.1.0/24 network range. First Match Wins :

When there are multiple paths available from the same source, AWS uses the first match rule that is more specific and has fewer AS_PATH attribute values. In this case, VIF 2 is a subset of VIF 1, so it will be used for routing traffic to destinations in the 172.16.1.0/24 network range.

AzureDP900 1 year, 2 months ago

B is right The AS_PATH attribute value in VIF 1 only includes one value (65000), indicating that the route for 172.16.0.0/16 is directly connected to the data center and not learned from another BGP peer. In contrast, the AS_PATH attribute value in VIF 2 includes three values (65000, 65000, 65000), indicating that the route for 172.16.1.0/24 is learned from another BGP peer with an additional ASN of 65000. Because the route for 172.16.1.0/24 includes an additional ASN, it will be preferred over the route for 172.16.0.0/16 when routing traffic within the data center. Therefore, AWS will route all traffic destined for the 172.16.1.0/24 network range by using VIF 2

strike3test 1 year, 9 months ago

Selected Answer: B

B. AWS will route all traffic by using VIF 2. In AWS Direct Connect, traffic is routed based on the most specific route. In this scenario, there are two VIFs advertising routes for different portions of the 172.16.0.0/16 network: VIF 1 advertises the 172.16.0.0/16 network. VIF 2 advertises the more specific subnet 172.16.1.0/24 within the 172.16.0.0/16 network. Since VIF 2 advertises a more specific route (172.16.1.0/24), AWS will prefer this route for traffic destined for the 172.16.1.0/24 network. Therefore, the correct answer is:

AXH 1 year, 9 months ago

B, most specific prefix wins!

https://zhangxuetu.online

[202610]

Question #203 Topic 1

A company is planning to host external websites on AWS. The websites will include multiple tiers such as web servers, application logic services, and databases. The company wants to use AWS Network Firewall, AWS WAF, and VPC security groups for network security.

The company must ensure that the Network Firewall firewalls are deployed appropriately within relevant VPCs. The company needs the ability to centrally manage policies that are deployed to Network Firewall and AWS WAF rules. The company also needs to allow application teams to manage their own security groups while ensuring that the security groups do not allow overly permissive access.

What is the MOST operationally efficient solution that meets these requirements?

A. Define Network Firewall firewalls, AWS WAFV2 web ACLs. Network Firewall policies, and VPC security groups in code. Use AWS CloudFormation to deploy the objects and initial policies and rule groups. Use CloudFormation to update the AWS WAFv2 web ACLs. Network Firewall policies, and VPC security groups. Use Amazon GuardDuty to monitor for overly permissive rules.

B. Define Network Firewall firewalls. AWS WAFV2 web ACLs, Network Firewall policies, and VPC security groups in code. Use the AWS Management Console or the AWS CLI to manage the AWS WAFv2 web ACLs. Network Firewall policies, and VPC security groups. Use Amazon GuardDuly to invoke an AWS Lambda function to evaluate the configured rules and remove any overly permissive rules.

C. Deploy AWS WAFv2 IP sets and AWS WAFv2 web ACLs with AWS CloudFormation. Use AWS Firewall Manager to deploy Network Firewall firewalls and VPC security groups where required and to manage the AWS WAFv2 web ACLs, Network Firewall policies, and VPC security groups.

D. Define Network Firewall firewalls, AWS WAFv2 web ACLS, Network Firewall policies, and VPC security groups in code. Use AWS CloudFarmation to deploy the objects and initial policies and rule groups. Use AWS Firewall Manager to manage the AWS WAFV2 web ACLS, Network Firewall policies, and VPC security groups. Use Amazon GuardDuty to monitor for overly permissive rules. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: D

The correct answer is indeed D. Define Network Firewall firewalls, AWS WAFv2 web ACLs, Network Firewall policies, and VPC security groups in code. Use AWS CloudFormation to deploy the objects and initial policies and rule groups. Use AWS Firewall Manager to manage the AWS WAFv2 web ACLs, Network Firewall policies, and VPC security groups. Use Amazon GuardDuty to monitor for overly permissive rules.

woorkim 1 year, 3 months ago

D is right! Option D is the most operationally efficient solution. It combines CloudFormation for consistent deployments, Firewall Manager for centralized policy management, and GuardDuty for monitoring and alerting on overly permissive rules

aragon_saa 1 year, 7 months ago

Selected Answer: D

Answer is D

Cacheirez 1 year, 7 months ago

Selected Answer: D

Firewall Manager makes it easier to centrally configure and manage AWS WAF, AWS Shield Advanced, and VPC security group policies across multiple accounts and applications in an AWS Organization. It also manages AWS Network Firewall policies.

https://zhangxuetu.online

[202610]

Question #204 Topic 1

A company has deployed an application in which the front end of the application communicates with the backend instances through a Network Load Balancer (NLB) in the same VPC. The application is highly available across two Availability Zones. The company wants to limit the amount of traffic that travels across the Availability Zones. Traffic from the front end of the application must stay in the same Availability Zone unless there is no healthy target in that Availability Zone behind the NLB. If there is no healthy target in the same Availability Zone, traffic must be sent to the other Availability Zone.

Which solution will meet these requirements?

A. Create a private hosted zone with weighted routing for each Availability Zone. Point the primary record to the local Availability Zone NLB DNS record. Point the secondary record to the Regional NLB DNS record. Configure the front end of the application to perform DNS lookups on the local private hosted zone records.

B. Turn off cross-zone load balancing on the NLConfigure the front end of the application to perform DNS lookups on the local Availability Zone NLB DNS record.

C. Create a private hosted zone. Create a failover record for each Availability Zone. For each failover record, point the primary record to the local Availability Zone NLB DNS record and point the secondary record to the Regional NLB DNS record. Configure the front end of the application to perform DNS lookups on the local private hosted zone records. **Most Voted**

D. Enable sticky sessions (session affinity) so that the NLB can bind a user's session to targets in the same Availability Zone.

Correct Answer: C

Community vote distribution



Comments

AikAWS 6 months, 1 week ago

Selected Answer: C

When cross-zone load balancing is disabled on a Network Load Balancer (NLB): Each NLB node routes requests only to targets in the same Availability Zone (AZ) as the node. If that AZ has no healthy targets, the NLB node fails the requests — it does not automatically reroute them to another AZ.

1a17d1e 7 months, 3 weeks ago

Selected Answer: C

If you disable cross-zone load balancing on an NLB, traffic is routed only to targets in the same AZ as the DNS name resolved. Failover does not happen automatically if that AZ becomes impaired which is a requirement for this solution. However, Route 53 can remove the zonal DNS record from resolution if the NLB node in that AZ fails health checks. If your application retries DNS resolution and uses another AZ's DNS name, manual failover can occur — but only if your app logic supports it.

c1193d4 1 year, 2 months ago

Selected Answer: C

If B: I don't see how the failover would work if cross-zone load-balancing is OFF and only the AZ NLB endpoint is used
A better solution would be to tweek the "AZ routing configuration" to "AZ affinity" but it's not describe as a solution

AzureDP900 1 year, 2 months ago

Selected Answer: B

By disabling cross-zone load balancing, traffic will only be routed within the same Availability Zone unless there are no healthy targets available in that zone. This ensures that traffic from the front end of the application stays within the same Availability Zone unless necessary.

cas_tori 1 year, 6 months ago

Selected Answer: B

this is B

aragon_saa 1 year, 7 months ago

Selected Answer: B

Answer is B

Cacheirez 1 year, 7 months ago

Selected Answer: B

By disabling cross-zone load balancing on the NLB, the NLB will only route traffic to targets within the same Availability Zone as the incoming request. If no healthy targets exist in the local AZ, the NLB will route the traffic automatically to targets in another AZ.

secdaddy 1 year, 1 month ago

B says "Configure the front end of the application to perform DNS lookups on the ** local Availability Zone ** NLB DNS record." so it is restricted in any event to the local AZ.

jfedotov 1 year, 2 months ago

That's not true

https://zhangxuetu.online

[202610]

Question #205 Topic 1

A company needs to protect against potential botnet command and control traffic from any Amazon EC2 instances that is in in the company's AWS Environment.

Which solution will meet these requirements?

A. Use AWS Shield Advanced. Activate Shield Advanced protections on the EC2 instances to filter and block botnet traffic.

B. Use Amazon Route 53 Resolver DNS Firewall. Add a rule to a rule group to use the AWSManagedDomainsBotnetCommandandControl managed domain list with an action to block botnet traffic. **Most Voted**

C. Use AWS WAF Bot Control. Configure a managed rule group that uses an AWS managed rule set to block botnet traffic.

D. Use AWS Systems Manager. Run a Systems Manager Automation runbook on the EC2 instances to configure the instances to block botnet traffic.

Correct Answer: B

Community vote distribution

B (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: B

It provides a proactive and automated way to block known botnets and their command and control traffic.

woorkim 1 year, 3 months ago

Selected Answer: B

Amazon Route 53 Resolver DNS Firewall with the AWSManagedDomainsBotnetCommandandControl managed rule group: Scalable and Managed: Automatically updates the list of known botnet domains. Preemptive Blocking: Prevents EC2 instances from resolving malicious domains. Low Operational Overhead: Easy to implement and maintain.

luisgu 1 year, 6 months ago

Selected Answer: B

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-dns-firewall-managed-domain-lists.html

cas_tori 1 year, 6 months ago

Selected Answer: B

this is B

Cacheirez 1 year, 7 months ago

Selected Answer: B

The question talks about "botnet command and control traffic". The most common and effective way to intercept such traffic is at the DNS level, where many botnets rely on domain names to communicate with their C2 servers. The Amazon Route 53 Resolver DNS Firewall is specifically designed to block DNS queries to known malicious domains, including those used for botnet C2 traffic. If it was application-level traffic AWS WAF Bot Control would apply.

jhon648274 1 year, 7 months ago

Correct answer should be B - this avoids instances from responding / connecting to malicious controllers

https://zhangxuetu.online

[202610]

Question #206 Topic 1

A company has two on-premises data centers. The first data center is in the us-east-1 Region. The Second data canter is in the us-east-2 Region. Each data center connects to the closest AWS Direct Connect facility. The company uses Direct Connect connections, transit VIFs, and a single Direct Connect gateway to establish connectivity to VPCs in us-east-1 and us-east-2 from the company's data centers. The company also has private connectivity from a telecommunications provider that connects the first data center to the second data center.

Recently, there have been multiple connection disruptions to the private connectivity between the data centers. The company needs a solution to improve the reliability of the connection between the two data centers.

Which solution will meet these requirements?

A. Create a new Direct Connect gateway. Enable the Direct Connect SiteLink feature on the transit VIF. Share the CIDR blocks from the first data center and the second data center with each other.

B. Create a new public VIF to both Regions. Enable the Direct Connect SiteLink feature on the new public VIF.

C. Enable the Direct Connect SiteLink feature on the existing Direct Connect connections.

D. Enable the Direct Connect SiteLink feature on the existing transit VIFS that are attached to the existing Direct Connect gateway. Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Comments

AzureDP900 1 year, 2 months ago

Selected Answer: D

D is right. By enabling SiteLink on the existing transit VIFS, we can establish a site-to-site link between the two data centers, which will allow traffic to be routed through both connections and ensure high availability in case of a connection disruption. This solution meets the requirements

woorkim 1 year, 3 months ago

Selected Answer: D

Option D is the best solution because it enables reliable and direct communication between the two data centers using the existing transit VIFs and Direct Connect infrastructure. This approach minimizes changes, reduces complexity, and improves the reliability of the connection.

koukiman0514 1 year, 6 months ago

Selected Answer: D

this is D

cas_tori 1 year, 6 months ago

Selected Answer: D

this is D

Cacheirez 1 year, 7 months ago

Selected Answer: D

Direct Connect SiteLink allows data transfer between two Direct Connect locations over the AWS global network, bypassing the need for private connectivity between on-premises data centers. By enabling SiteLink on the existing transit VIFs that are attached to the Direct Connect gateway, you can leverage AWS's backbone network to facilitate communication between the two data centers without relying on potentially unreliable private connectivity.

jhon648274 1 year, 7 months ago

D is correct https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-direct-connect-sitelink/

https://zhangxuetu.online

[202610]

Question #207 Topic 1

A network engineer is working on a large migration effort from an on-premises data center to an AWS Control Tower based multi-account environment. The environment has a transit gateway that is deployed to a central network services account. The central network services account has been shared with an organization in AWS Organizations through AWS Resource Access Manager (AWS RAM).

A shared services account also exists in the environment. The shared services account hosts workloads that need to be shared with the entire organization.

The network engineer needs to create a solution to automate the deployment of common network components across the environment. The solution must provision a VPC for application workloads to each new and existing member account. The VPCs must be connected to the transit gateway in the central network services account.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

A. Deploy an AWS Lambda function to the shared services account. Program the Lambda function to assume a role in the new and existing member accounts to provision the necessary network infrastructure. **Most Voted**

B. Update the existing accounts with an Account Factory Customization (AFC). Select the same AFC when provisioning new accounts.

C. Create an AWS CloudFormation template that describes the infrastructure that needs to be created in each account. Upload the template as an AWS Service Catalog product to the shared services account. **Most Voted**

D. Deploy an Amazon EventBridge rule on a default event bus in the shared services account. Configure the EventBridge rule to react to AWS Control Tower CreateManagedAccount lifecycle events and to invoke the AWS Lambda function. **Most Voted**

E. Create an AWSControlTowerBlueprintAccess role in the shared services account.

F Create an AWSControlTowerBlueprintAccess role in each member account.

Correct Answer: ACD

Community vote distribution



Comments

yismail 2 months, 3 weeks ago

Selected Answer: BCE

Option A is less preferred, as Lambda function could work, it carries high operational overhead because you must maintain the code, handle retry logic, and manage cross-account IAM permissions manually. Option D, EventBridge and Lambda is old way of doing customizations

953bf6d 6 months ago

Selected Answer: BC

B: Use Account Factory Customizations (AFC) to baseline existing accounts and apply the same customization to new accounts with minimal ops. C: Package the VPC + TGW attachment as a CloudFormation template and publish it as a Service Catalog product in the shared services account. F: Create the AWSControlTowerBlueprintAccess role in each member account so AFC can provision the product automatically across accounts.

ryuhei 8 months, 2 weeks ago

Selected Answer: ACD

Combination A, C, and D is the solution with the least operational overhead because it leverages AWS Control Tower lifecycle events and combines CloudFormation templates and Lambda functions to automate the provisioning of network infrastructure.

0xab3d 8 months, 3 weeks ago

Selected Answer: ACD

Correct answer is ACD

Rollizo 1 year, 1 month ago

Selected Answer: ACD

For me you have to use Cloudformation, later event Bridge and Lambda Function

AzureDP900 1 year, 2 months ago

Selected Answer: BCE

BCE (Create an AWS CloudFormation template, Deploy an Amazon EventBridge rule, and Update the existing accounts with an Account Factory Customization) is actually a more efficient and streamlined approach.

cas_tori 1 year, 6 months ago

Selected Answer: BCE

this is BCE

aragon_saa 1 year, 7 months ago

Selected Answer: BCE

Answer is BCE

https://zhangxuetu.online

[202610]

Question #208 Topic 1

An online retail company is running a web application in the us-wast-2 Region and serves consumers in the United States. The company plans to expand across several countries in Europe and wants to provide low latency for all its users.

The application needs to identify the users' IP addresses and provide localized content based on the users' geographic location. The application uses HTTP GET and POST methods for its functionality. The company also needs to develop a failover mechanism that works for GET and POST methods and is based on health checks. The failover must occur in less than 1 minute for all clients.

Which solution will meet these requirements?

A. Configure a Network Load Balancer (NLB) for the application in each environment in the new AWS Regions. Create an AWS Global Accelerator accelerator that has endpoint groups that point to the NLBs in each Region.

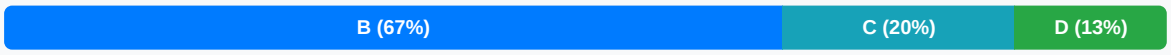
B. Configure an Application Load Balancer (ALB) for the application in each environment in the new AWS Regions. Create an AWS Global Accelerator accelerator that has endpoint groups that point to the ALBs in each Region. **Most Voted**

C. Configure an Application Load Balancer (ALB) for the application in each environment in the new AWS Regions. Create Amazon Route 53 public hosted zones that have failover routing policies.

D. Configure a Network Load Balancer (NLB) for the application in each environment in the new AWS Regions. Create an Amazon CloudFront distribution. Configure an origin group with origin failover options.

Correct Answer: B

Community vote distribution



Comments

46f094c 1 year, 2 months ago

Selected Answer: D

the only option that could handle "provide localized content based on the users' geographic location". For POST using a lamda@edge.

AzureDP900 1 year, 2 months ago

Selected Answer: B

B is right In this case, since the application uses HTTP GET and POST methods, an ALB might be more suitable due to its support for more advanced request processing features like path-based routing and Lambda functions for custom processing.

woorkim 1 year, 3 months ago

B is correct! ALB: Handles HTTP-specific features like identifying user IPs and routing based on geolocation. Global Accelerator: Provides low-latency global routing and fast failover (less than 1 minute) with health checks.

Nel07 1 year, 5 months ago

Answer is B

VerRi 1 year, 5 months ago

Selected Answer: B

HTTP req, A&D out. Global Accelerator is closer to the user; it can react faster than Route 53.

AlirezaNetWorld 1 year, 6 months ago

B is the correct answer

luisgu 1 year, 6 months ago

Selected Answer: B

Option A: While NLBs are performant, they are better suited for TCP rather than HTTP/HTTPS traffic. Option C: Route 53 might not meet the sub-minute failover requirement due to DNS propagation delays. Option D: CloudFront is more suited for static content, not necessarily for dynamic applications requiring HTTP GET and POST failover. Option B : ALB: Specifically designed for HTTP/HTTPS traffic and provides features like path-based routing and host-based routing. AWS Global Accelerator: Ensures low latency by routing traffic to the optimal region and provides quick failover mechanisms with health checks.

cas_tori 1 year, 6 months ago

Selected Answer: C

this is C

aragon_saa 1 year, 7 months ago

Selected Answer: C

Answer is C

https://zhangxuetu.online

[202610]

Question #209 Topic 1

A company has VPCs across 50 AWS accounts and is using AWS Organizations. The company wants to implement web filtering. The requirements for how the traffic must be filtered are the same for all the VPCs. A network engineer plans to use AWS Network Firewall. The network engineer needs to implement a solution that minimizes the number of firewall policies and rule groups that are necessary for this web filtering.

Which combination of steps will meet these requirements? (Choose three.)

A. Create a firewall policy or rule group in each account.

B. Use SCPs to share the firewall policy or rule group.

C. Create a firewall policy or rule group in the management account **Most Voted**

D. Use AWS Resource Access Manager (AWS RAM) to share the firewall policy or rule group. **Most Voted**

E. Enable sharing within Organizations. **Most Voted**

F. Create OUs to share the firewall policy or rule group.

Correct Answer: CDE

Community vote distribution



Comments

AzureDP900 1 year, 2 months ago

Selected Answer: CDE

The correct options are: C, D, and E. Option F (creating OUs) is not relevant for implementing web filtering or sharing firewall policies and rule groups across VPCs.

Spaurito 1 year, 4 months ago

CDE - Firewall policy and rule group sharing integrates with AWS Resource Access Manager (AWS RAM). AWS RAM is a service that enables you to share your AWS resources with any AWS account or through AWS Organizations. With AWS RAM, you share resources that you own by creating a resource share. A resource share specifies the resources to share, and the consumers with whom to share them. Consumers can be individual AWS accounts, organizational units, or an entire organization in AWS Organizations. https://docs.aws.amazon.com/network-firewall/latest/developerguide/sharing.html

cas_tori 1 year, 6 months ago

Selected Answer: CDE

this is CDE

hcong 1 year, 7 months ago

Selected Answer: ADE

This combination provides a comprehensive solution to prevent SQL injection attacks: Create a WAF web ACL with appropriate rules Use ALB that can be integrated with WAF Associate WAF with ALB for practical application protection Options B and F are not necessary because the application is internal and does not need CloudFront distribution. Option D is not applicable because NLB cannot be directly integrated with WAF. By implementing these three steps, the company can significantly improve the defense ability of its applications against SQL injection attacks.

hcong 1 year, 7 months ago

sorry it should be ACE

aragon_saa 1 year, 7 months ago

Selected Answer: CDE

Answer is CDE

Cacheirez 1 year, 7 months ago

Selected Answer: CDE

By creating the firewall policy or rule group in the management account (the central account in AWS Organizations), the engineer can manage these policies centrally, which reduces the need to create and manage separate policies in each of the 50 accounts. AWS RAM allows you to share AWS resources, such as firewall policies and rule groups, across multiple AWS accounts within your organization. This helps minimize the number of policies that need to be created and ensures consistent web filtering across all accounts. Enabling sharing within AWS Organizations allows the resources shared via AWS RAM (such as firewall policies and rule groups) to be accessed by all accounts within the organization. This facilitates the centralized management and application of the web filtering rules across all VPCs in the 50 accounts.

https://zhangxuetu.online

[202610]

Question #210 Topic 1

A company has an internal web-based application that employees use. The company hosts the application over a VPN in the company's on-premises network. The application runs on a fleet of Amazon EC2 instances in a private subnet behind a Network Load Balancer (NLB) in the same subnet. The instances are in an Amazon EC2 Auto Scaling group.

During a recent security incident, SQL injection occurred on the application. A network engineer must implement a solution to prevent SQL injection attacks in the future.

Which combination of steps will meet these requirements? (Choose three.)

A. Create an AWS WAF web ACL that includes rules to block SQL injection attacks. **Most Voted**

B. Create an Amazon CloudFront distribution. Specify the EC2 instances as the origin.

C. Replace the NLB with an Application Load Balancer. **Most Voted**

D. Associate the AWS WAF web ACL with the NLB.

E. Associate the AWS WAF web ACL with the Application Load Balancer. **Most Voted**

F. Associate the AWS WAF web ACL with the Amazon CloudFront distribution.

Correct Answer: ACE

Community vote distribution

ACE (100%)

Comments

woorkim 1 year, 3 months ago

Selected Answer: ACE

While CloudFront can be used as a content delivery network (CDN), it is not necessary in this case. CloudFront is typically used to distribute content to end users with low latency, but it is not required to protect against SQL injection attacks if AWS WAF is applied directly to the ALB.

AlohaEva 1 year, 6 months ago

Selected Answer: ACE

NLB is a Layer 3/4 component WAF is a Layer 7 protection component WAF is not capable of acting on the content of not terminated TLS session (encrypted data) WAF is only available for ALB. So, consider changing NLB to ALB and use WAF with ALB

cas_tori 1 year, 6 months ago

Selected Answer: ACE

this is ACE

aragon_saa 1 year, 7 months ago

Answer is ACE

Cacheirez 1 year, 7 months ago

Selected Answer: ACE

AWS WAF (Web Application Firewall) can help protect your application from common web exploits, including SQL injection. By creating a web ACL (Access Control List) with rules specifically designed to detect and block SQL injection attempts, you can add a layer of protection to your application. AWS WAF can only be associated with an Application Load Balancer (ALB), not a Network Load Balancer (NLB). Replacing the NLB with an ALB is necessary to enable WAF protection for your web application. Once the ALB is in place, you can associate the AWS WAF web ACL with the ALB. This ensures that incoming traffic is inspected by the WAF rules, providing protection against SQL injection attacks.

https://zhangxuetu.online

[202610]

Question #211 Topic 1

A company is running business applications on AWS. The company uses 50 AWS accounts, thousands of VPCs, and 3 AWS Regions across the United States and Europe.

A network engineer needs to establish network connectivity between an on-premises data center and the Regions. The network engineer also must establish connectivity between the VPCs. On-premises: users and applications must be able to connect to applications that run in the VPCs.

The company has an existing AWS Direct Connect connection that the network engineer can use. The network engineer creates a transit gateway in each Region and configures the transit gateways as inter-Region peers.

Which solution will provide network connectivity from the on-premises data center to the Regions and will provide inter-VPC communications across the different Regions?

A. Create a private VIF with a gateway type of virtual private gateway. Configure the private VIF to use a virtual private gateway that is associated with one of the VPCs.

B. Create a private VIF to a new Direct Connect gateway. Associate the new Direct Connect gateway with a virtual private gateway in each VPC.

C. Create transit VIF with a gateway association to a new Direct Connect gateway. Associate each transit gateway with the new Direct Connect gateway. **Most Voted**

D. Create an AWS Site-to-Site VPN connection that uses a public VIF for the Direct Connect connection. Attach the Site-to-Site VPN connection to the transit gateways.

Correct Answer: C

Community vote distribution

C (100%)

Comments

Cacheirez **Highly Voted** 1 year, 7 months ago

Selected Answer: C

A transit VIF (Virtual Interface) allows you to connect your Direct Connect connection to a Direct Connect gateway. The Direct Connect gateway can then be associated with multiple transit gateways across different Regions, enabling seamless communication between on-premises networks and multiple VPCs across multiple Regions. By associating the transit gateways in each Region with the Direct Connect gateway, you enable on-premises connectivity to all VPCs attached to these transit gateways. This also allows for inter-VPC communication across the different Regions, as the transit gateways are configured as inter-Region peers. This setup is scalable and aligns with the company's

architecture, which includes thousands of VPCs and multiple Regions. The transit VIF with a Direct Connect gateway enables centralized management of your network, reducing complexity and operational overhead.

woorkim 1 year, 3 months ago

its c! only TGW has to be connected thru transit VIF!

cas_tori 1 year, 6 months ago

Selected Answer: C

this is C

aragon_saa 1 year, 7 months ago

Selected Answer: C

Answer is C

https://zhangxuetu.online

[202610]

Question #212 Topic 1

A company has two data centers that are interconnected with multiple redundant links from different suppliers. The company Uses IP addresses that are within the 172.16,0.0/16 CIDR block. The company is running iBGP between the two data centers by using a private Autonomous System Number (ASN) and IGP.

The company is moving toward a hybrid setup in which the company will initially use one VPC in the AWS Cloud. An AWS Direct Connect connection runs from the first data center to a Direct Connect gateway by using a private VIF. On the connection, the company advertises a summarized route for the 172.16.0.0/16 network. The company is planning to set up a second summarized route from the second data center to a different Direct Connect location.

The company needs to implement a solution to route traffic to and from AWS through the first Direct Connect connection. The solution must use the second Direct Connect connection for failover purposes only.

Which solution will meet these requirements?

A. Prepend the private ASN on the BGP announcements to AWS from the second data center. Add a second VIF in the first Direct Connect connection. Advertise the same network without any prepends from the first data center. Implement the same setup for the BGP announcement from AWS to the two data centers.

B. Tag the BGP announcements with the local preference BGP community tags. Set the tag to high preference for the first data center. Set the tag to low preference for the second data center. Configure the second data center's router to have a lower local preference for the direct AWS BGP advertisements than for the advertisement from the fist data center. **Most Voted**

C. Configure the Direct Connect gateway to prefer routing through the Direct Connect connection with the first data center. Configure the second data center's router to have a lower local preference for the direct AWS BGP advertisements than for the advertisement from the first data center.

D. Configure the focal AWS Region BGP community tag on the BGP route that is advertised from the fist data center. Configure AS_PATH prepends on the BGP announcements from the second data center.

Correct Answer: B

Community vote distribution



Comments

TigerDrev 1 month, 2 weeks ago

Selected Answer: A

Prepend incoming and outgoing advertisements will do it. Local preference only affects outbound traffic not inbound

AikAWS 6 months, 1 week ago

Selected Answer: B

It's B https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html#:~:text=Local%20preference%20BGP%20community%20tags%20are%20evaluated%20before%20any%20AS_PATH%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20attribute%2C%20and%20are%20evaluated%20in%20order%20from%20lowest%20to%20highest%20preference%20(where%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20highest%20preference%20is%20preferred)

46f094c 1 year, 2 months ago

Selected Answer: B

B is the only one taking into consideration out (aws-dtc with prepend from the DTC) and in traffic (dtc-aws with local pref in the second DTC pointing to the primary). A: prepend is only be user from DTC to AWS, but not from AWS to DTC C: can't configure preference in a DXG D: talks about regions but there no region in the question, plus they are used for diferent purposes. Filtering/manupulation at the DTC, propagation at AWS

woorkim 1 year, 3 months ago

B is correct! To support failover across multiple AWS Direct Connect connections (active/passive), apply a community tag with a higher preference to the prefixes for the primary or active virtual interface and a lower preference to the prefixes for the backup or passive virtual interface. For example, set the BGP community tags for your primary or active virtual interfaces to 7224:7300 (high preference) and 7224:7100 (low preference) for your passive virtual interfaces. Local preference BGP community tags are evaluated before any AS_PATH attribute, and are evaluated in order from lowest to highest preference (where highest preference is preferred).

meseerie 1 year, 4 months ago

Selected Answer: D

After reading the following answers seems to be D
https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

siheom 1 year, 4 months ago

Selected Answer: A

VOTE A

VerRi 1 year, 5 months ago

Selected Answer: A

A. updating AS_PATH for both 1st and 2nd data centres, making 2nd data centre less preferable. When 1st is down, they will switch to 2nd. B. local preference in BGP is used to control outbound traffic. The question says "to route traffic to and from AWS" so it does not cover the inbound C.DXG does not handle this level of config D. It suggests using both community tags and AS_PATH prepends, but for the same reason as B

luisgu 1 year, 6 months ago

Selected Answer: B

local region BGP communities do not apply in this case; only for public VIFs

cas_tori 1 year, 6 months ago

Selected Answer: D

this is D

aragon_saa 1 year, 7 months ago

Selected Answer: B

Answer is B

https://zhangxuetu.online

[202610]

Question #213 Topic 1

A company is replatforming a legacy data processing solution to AWS. The company deploys the solution on Amazon EC2 Instances in private subnets that are in one VPC.

The solution uses Amazon S3 for abject storage. Both the data that the solution processes and the data the solution produces are stored in Amazon S3. The solution uses Amazon DynamoDB to save its own state. The company collects flow logs for the VPC. The solution uses one NAT gateway to register its license through the internet. A software vendor provides a specific hostname so the solution can register its license.

The company notices that the AWS bill exceeds the projected budget for the solution. A network engineer uses AWS Cost Explorer to investigate the bill. The network engineer notices that the USE2-NatGateway-Bytes($) usage type is the root cause of the higher than expected bill.

What should the network engineer do to resolve the issue? (Choose two.)

A. Set up Amazon VPC Traffic Mirroring. Analyze the traffic to identify the traffic that the NAT gateway processes.

B. Examine the VPC flow logs to identity the traffic that traverses the NAT gateway. Most Voted

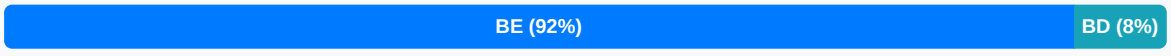
C. Set up an AWS Cost and Usage Report in the AWS Billing and Cost Management console. Examine the report to find more details about the NAT gateway charges.

D. Verify that the security groups attached to the EC2 instances allow outgoing traffic only to the IP addresses that the hostname resolves to, the VPC CIDR block, and the AWS IP address ranges for Amazon S3 and DynamoDB.

E. Verify that the gateway VPC endpoints for Amazon S3 and DynamoDB are both set up and associated with the route tables of the private subnets. Most Voted

Correct Answer: BE

Community vote distribution



Comments

AzureDP900 1 year, 2 months ago

Selected Answer: BE

B. Examine the VPC flow logs to identify the traffic that traverses the NAT gateway. This can provide insight into what's being processed by the NAT gateway, which may be contributing to the higher-than-expected bill. E. Verify that

the gateway VPC endpoints for Amazon S3 and DynamoDB are both set up and associated with the route tables of the private subnets. This will help ensure that data from these services can be accessed through the VPC without using the NAT gateway, which is likely to save on costs. By analyzing the VPC flow logs and verifying the setup of gateway VPC endpoints for Amazon S3 and DynamoDB, the network engineer can gain a better understanding of the traffic patterns and take steps to optimize usage of the NAT gateway.

woorkim 1 year, 3 months ago

B,E is answer! B. Examine the VPC flow logs to identify the traffic that traverses the NAT gateway. VPC flow logs provide detailed information about the traffic that flows through the NAT gateway. By analyzing these logs, the network engineer can identify which traffic is unnecessarily routed through the NAT gateway and contributing to the high costs. E. Verify that the gateway VPC endpoints for Amazon S3 and DynamoDB are both set up and associated with the route tables of the private subnets. NAT gateway costs increase because traffic to Amazon S3 and DynamoDB is traversing the NAT gateway instead of using gateway VPC endpoints. Setting up gateway endpoints for these services ensures that traffic stays within the AWS network, eliminating NAT gateway charges for these services.

Spaurito 1 year, 4 months ago

BE - are correct A - Traffic mirroring not needed and added cost B - Allows to review traffic for the NAT GW C - Cost and Billing Reports will help but not specific traffic details D - Lots of Overhead - This could work but not necessary. E - Verify the S3 and DynamoDB endpoints are configured properly.

VerRi 1 year, 5 months ago

Selected Answer: BE

B. Investigation D. It restricts traffic to the gateway endpoint and the NAT gateway, but it does not provide info about the traffic E. Ensure to use the internal traffic

AlirezaNetWorld 1 year, 6 months ago

DE are the right answers.

qomtodie 1 year, 6 months ago

Selected Answer: BE

nerver D

cas_tori 1 year, 6 months ago

Selected Answer: BE

this is BE

Cacheirez 1 year, 7 months ago

Selected Answer: BE

VPC flow logs will help you identify the specific traffic that is being routed through the NAT gateway. This is crucial for understanding which parts of your architecture are causing the excessive NAT gateway usage. By analyzing these logs, you can pinpoint whether traffic to services like Amazon S3, DynamoDB, or other external services is responsible for the high costs. VPC endpoints (specifically gateway endpoints for S3 and DynamoDB) allow traffic between your VPC and these AWS services to bypass the NAT gateway, thus reducing the data transfer costs associated with the NAT gateway. Ensuring that these endpoints are correctly configured and associated with the route tables of your private subnets will ensure that traffic to S3 and DynamoDB does not unnecessarily traverse the NAT gateway.

komorebi 1 year, 7 months ago

Selected Answer: BD

Answer is BD

jhon648274 1 year, 7 months ago

BE Endpoints can be used to access the s3 and dynamodb services at a reduced cost - avoids using nat gateway S3 vpc endpoint gateway is free

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #214 Topic 1

A company ran out of IP address space in one of the Availability Zones in an AWS Region that the company uses. The Availability Zone that is out of space is assigned the 10.10.1.0/24 CIDR block. The company manages its networking configurations in an AWS CloudFormation stack. The company' VPC is assigned the 10 10.0.0/16 CIDR block and has available capacity in the 10.10.1.0/22 CIDR block.

How should a network specialist add more IP address space in the existing VPC with the LEAST operational overhead?

A. Update the AWS::EC2::Subnet resource for the Availability Zone in the CloudFormation stack. Change the CidrBlock property to 10.10.1.0/22.

B. Update the AWS::EC2::VPC resource in the CloudFormation stack. Change the CidrBlock property to 10.10.1.0/22.

C. Copy the CloudFormation stack. Set the AWS::EC2::VPC resource CidrBlock property to 10.10.0.0/16. Set the AWS::EC2::Subnet resource CidrBlock property to 10.10.1.0/22 for the Availability Zone.

D. Create a new AWS::EC2::Subnet resource for the Availability Zone in the CloudFormation stack. Set the CidrBlock property to 10.10.2.0/24. Most Voted

Correct Answer: D

Community vote distribution

D (92%) A (8%)

Comments

Cacheirez Highly Voted 1 year, 7 months ago

Selected Answer: D

By creating a new subnet with a different CIDR block (10.10.2.0/24) within the same Availability Zone, you can expand the IP address space available for that AZ without altering existing configurations. This approach is straightforward and minimizes the risk of disruption to the existing resources. This option allows you to quickly and easily increase the available IP space without needing to modify or replace existing subnets, which could cause service disruptions or require reassigning resources within the AZ. It avoids the complexities and potential issues associated with resizing subnets or VPCs, which can be more involved and risky. Changing the CIDR block of an existing subnet is not supported directly because subnets cannot be resized or modified after creation. Doing so would require deleting and recreating the subnet, which would disrupt any resources tied to it.

AzureDP900 1 year, 2 months ago

Selected Answer: D

To add more IP address space in the existing VPC with the LEAST operational overhead, I would recommend: • D. Create a new AWS::EC2::Subnet resource for the Availability Zone in the CloudFormation stack. Set the CidrBlock property to 10.10.1.0/24. This option has minimal operational overhead because it doesn't require any changes to existing infrastructure or resources within the VPC. It simply creates a new subnet with a larger CIDR block, which can be used to provide additional IP addresses.

Spaurito 1 year, 4 months ago

D - This meets the requirements and is the solution. The others would not work and CF will rebuild the subnet if provisioned.

VerRi 1 year, 5 months ago

Selected Answer: D

A. Cannot update CIDR of the existing subnet B. Cannot update CIDR of the existing subnet C. Not recommended for IP Reassignment

qomtodie 1 year, 6 months ago

Selected Answer: D

This is D

cas_tori 1 year, 6 months ago

Selected Answer: D

this is D

aragon_saa 1 year, 7 months ago

Selected Answer: A

Answer is A

https://zhangxuetu.online

[202610]

Question #215 Topic 1

A company's network engineer must implement a cloud-based networking environment for a network operations team to centrally manage. Other Teams will use the environment. Each team must be able to deploy infrastructure to the environment and must be able to manage its own resources. The environment must feature IPv4 and IPv6 support and must provide internet connectivity in a dual-stack configuration.

The company has an organization in AWS Organizations that contains a workload account for the teams. The network engineer creates a new networking account in the organization.

Which combination of steps should the network engineer take next to meet the requirements? (Choose three.)

A. Create a new VPC. Associate an IPv4 CIDR block of 10.0.0.0/16 and specify an IPv6 block of 2001:db8:c5a:6000::/56. Provision subnets by assigning /24 IPv4 CIDR blocks and /64 IPv6 CIDR blocks.

B. Create a new VPC. Associate an IPv4 CIDR block of 10.0.0.0/16 and use an Amazon-provided IPV6 CIDR block. Provision subnets by assigning /24 IPv4 CIDR blocks and /64 IPV6 CIDR blocks. Most Voted

C. Enable sharing of resources within the organization by using AWS Resource Access Manager (AWS RAM). Create a resource share in the networking account, select the provisioned subnets, and share the provisioned subnets with the target workload account. Use the workload account to accept the resource share through AWS RAM. Most Voted

D. Enable sharing of resources within the organization by using AWS Resource Access Manager (AWS RAM). Create a resource share in the networking account, select the new VPC, and share the new VPC with the target workload account. Use the workload account to accept the resource share through AWS RAM.

E. Create an internet gateway and an egress-only internal gateway. Deploy NAT gateways to the public subnets. Associate the internet gateway with the new VPC. Update the route tables. Associate the route tables with the relevant subnets. Most Voted

F. Create an internet gateway. Deploy NAT instances to public subnets. Update the route tables. Associate the route tables with the relevant subnets.

Correct Answer: BCE

Community vote distribution

BCE (83%) ACE (17%)

Comments

Cacheirez Highly Voted 1 year, 7 months ago

Selected Answer: BCE

BCE are better options than the rest: Option A: Specifies a manual IPv6 block rather than using Amazon-provided IPv6 blocks, which are preferred for their global uniqueness and routability. Option D: Suggests sharing an entire VPC, which is less secure and harder to manage compared to sharing specific subnets. Option F: Suggests using NAT instances, which are less scalable and more maintenance-intensive than NAT gateways.

46f094c 1 year, 2 months ago

Selected Answer: BCE

A: range /48 and bigger (space-wise) is possible to import to AWS, not a smaller one like /56 in the question

woorkim 1 year, 3 months ago

B,C,E ois correct! A. Manually specifying an IPv6 block is unnecessary D. Sharing the entire VPC would give workload accounts full control over the VPC, which is not desirable in a centrally managed networking setup. F. Using NAT instances introduces operational overhead and is not recommended unless cost is a critical concern.

cas_tori 1 year, 6 months ago

Selected Answer: BCE

this is BCE

aragon_saa 1 year, 7 months ago

Selected Answer: ACE

Answer is ACE

AzureDP900 1 year, 2 months ago

yes, ACE is correct This step provides internet connectivity for the VPC, enabling communication between the VPC and the internet. The egress-only internal gateway ensures that only outgoing traffic from the VPC can access the internet, while the NAT gateways provide necessary network address translation for incoming traffic.

https://zhangxuetu.online

[202610]

Question #216 Topic 1

A company is using third-party firewall appliances to monitor and inspect traffic on premises. The company wants to use the same model on AWS. The Company has a single VPC with an internet gateway. The VPC has a fleet of web servers that run on Amazon EC2 instances that are managed by an Auto Scaling group.

The company's network team needs to work with the security team to establish inline inspection of all packets that are sent to and from the web servers. The solution must scale as the fleet of virtual firewall appliances scales

Which combination of steps should the network team take to implement this solution? (Choose three.)

A. Create a new VPC, and deploy a fleet of firewall appliances. Create a Gateway Load Balancer. Add the firewall appliances as targets. **Most Voted**

B. Create a security group for use with the firewall appliances, and allow port 443. Allow a port for the Galeway Load Balancer to perform health checks.

C. Create a security group for use with the firewall appliances, and allow port 6081. Allow a port for the Gateway Load Balancer to perform health checks. **Most Voted**

D. Deploy a fleet of firewall appliances to the existing VPC. Create a Gateway Load Balancer. Add the firewall appliances as targets.

E. Update the internet gateway route table and the web server route table to send traffic to and from the internet to the VPC endpoint ID of the Gateway Load Balancer. Update the subnet route table that is associated with the Gateway Load Balancer endpoint to direct internet traffic to the internet gateway.

F. Create a new route table inside the web server VPC. Create a new edge association with the internet gateway. Update the internet gateway route table and the web server route table to send traffic to and from the internet to the VPC endpoint ID of the Gateway Load Balancer. Update the subnet route table that is associated with the Gateway Load Balancer endpoint to direct internet traffic to the internet gateway. **Most Voted**

Correct Answer: ACF

Community vote distribution



Comments

18641c6 **Highly Voted** 1 year ago

Selected Answer: ACF

I don't see why ACE is correct, I prefer ACF. When you create a new VPC there is no route table with edge association. So, a new route table must be created and then it gets associated with the edge. Or do I miss a certain point here?

woorkim **Highly Voted** 1 year, 3 months ago

ACE is answer! B. Port 443 is for HTTPS traffic, but this does not apply to the Gateway Load Balancer D. Deploying the firewalls in the same VPC as the web servers complicates routing and scaling F. Creating a new edge association with the internet gateway is unnecessary. Updating the existing route tables (as described in Option E) is sufficient to route traffic through the Gateway Load Balancer.

a0e6696 7 months ago

Selected Answer: ACF

I will go with the ACF as here they didn't mention webserver hosted in the which subnet[public or private]

Wardove 11 months ago

Selected Answer: ACF

There is no way to define route for IGW out of the box, you need a new RT and edge association.

Canvill 1 year, 1 month ago

Selected Answer: CDF

CDF. Only a single VPC is mentioned

VerRi 1 year, 5 months ago

Selected Answer: ACE

ACE is good for this case

AlirezaNetWorld 1 year, 6 months ago

ACE is the best answer.

qomtodie 1 year, 6 months ago

Selected Answer: ACE

https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/target-groups.html

cas_tori 1 year, 6 months ago

Selected Answer: DEF

this is DEF

aragon_saa 1 year, 6 months ago

Selected Answer: ADE

Answer is A,D,E

https://zhangxuetu.online

[202610]

Question #217 Topic 1

A financial company offers investment forecasts and recommendations to authorized users through the internet. All the services are hosted in the AWS Cloud. A new compliance requirement states that all the internet service traffic from any host must be logged and retained for 2 years. In its development AWS accounts, the company has designed, tested, and verified a solution that uses Amazon VPC Traffic Mirroring with a Network Load Balancer (NLB) as the traffic mirror target. While the solution runs in one AWS account, the solution mirrors the traffic to another AWS account.

A network engineer notices that not all traffic is mirrored when the solution is deployed into the production environment. The network engineer also notices that this behavior is random.

Which statements are possible explanations for why not all the traffic is mirrored? (Choose two.)

A. The security groups are misconfigured on the production AWS account that hosts the company's services.

B. The Amazon EC2 instance that is being monitored cannot handle the extra traffic that Traffic Mirroring has introduced. Most Voted

C. The IAM policy that allows the creation of traffic mirror sessions is misconfigured

D. The mirrored traffic has a lower priority than the production traffic and is being dropped when network congestion occurs. Most Voted

E. The NLB is experiencing warm-up delay because of sudden and significant increases in traffic.

Correct Answer: BD

Community vote distribution



Comments

luisgu Highly Voted 1 year, 6 months ago

Selected Answer: DE

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-network-limitations.html#traffic-mirroring-bandwidth

Ohnet 3 months, 2 weeks ago

Selected Answer: BD

BD>.....

Ohnet 3 months, 3 weeks ago

Selected Answer: BD

BD.....

dcantos 8 months, 2 weeks ago

Selected Answer: BD

B and D B and D

AWSLoverLoverLoverLoverLover 11 months, 3 weeks ago

Selected Answer: BD

Answer B & D

dspd 1 year, 1 month ago

Selected Answer: BD

B and D E can not because The NLB is experiencing warm-up delay because of sudden and significant increases in traffic. While NLBs can experience some warm-up delay when there are sudden traffic increases, this is unlikely to be the primary cause of the random mirroring issues. NLBs are designed to handle high volumes of traffic and scale quickly. The warm-up period is typically short and wouldn't explain ongoing random mirroring failures.

woorkim 1 year, 3 months ago

B, D is correct! A. Traffic Mirroring operates at the ENI level and does not depend on security group configurations. This is unlikely to cause random packet drops. C. Since the issue is random and traffic mirroring is partially working, this is not the cause. E. While NLB warm-up delays can occur, they typically affect the ability to handle new connections, not random packet drops.

Christina666 1 year, 3 months ago

Selected Answer: BD

network congestion can drop the mirror traffic

seongheon 1 year, 6 months ago

Selected Answer: BD

Answer is B, D E is wrong. There is no case NLB is experiencing warm-up delay

kupo777 1 year, 6 months ago

Answer is D, E The following choices can be ruled out because events in which all traffic is not mirrored occur at random. A, C Also, because traffic mirroring is a low priority, The replicated traffic generated by each instance is counted against the total bandwidth available to this instance, and if traffic is delayed, the mirrored traffic is dropped first

cas_tori 1 year, 6 months ago

Selected Answer: DE

this is DE

aragon_saa 1 year, 6 months ago

Selected Answer: AE

Answer is A, E

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #218 Topic 1

A company has a VPC in the AWS Cloud. The company recently acquired a competitor that also has a VPC the AWS Cloud. A network engineer discovers an IP address overlap between the two VPCs. Both VPCs require access to an AWS Marketplace partner service.

Which solution will ensure interoperability among the VPC hosted services and the AWS Markelplace partner service?

A. Configure VPC peering with static routing between the VPCs. Configure an AWS Site-to-Site VPN connection with static routing to the partner service.

B. Configure a NAT gateway in the VPCs. Configure default routes in each VPC to point to the local NAT gateway. Attach each NAT gateway to a transit gateway. Configure an AWS Site-to-Site VPN connection with static routing to the partner service.

C. Configure AWS PrivateLink to facilitate connectivity between the VPCs and the partner service. Use the DNS name that is created with the associated interface endpoints to route traffic between the VPCs and the partner service. **Most Voted**

D. Configure a NAT instance in the VPCs. Configure default routes in each VPC to point to the local NAT instance. Configure an interface endpoint in each VPC to connect to the partner service. Use the DNS name that is created with the associated interface endpoints to route traffic between the VPCs and the partner service.

Correct Answer: C

Community vote distribution

C (100%)

Comments

AzureDP900 1 year, 2 months ago

C is right This solution will ensure interoperability among the VPC hosted services and the AWS Marketplace partner service while avoiding any IP address conflicts. By using AWS PrivateLink, both VPCs can connect directly to the partner service without exposing their private IP addresses to the internet. The interface endpoints created for each VPC will have unique, private DNS names that can be used to route traffic between the VPCs and the partner service. This solution does not require any additional network configurations or routing changes, as traffic will be automatically routed through AWS PrivateLink.

woorkim 1 year, 3 months ago

C is right! A. VPC peering does not support overlapping IP address ranges. B. A transit gateway does not resolve IP overlap issues. The partner service requires a direct interface endpoint (e.g., via PrivateLink) rather than routing through NAT gateways. D.NAT instances do not solve the overlapping IP address problem between VPCs.

ArunRav 1 year, 4 months ago

Selected Answer: C

Since the ips are overlapping, VPC peering is out and also TGW is also. Nat instance option is not preferred when you considered IP overlaps. Hence C is the correct answer

qomtodie 1 year, 6 months ago

Selected Answer: C

Absolutely C

cas_tori 1 year, 6 months ago

Selected Answer: C

this is C

aragon_saa 1 year, 6 months ago

Selected Answer: C

Answer is C

https://zhangxuetu.online

[202610]

Question #219 Topic 1

A company uses the us-east-1 Region and the ap-south-1 Region for its business units (BUs). The BUS are named BU-1 and BU-Z. For each BU, there are two VPCs in us-east-1 and one VPC in ap-south-1.

Because of workload isolation requirements, resources can communicate within the same BU but cannot communicate with resources in the other BU. The company plans to add more BUs and plans to expand into more Regions

Which solution will meet these requirements with the MOST operational efficiency?

A. Configure an AWS Cloud WAN network that operates in the required Regions. Attach all BU VPCs to the AWS Cloud WAN core network. Update the AWS Cloud WAN segment actions to configure new routes to deny traffic between the different BU segments.

B. Configure a transit gateway in each Region. Configure peering between the transit gateways. Attach the BU VPCs to the transit gateway in the corresponding Region. Configure the transit gateway and VPC route tables to isolate traffic between BU VPCs.

C. Configure an AWS Cloud WAN network that operates in the required Regions. Attach all BU VPCs to the AWS Cloud WAN core network. Update the core network policy by setting the isolate-attachments parameter for each segment.

D. Configure an AWS Cloud WAN network that operates in the required Regions. Create AWS Cloud WAN segments for each BU Configure VPC attachments for each BU's VPCs to the corresponding BU segment. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

woorkim 1 year, 3 months ago

Selected Answer: D

A. Using segment actions to deny traffic is less efficient and error-prone compared to using segments for isolation. B. Scaling to multiple BUs and Regions would require more peering connections, route table configurations, and ongoing maintenance. C. isolate-attachments parameter only isolates individual VPC attachments within a single segment. It does not provide logical separation between BUs.

ArunRav 1 year, 4 months ago

Selected Answer: D

D, since segment level isolation is the best option for traffic level isolation.

qomtodie 1 year, 6 months ago

Selected Answer: D

D, I agree

cas_tori 1 year, 6 months ago

Selected Answer: D

this is D

https://zhangxuetu.online

[202610]

Question #220 Topic 1

A company has many application VPCs that use AWS Site-to-Site VPN connections for connectivity to an on-premises location. The company's network team wants to gradually migrate to AWS Transit Gateway to provide VPC-to-VPC connectivity.

The network team sets up a transit gateway that uses equal-cost multi-path (ECMP) routing. The network team attaches two temporary VPCs to the transit gateway for testing. The test VPCs contain Amazon EC2 instances to confirm connectivity over the transit gateway between the on-premises location and the VPCs. The network team creates two new Site-to-Site VPN connections to the transit gateway.

During testing, the network team cannot reach the required bandwidth of 2.5 Gbps over the pair of new Site-o-Site VPN connections.

Which combination of steps should the network team take to improve bandwidth performance and minimize network congestion? (Choose three.)

A. Enable acceleration for the existing Site-to-Site VPN connections to the transit gateway.

B. Create new accelerated Site-to-Site VPN connections to the transit gateway. Most Voted

C. Advertise the on-premises prefix to AWS with the same BGP AS_PATH attribute across all the Site-to-Site VPN connections. Most Voted

D. Advertise the on-premises prefix to AWS with a different BGP AS_PATH attribute across all the Site-to-Site VPN connections.

E. Verify that the transit gateway attachments are present in the Availability Zones of the test VPC.

F. Verify that the on-premises location is sending traffic by using multiple lows. Most Voted

Correct Answer: BCF

Community vote distribution



Comments

luisgu Highly Voted 1 year, 6 months ago

Selected Answer: BCF

https://repost.aws/knowledge-center/transit-gateway-ecmp-multiple-tunnels It's C and not D

luisgu 1 year, 6 months ago

It is B and not A because you cannot enable acceleration on existing VPN connections.

Nouwara 10 months, 1 week ago

Selected Answer: BCF

lows =flows ;)

dspd 1 year, 1 month ago

Selected Answer: BCF

lows should be flow ?

AzureDP900 1 year, 2 months ago

Selected Answer: BCF

The correct answers are: B, C, and F. Create new accelerated Site-to-Site VPN connections to the transit gateway (Option B). Acceleration enables higher bandwidth and lower latency performance for your VPN connections. Advertise the on-premises prefix to AWS with the same BGP AS_PATH attribute across all the Site-to-Site VPN connections (Option C). Having consistent BGP AS_PATH attributes ensures optimal routing and reduces the chances of network congestion or suboptimal paths. Verify that the on-premises location is sending traffic by using multiple Availability Zones (Option F). Ensuring that the on-premises location is sending traffic from multiple availability zones will help distribute the load and prevent any single zone from becoming a bottleneck, thus improving overall performance and reducing network congestion.

woorkim 1 year, 3 months ago

Selected Answer: BCF

A. Acceleration cannot be retroactively applied to existing Site-to-Site VPN connections. New accelerated VPN connections must be created. D. This negates ECMP routing and leads to underutilization of available bandwidth. E. Transit gateway attachments are not specific to Availability Zones.

ArunRav 1 year, 4 months ago

Selected Answer: BCF

B- Because you need a new Site to Site VPN for enabling acceleration, hence not A C-ECMP requires same attribute to make sure the flow is uniform, hence not D F-Multiple traffic flow from on-premises will help to increase the traffic bandwidth.

siheom 1 year, 6 months ago

Selected Answer: BCF

vote BCF

cas_tori 1 year, 6 months ago

Selected Answer: BDF

this is BDF

ForDummies 1 year, 6 months ago

Well, BCF

hcong 1 year, 7 months ago

Selected Answer: BDF

This combination provides a comprehensive approach to improving bandwidth performance: Improve the performance of individual connections by speeding up VPNs Achieve better load balancing through BGP routing optimization More efficient use of available bandwidth through multi-stream transmission Option A is less effective than B because creating a new accelerated connection is more flexible than modifying an existing one. Option C uses the same AS_PATH attribute, which may not take full advantage of ECMP routing. Although important, option E has less direct

impact on improving bandwidth performance. By implementing B, D, and F, network teams can significantly improve bandwidth performance while minimizing network congestion.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #221 Topic 1

A company is migrating its on-premises network from its data center in Virginia to its data center in New York. The AWS Direct Connect connections for the Virginia and New York data center locations are both associated to the us-east-1 Region. The company needs to migrate a private VIF on an existing Direct Connect hosted connection from Virginia to New York. The company's on-premises network uses the connection to access VPCs through a Direct Connect gateway in us-east-1.

The company has already requested a new Direct Connect hosted connection from the new data center to the New York Direct Connect location.

Which solution will meet these requirements with the LEAST downtime?

A. Create a new private VIF on the new Direct Connect hosted connection. Create a new Direct Connect gateway and attach the gateway to the new private VIF. Configure BGP routing on the new private VIF as a backup route. Perform the switchover during a maintenance window by shutting down BGP on the existing private VIF. Decommission the existing Direct Connect connection.

B. Create a new private VIF on the new Direct Connect hosted connection. Attach the new private VIF to the existing Direct Connect gateway. Configure BGP routing on the new private VIF as a backup route. Perform the switchover during a maintenance window by shutting down BGP on the existing private VIF. Decommission the existing Direct Connect connection. **Most Voted**

C. During a maintenance window, migrate the existing private VIF to the new Direct Connect hosted connection. Attach the existing private VIF to the existing Direct Connect gateway. Decommission the existing Direct Connect connection.

D. During a maintenance window, delete the existing private VIF and create a new private VIF to the new Direct Connect hosted connection. Attach the new private VIF to the existing Direct Connect gateway. Decommission the existing Direct Connect hosted connection.

Correct Answer: B

Community vote distribution

B (100%)

Comments

AzureDP900 1 year, 2 months ago

B: Create a new private VIF on the new Direct Connect hosted connection. Attach the new private VIF to the existing Direct Connect gateway. Configure BGP routing on the new private VIF as a backup route. Perform the switchover

during a maintenance window by shutting down BGP on the existing private VIF. Decommission the existing Direct Connect connection.

AzureDP900 1 year, 2 months ago

With the AS_PATH attribute values, it's clear that VIF 2 has a more specific network address and uses the same AS_PATH value as VIF 1, but with an additional path element. This means that when traffic is sent from the Direct Connect gateway with a destination address in the 172.16.1.0/24 network range, AWS will use VIF 2 to route the traffic. So, the correct answer is indeed B: AWS will route all traffic by using VIF 2.

woorkim 1 year, 3 months ago

Selected Answer: B

Option A:Creating a new Direct Connect gateway introduces unnecessary complexity and does not align with the requirement to use the existing gateway. Option C:Migrating the existing private VIF directly to the new connection during the maintenance window would cause downtime because the VIF would need to be detached and reattached. Option D:Deleting the existing private VIF before creating a new one would lead to downtime, as there would be no active connection during the transition.

Nel07 1 year, 4 months ago

least downtime with backup. So the answer is B

ArunRav 1 year, 4 months ago

Selected Answer: B

Since we are setting a new connection as a backup route before we disable the old connection, it provide a lowest downtime.

https://zhangxuetu.online

[202610]

Question #222 Topic 1

A retail company is migrating its on-premises application to the AWS Cloud. Currently, the company has two on-premises data center locations. One data center is on the east coast of the United States, and one data center is on the west coast.

Each data center hosts four database systems. The largest database system stores 500 GB of data. The data centers are interconnected by two 10 GbE circuits for data synchronization. Each data center has two separate 1 GbE upstream internet connections. The company plans to have eight total VPCs to service its multiple business units. Four VPCs will be in the us-east-1 Region, and four will be in the us-west-2 Region.

A network engineer needs to design a connectivity solution that allows VPC-to-VPC connectivity. The solution must also allow secure connections between the on-premises data centers and AWS during the migration process. The company expects spikes in traffic among the VPCs during database synchronization. The company wants to run the migration plan during one weekend and as soon as technically possible. The company also wants to minimize long-term operational and human resources costs.

Which combination of steps will meet these requirements? (Choose two.)

A. Deploy one transit gateway and attach all VPCs to it. Update the transit gateway and VPC route tables to allow any VPC to connect to any other VPC.

B. Configure VPC peering between all the VPCs. Update the VPC route tables to allow connectivity. Most Voted

C. Provision two AWS Direct Connect connections from two Direct Connect locations that serve us-east-1 and us-west-2 to provide connectivity between the data centers and AWS.

D. Provision one transit gateway VPN attachment for each data center to build connectivity between the on-premises data centers and AWS VPCs.

E. Provision one AWS Site-to-Site VPN connection for each data center and for each VPC to build connectivity between the on-premises data centers and AWS VPCs. Most Voted

Correct Answer: BE

Community vote distribution



Comments

secdaddy Highly Voted 1 year, 1 month ago

Selected Answer: BE

Voted solution CD doesn't work as does not provide VPC-VPC connectivity. A is hard out as VPC-TGW cross regional peering is impossible. Without A we can also eliminate D as A was the only one provisioning TGW. C and E both say between DCs and AWS so we are left with B for VPC-VPC (also keeping long term costs down) and either C or E for DC-AWS. C is generally better but slower to put in place whereas E gives us both faster deployment and secure connections for the migration. E should provide enough bandwidth to accomplish the migration during a weekend. If we assume the DCs go away post migration DX is even less interesting.

49ca6f2 1 year, 1 month ago

This looks like only possible explanation. A is definitely wrong option. TGW won't allow the cross region vpc attachment. And DX is slow , not cost effective. VPN is faster to deploy and plus it is cost effective. Correct option is BE.

953bf6d 6 months ago

Selected Answer: AC

Interpret Option A as “use Transit Gateway for VPC-to-VPC,” which in practice means: Create two TGWs: one in us-east-1 and one in us-west-2. Attach the four local VPCs to their regional TGW. Create a TGW peering attachment between the two TGWs and add routes so VPCs can talk cross-Region. Then pair with Option C: Build two Direct Connect connections and a DX Gateway. Associate the DX Gateway with both TGWs (DXGW–TGW associations) so on-prem can reach all VPCs in both Regions. Enable route propagation/advertisements via BGP as needed. This gives transitive VPC-to-VPC and on-prem connectivity across both Regions with low operational overhead.

8be7437 11 months, 1 week ago

Selected Answer: DE

This is broken. It cannot be A because we have 2 regions, and you would need 2 TGW. B is broken because peering of 8 VPC would not "minimize long-term operational and human..." 28 peerings! C is broken because they want to do this "as soon as technically possible" and a direct connect takes 3 months! D may be broken, even if it looks ok, but it doesn't mention association to VPC, and you need the TGW (see A!). E Also is broken because something is missing in the wording and if "for each VPC, a VPN" that is not sustainable either. Since we have to choose two, this question does VERY little sense. So the ones I feel approximate is D and E, because I bet the missing part on E I presume may be correcting this mess.

1a17d1e 8 months, 2 weeks ago

Like your thought process, but I'd choose B over D because it doesn't say that there would be a lot more peerings necessary in the future so long term it wouldn't be too big a long-term operational nightmare administrative burden, fits the traffic requirements, is better on costs, etc. I'm going with B, E.

AWSLoverLoverLoverLoverLover 11 months, 3 weeks ago

Selected Answer: CD

C & D are correct human resources costs. Not cost

ashk123456 11 months, 4 weeks ago

Selected Answer: AC

AC are corrected

jfedotov 1 year, 2 months ago

Selected Answer: CD

CD are correct

AzureDP900 1 year, 2 months ago

Selected Answer: CD

The combination of C and D meets the requirements: VPC-to-VPC connectivity: The Direct Connect connections provide direct access to the VPCs, allowing them to communicate with each other. Secure connections between on-premises data centers and AWS: The transit gateway VPN attachments ensure secure connections between the data centers and AWS, enabling database synchronization. The other options do not meet all the requirements: A provides VPC-to-VPC connectivity but does not provide direct connections to the on-premises data centers. B provides VPC-to-VPC connectivity but may not be the most efficient or cost-effective solution for the company's needs. E is not necessary, as it would require multiple Site-to-Site VPN connections that would increase operational costs.

18641c6 1 year ago

Well, VPC-to-VPC is definitely more cost-effective than TGW or direct connections. So I definitely choose B. One transit gateway is not sufficient, since TGWs are regional. So I prefer E over D

mic8 1 year, 3 months ago

Selected Answer: CD

Since a single transit gateway cannot attach VPCs from different regions, option A is indeed incorrect.

ArunRav 1 year, 4 months ago

Selected Answer: AC

A - to minimise the operational cost and handle traffic spike C - help the steady and low latency connection

Nel07 1 year, 4 months ago

A is faulse. we can't attach VPC in different regions to the same TGW. TGW is a regional service

https://zhangxuetu.online

[202610]

Question #223 Topic 1

A company is developing an API-based application on AWS for its process workflow requirements. The API will be invoked by clients in the company's on-premises data centers. The company has set up an AWS Direct Connect connection between on premises and AWS. A network engineer decides to implement the API as a private REST API in Amazon API Gateway. The network engineer wants to ensure that clients can reach the API endpoint through private communication.

Which solution can the network engineer use to invoke the API without any additional infrastructure setup?

A. Create an interface VPC endpoint for API Gateway with private DNS names enabled. Access the API by using the private DNS name of the endpoint.

B. Create an interface VPC endpoint for API Gateway with private DNS names enabled. Access the API by using an Amazon Route 53 alias of the endpoint.

C. Create an interface VPC endpoint for API Gateway. Associate the endpoint with the private REST API, Access the API by using an Amazon Route 53 alias of the endpoint.

D. Create an interface VPC endpoint for API Gateway with private DNS names enabled. Access the API by using the public DNS name of the endpoint. Most Voted

Correct Answer: D

Community vote distribution



Comments

304faa7 Highly Voted 1 year, 3 months ago

Selected Answer: D

D is the correct answer here as we don't want to setup additional infra(inbound endpoints) here as asked in the question. Only through inbound endpoints we will be able to use private DNS. Below is from AWS documentation : its a tricky question. Invoke a private API using AWS Direct Connect You can use AWS Direct Connect to establish a dedicated private connection from an on-premises network to Amazon VPC and access your private API endpoint over that connection by using public DNS names. You can also use private DNS names to access your private API from an on-premises network by setting up an Amazon Route 53 Resolver inbound endpoint and forwarding it all DNS queries of the private DNS from your remote network. For more information, see Forwarding inbound DNS queries to your VPCs in the Amazon Route 53 Developer Guide

a0e6696 7 months ago

Selected Answer: A

to use public dns, AWS side we will have to created route53 inbound endpoint and on-prem side need to change DNS configuration to forward to IP address of route53 inbound endpoint

a0e6696 7 months ago

Selected Answer: A

In AWS VPC, using the public endpoint will work and it will resolve the private IP address. But, how on-prem will come to know the private IP address for the public endpoint. Here we need additional configuration from the on-prem side to either DNS mapping or forwarding domain to AWS using the Route53 resolver endpoint. In this case, I will go with the A.

8be7437 11 months, 1 week ago

Selected Answer: D

mmmmmm but. is creating an alias "creating additional infrastructure setup?" I guess it is ok to let C out because there is no mentioning of R53, unless it is implicit with "through private communitation". This are very bad questions

dspd 1 year, 1 month ago

Selected Answer: C

Answer C D - This option is incorrect because it suggests using the public DNS name of the endpoint, which contradicts the requirement for private communication. Additionally, like options A and B, it doesn't mention the necessary step of associating the endpoint with the private REST API.

chrootxxx 1 year, 3 months ago

Selected Answer: D

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-api-test-invoke-url.html Invoke a private API using AWS Direct Connect You can use AWS Direct Connect to establish a dedicated private connection from an on-premises network to Amazon VPC and access your private API endpoint over that connection by using public DNS names.

304faa7 1 year, 4 months ago

D is the correct answer here as we don't want to setup additional infra(inbound endpoints) here as asked in the question. Only through inbound endpoints we will be able to use private DNS. Below is from AWS documentation : its a tricky question. Invoke a private API using AWS Direct Connect You can use AWS Direct Connect to establish a dedicated private connection from an on-premises network to Amazon VPC and access your private API endpoint over that connection by using public DNS names. You can also use private DNS names to access your private API from an on-premises network by setting up an Amazon Route 53 Resolver inbound endpoint and forwarding it all DNS queries of the private DNS from your remote network. For more information, see Forwarding inbound DNS queries to your VPCs in the Amazon Route 53 Developer Guide.

Nel07 1 year, 4 months ago

Selected Answer: A

option A

ArunRav 1 year, 4 months ago

Selected Answer: A

Using option A, engineer can invoke API end point connectivity using private communication and can avoid additional route 53 setup needed

304faa7 1 year, 4 months ago

D is the correct answer ; https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-api-test-invoke-url.html#w78aac15c20c17c15c17

ArunRav 1 year, 4 months ago

https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-api-test-invoke-url.html#w78aac15c20c17c15c15

https://zhangxuetu.online

[202610]

Question #224 Topic 1

A banking company has an application that must connect to specific public IP addresses from a VPC. A network engineer has configured routes in the route table that is associated with the application's subnet to the required public IP addresses through an internet gateway.

The network engineer needs to set up email notifications that will alert the network engineer when a user adds a default route to the application subnet's route table with the internet gateway as a target.

Which solution will meet these requirements with the LEAST implementation effort?

A. Create an AWS Lambda function that reads the routes in the route table and sends an email notification. Configure the Lambda function to send an email notification if any route is configured with 0.0.0.0/0 or ::/0 CIDRs to the internet gateway. Configure the Lambda function to run every minute.

B. Create an AWS Lambda function that will be invoked by an Amazon EC2 CreateRoute API call. Configure the Lambda function to send an email notification. Configure the Lambda function to send an email notification if any route is configured with 0.0.0.0/0 or ::/0 CIDRs to the internet gateway.

C. Create AWS Config rules for the route table by using the internet-gateway-authorized-vpc-only managed rule. Create an Amazon EventBridge rule to match the AWS Config rule and to route to an Amazon Simple Notification Service (Amazon SNS) topic to send an email notification.

D. Create an AWS Config rule for the route table by using the no-unrestricted-route-to-igw managed rule. Create an Amazon EventBridge rule to match the AWS Config rule and to route to an Amazon Simple Notification Service (Amazon SNS) topic to send an email notification. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

AzureDP900 1 year, 2 months ago

Selected Answer: D

This solution has less implementation effort because: It uses a pre-configured AWS managed rule (no-unrestricted-route-to-igw) that is specifically designed for this use case, eliminating the need to write custom code. It leverages Amazon EventBridge (formerly CloudWatch Events) and Amazon SNS, which are well-established services with minimal configuration required.

AzureDP900 1 year, 2 months ago

Selected Answer: D

D Create an AWS Config rule for the route table by using the no-unrestricted-route-to-igw managed rule would meet these requirements with the LEAST implementation effort. This solution leverages pre-built AWS Config rules, which monitor the resource configuration and trigger an Amazon EventBridge rule when a rule violation is detected. The email notification can then be sent to the network engineer through an Amazon SNS topic.

woorkim 1 year, 3 months ago

Selected Answer: D

C. AWS Config rule using internet-gateway-authorized-vpc-only: This rule checks if an internet gateway is attached only to authorized VPCs. It does not specifically monitor for unrestricted routes (0.0.0.0/0 or ::/0) to the internet gateway, which is the requirement.

meseerie 1 year, 3 months ago

Selected Answer: D

answer is cleary D https://docs.aws.amazon.com/config/latest/developerguide/no-unrestricted-route-to-igw.html "Checks if there are public routes in the route table to an Internet gateway (IGW). The rule is NON_COMPLIANT if a route to an IGW has a destination CIDR block of '0.0.0.0/0' or '::/0' or if a destination CIDR block does not match the rule parameter."

ArunRav 1 year, 4 months ago

Selected Answer: D

A and B is out as lambda need effort. C only check if igw is attached to authorized vpc. For checking unrestricted route getting attached to igw D is the best option and needs very less operational effort as it is using aws native tool.

46f094c 1 year, 4 months ago

Selected Answer: C

https://docs.aws.amazon.com/config/latest/developerguide/no-unrestricted-route-to-igw.html

https://zhangxuetu.online

[202610]

Question #225 Topic 1

A company is building an internet-facing application that is hosted on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The company is using the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes for pod networking connectivity. The company needs to expose its application to the internet by using a Network Load Balancer (NLB).
The pods that host the application must have visibility of the source IP address that is contained in the original packet that the NLB receives.

How should the network engineer configure the NLB and Amazon EKS settings to achieve these goals?

A. Specify the ip target type for the NLB. Set the externalTrafficPolicy attribute to Local in the Kubernetes service specification. **Most Voted**

B. Specify the instance target type for the NLSet the externalTrafficPolicy attribute to Cluster in the Kubernetes service specification.

C. Specify the instance target type for the NLB. Set the externalTrafficPolicy attribute to Local in the Kubernetes service specification.

D. Specify the ip target type for the NLB. Set the externalTrafficPolicy attribute to Cluster in the Kubernetes service specification.

Correct Answer: A

Community vote distribution

A (100%)

Comments

zanhsieh 1 year ago

Selected Answer: A

https://docs.aws.amazon.com/eks/latest/best-practices/load-balancing.html#:~:text=service.beta.kubernetes.io/aws%2Dload%2Dbalancer%2Dnlb%2Dtarget%2Dtype%3A%20ip
https://docs.aws.amazon.com/eks/latest/best-practices/sgpp.html#:~:text=Kubernetes%20services%20support-,externalTrafficPolicy,-%3Dlocal%20to%20support

woorkim 1 year, 3 months ago

Selected Answer: A

To expose an internet-facing application with source IP visibility, use the ip target type for the NLB and set the Kubernetes service's externalTrafficPolicy to Local. This configuration ensures that the original source IP address is preserved and visible to the pods.

ArunRav 1 year, 4 months ago

Selected Answer: A

ip target type make sure that NLB send the traffic to pod ips. externalTrafficPolicy to local will help the pod ips to be shown. Combining both of these options will help to meet the requirements.

https://zhangxuetu.online

[202610]

Question #226 Topic 1

A company is running its application servers on Amazon EC2 instances. The EC2 instances run in separate VPCs that are connected by a transit gateway. The EC2 instances launch in a private subnet with a route to the transit gateway for internal and external connectivity. The external connectivity is provided by a VPC with firewall devices that perform an inspection for packets that ingress and egress through an internet gateway.

A network engineer needs to help the company's application team increase the payload size per packet delivery between the EC2 instances. All network connectivity must be through the transit gateway

What should the network engineer do to meet these requirements?

A. Enable jumbo frames on the transit gateway. Instruct the application team to set the maximum transmission unit (MTU) of the system's network interfaces to 9001 bytes.

B. Instruct the application team to set the maximum transmission unit (MTU) of the VPC to 8500 bytes.

C. Instruct the application team to set up enhanced networking on the system by using the enhanced networking adapter. Set the maximum transmission unit (MTU) to 9001 bytes.

D. Instruct the application team to set the maximum transmission unit (MTU) of the system's network interfaces to 8500 bytes. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: A

To achieve jumbo frame support, the MTU should be set to 9001 bytes, not 8500 bytes.

49ca6f2 1 year, 1 month ago

Selected Answer: C

I think answer is C. TGW supports 8500 MTU by default and enforces MSS Clamping on all traffic. Hence if the EC2 is 9001 with Enhanced networking , MSS clamping on TGW will ensure that EC2 sends only 8500 and does not exceeds the MTU of TGW.

woorkim 1 year, 3 months ago

Selected Answer: D

The correct answer is D because: 8500 bytes is the maximum MTU supported by Transit Gateway Setting the system interfaces to 8500 ensures compatibility Prevents packet fragmentation Maximizes payload size while maintaining network stability Works with the existing architecture including firewalls

0acf5ca 1 year, 3 months ago

Selected Answer: D

D - All network connectivity between EC2 instances must be through the transit gateway. Although MTU 9001 is enabled on EC2 by default and MTU 8500 is enabled on TGW by default, any frame more than 8500 bytes would be silently dropped by TGW.

a4002bd 1 year, 3 months ago

Selected Answer: D

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-quotas.html D. Packets with a size larger than 8500 bytes that arrive at the transit gateway are dropped.

304faa7 1 year, 4 months ago

Correct Answer is D

Momiac5 1 year, 4 months ago

D Question: "All network connectivity must be through the transit gateway" Docs: Packets with a size larger than 8500 bytes that arrive at the transit gateway are dropped. https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-quotas.html

ArunRav 1 year, 4 months ago

Selected Answer: A

Enabling Jumbo frames and setting up MTU of the network interfaces to 9001 will help to improve the connectivity.

https://zhangxuetu.online

[202610]

Question #227 Topic 1

A network engineer needs to monitor internet metrics for an application that is in a VPC. The metrics include user experiences such as health events, latency, and traffic insights.

The network engineer sets up Amazon CloudWatch Internet Monitor for the application. The engineer wants to push the internet health events to a third-party target.

Which solution will meet these requirements with the LEAST implementation effort?

A. Create a third-party API endpoint in Amazon EventBridge. Configure internet Monitor to send the events to the third-party API endpoint in EventBridge.

B. Create a third-party API endpoint in Amazon EventBridge. Create a rule in EventBridge that uses Internet Monitor as the source and the third-party API endpoint in EventBridge as the destination. **Most Voted**

C. Create a third-party API endpoint in internet Monitor. Configure Internet Monitor to send the events to an Amazon S3 bucket. Configure an AWS Lambda function to send the events to the third-party API endpoint in Internet Monitor.

D. Create a third-party API endpoint in Internet Monitor. Configure Internet Monitor to send the events to the third-party API endpoint in Internet Monitor.

Correct Answer: B

Community vote distribution

B (100%)

Comments

youonebe 1 year ago

Selected Answer: B

Answer is B, not D

woorkim 1 year, 3 months ago

Selected Answer: B

https://aws.amazon.com/blogs/networking-and-content-delivery/using-amazon-cloudwatch-internet-monitor-for-enhanced-internet-observability/ low-effort solution is to use Amazon EventBridge to create a rule that routes Internet Monitor events to the third-party API endpoint. This approach leverages native AWS integrations and avoids unnecessary complexity.

ArunRav 1 year, 4 months ago

Selected Answer: B

By setting a rule and forwarding the events to the third party endpoint will be least effort required option.

https://zhangxuetu.online

[202610]

Question #228 Topic 1

A company has a web application that runs in eight AWS Regions. In each Region, the application is hosted on multiple compute resources behind an Application Load Balancer (ALB).

The different Regions are using different domains. Each ALB is configured to accept only HTTPS traffic. Each ALB uses a certificate from AWS Certificate Manager (ACM).

The company wants to simplify the application's appearance on the web by using a new single domain for all Regions. A network engineer needs to implement this change by designing a solution that also will minimize latency for the application's end users.

Which combination of actions will meet these requirements? (Choose three.)

A. Use ACM to create an SSL/TLS certificate in the us-east-1 Region for the new domain.

B. Set up latency-based routing in Amazon Route 53 for the new domain. Add the ALBs from all the Regions as targets.

C. Create an alias record for the accelerator in Amazon Route 53 for the new domain. Most Voted

D. Create a standard accelerator in AWS Global Accelerator. Configure a listener for TCP traffic. Add all the ALBs as targets for the listener. Most Voted

E. Use ACM to create an SSLITLS certificate for each Region. Configure all the ALBs to use the certificate in their respective Regions. Most Voted

F. Create a custom routing accelerator in AWS Global Accelerator. Configure a listener for HTTPS traffic. Add all the ALBs as targets for the listener. Configure the accelerator to terminate TLS by using the SSLITLS certificate from ACM.

Correct Answer: CDE

Community vote distribution



Comments

youonebe 1 year ago

Selected Answer: ACD

For edge-optimized services like Global Accelerator, ACM certificates must be created in the us-east-1 Region. This certificate will be used for the single domain that will front all regional deployments.

https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-specify-certificate-for-custom-domain-name.html

secdaddy 1 year, 1 month ago

Selected Answer: ACF

Accelerator better than Route 53 as anycast and not dependent on DNS and delay measurement. (A) GA uses single certificate that must be in us-east-1. Need the alias (C) for GA to work. (F) Custom accelerator terminates TLS using the new certificate from (A).

djangoGroup 1 year, 2 months ago

Selected Answer: CDE

(C) Create an alias record for the accelerator in Route 53 for the new domain • This step stays the same. You want your users to resolve a single domain that leads to Global Accelerator. • (D) Create a standard accelerator in AWS Global Accelerator, configure a listener for TCP (or TLS pass-through), and add all the ALBs as endpoints • Also unchanged. A standard accelerator is how you route traffic at the edge into the correct Region. • (E) Use ACM to create an SSL/TLS certificate for each Region. Configure all the ALBs to use the certificate in their respective Regions • This step is correct if the Region supports ACM for requesting or importing a cert. • If not, you do manual certificate handling (import or direct upload).

c1193d4 1 year, 2 months ago

Selected Answer: CDE

F: NO HTTPS listener available with GA A: NO global certificate is necessary is this case (see CloudFront) B: Could be a solution but GA improves latency more than Route53

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #229 Topic 1

A company has a VPC that includes application workloads that run on Amazon EC2 instances in a single AWS Region. The company wants to use AWS Local Zones to deploy an extension of the application workloads that run in the Region. The extended workloads in the Local Zone need to communicate bidirectionally with the workloads in the VPC in the Region.

Which solution will meet these requirements MOST cost-effectively?

A. Create a new VPC in the Local Zone. Attach all the VPCs to a transit gateway. Configure routing for the transit gateway and the VPCs. Deploy instances in the new VPC.

B. Deploy a third-party appliance in a new VPC in the Region. Create a new VPC in the Local Zone. Create VPN connections to the appliance for the VPCs. Deploy instances in the new VPC in the Local Zone.

C. Create a new subnet in the Local Zone. Deploy a third-party appliance in the VPC with interfaces in each subnet. Configure the new subnet to route the Local Zone through the appliance. Deploy instances in the new subnet.

D. Create a new subnet in the Local Zone. Configure the new subnet to use a CIDR block that is within the VPC's CIDR block. Deploy instances in the new subnet in the Local Zone. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

tushar321 10 months, 2 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/local-zones/latest/ug/getting-started.html

AtomicNuke 1 year, 2 months ago

Selected Answer: D

D is correct - Enable the local zone via EC2 Console Management. When we create a new subnet in the VPC, the local zone will be shown

https://zhangxuetu.online

[202610]

Question #230 Topic 1

A company is using AWS Cloud WAN with one edge location in the us-east-1 Region and one edge location in the us-west-1 Region. A shared services segment exists at both edge locations. Each shared services segment has a VPC attachment to each inspection VPC in each Region. The inspection VPCs inspect traffic from a WAN by using AWS Network Firewall.

The company creates a new segment for a new business unit (BU) in the us-east-1 edge location. The new BU has three VPCs that are attached to the new BU segment. To comply with regulations, the BU VPCs must not communicate with each other. All internet-bound traffic must be inspected in the inspection VPC.

The company updates VPC route tables so any traffic that is bound for internet goes to the AWS Cloud WAN core network.

The company plans to add more VPCs for the new BU in the future. All future VPCs must comply with regulations.

Which solution will meet these requirements in the MOST operationally efficient way? (Choose two.)

A. Update the network policy to share the shared services segment with the BU segment. **Most Voted**

B. Create a network policy to share the inspection service segment with the BU segment. **Most Voted**

C. Set the isolate-attachments field to True for the BU segment. **Most Voted**

D. Set the isolate-attachments field to False for the BU segment.

E. Update the network policy to add static routes for the BU segment. Configure the shared services segment to route traffic related to VPC CIDR blocks to each respective VPC attachment.

Correct Answer: BC

Community vote distribution

BC (67%) AC (33%)

Comments

304faa7 **Highly Voted** 1 year, 4 months ago

A & C. There is no mention of inspection segment in the question. The only segment mentioned in the question is shared services segment which is why A is correct

AWSLoverLoverLoverLoverLover 11 months, 3 weeks ago

Selected Answer: BC

Answer B and C

ashk123456 11 months, 4 weeks ago

Selected Answer: BC

(A) incorrect because, The requirement does not mention that the BU VPCs need access to shared services. The key requirement is inspection and isolation, not shared services access.

woorkim 1 year, 3 months ago

Selected Answer: AC

Options A + C provide the most scalable solution No need to update routes for each new VPC Automatic handling of traffic flows Maintains compliance automatically for future VPCs

https://zhangxuetu.online

[202610]

Question #231 Topic 1

A company hosts a highly available, scalable, and resilient application on Amazon EC2 instances that are part of an Auto Scaling group. A network engineer is planning to integrate IPv6 support with the application deployment in phases. The first phase is to enable IPv6 service consumption on the public Network Load Balancers (NLBs) that are deployed across the infrastructure. The target groups for the NLBS are configured as the Auto Scaling groups of the EC2 instances that host the application. The NLBs are configured for dual-stack operation.

During the testing of the first phase, the IPv6 application queries are not reaching the backend servers.

What is the cause of this issue?

A. The subnets where the EC2 instances are deployed do not have IPv6 addresses configured. **Most Voted**

B. The route tables for the NLB subnets do not have IPV6 routing configured.

C. The route tables for the EC2 subnets do not have IPV6 routing configured.

D. The security groups that are associated with the NLBs do not allow IPv6 traffic.

Correct Answer: A

Community vote distribution



Comments

729847f 2 months, 1 week ago

Selected Answer: A

NLBs do not use security groups at all. Security groups apply to EC2 instances (and ALBs), not NLBs, so this can’t be the cause.

Ohnet 3 months, 3 weeks ago

Selected Answer: D

D.....

ashk123456 11 months, 4 weeks ago

Selected Answer: A

For IPv6 traffic to flow from the NLB to the backend EC2 instances, the EC2 instances need to have IPv6 addresses assigned. Since the first phase was only to enable IPv6 on the NLBs, the backend EC2 instances likely weren't prepared to handle IPv6 traffic. Without IPv6 addresses configured in the EC2 subnets, the NLB cannot forward IPv6 traffic to the targets.

c1193d4 1 year ago

Selected Answer: B

See https://docs.aws.amazon.com/whitepapers/latest/ipv6-on-aws/scaling-the-dual-stack-network-design-in-aws.html NLB does the IPv6 to IPv4 conversion during this first phase so that no IPv6 configuration is necessary in the EC2 subnet

c1193d4 1 year ago

D would probably be a good choice also ... I suppose that NLB dual-stack activation is no possible if the subnets have no IPv6 address

eff3 7 months, 3 weeks ago

I agree, if Dualstack mode converts to v4, then EC2 will see the IPv4 of NLB as the SRC which excludes A, B and C. I'm going for D

djangoGroup 1 year, 2 months ago

Selected Answer: A

The EC2 subnets (where the Auto Scaling group instances run) do not have IPv6 addresses configured. Therefore, even though the Network Load Balancer (NLB) is operating in dual-stack mode and can accept IPv6 connections, it cannot forward IPv6 traffic to instances that do not themselves have IPv6 addresses in the same subnet.

victian 1 year ago

but i think the ip address should be allocated when the elb launch the instance ?

https://zhangxuetu.online

[202610]

Question #232 Topic 1

A company wants to implement a distributed architecture on AWS that uses a Gateway Load Balancer (GWLB) and GWLB endpoints.

The company has chosen a hub-and-spoke model. The model includes a GWLB and virtual appliances that are deployed into a centralized appliance VPC and GWLB endpoints. The model also includes internet gateways that are configured in spoke VPCs.

Which sequence of traffic flow to the internet from the spoke VPC is correct?

A. 1. An application in a spoke VPC sends traffic to the GWLB endpoint based on the VPC route table configuration.
2. Traffic is delivered securely and privately to the GWLB.
3. The GWLB sends the traffic to a virtual appliance for inspection.
4. Return traffic flows back to the GWLB endpoint and out to the internet through the internet gateway. **Most Voted**

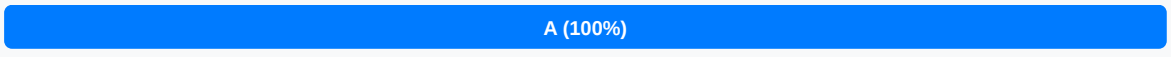
B. 1. An application in a spoke VPC sends traffic to the GWLB endpoint based on the VPC route table configuration.
2. Traffic is delivered securely and privately to the GWLB endpoint.
3. The GWLB sets the X-Forwarded-For request header and sends the traffic to a virtual appliance for inspection.
4. Return traffic flows back to the GWLB and out to the internet through an internet gateway.

C. 1. An application in a spoke VPC sends traffic to the GWLB endpoint.
2. Traffic is delivered securely and privately to the GWLB.
3. The GWLB sets the X-Forwarded-For request header and sends the traffic to a virtual appliance for inspection.
4. Return traffic flows back to the GWLB endpoint and out to the internet through the internet gateway.

D. 1. An application in a spoke VPC sends traffic to the GWLB.
2. Traffic is delivered securely and privately to the GWLB endpoint.
3. The GWLB sends the traffic to a virtual appliance for inspection.
4. Return traffic flows back to the GWLB and out to the internet through an internet gateway.

Correct Answer: A

Community vote distribution



Comments

djangoGroup Highly Voted 1 year, 2 months ago

Selected Answer: A

Option A: 1. An application in a spoke VPC sends traffic to the GWLB endpoint based on the VPC route table configuration. 2. Traffic is delivered securely and privately to the GWLB. 3. The GWLB sends the traffic to a virtual appliance for inspection. 4. Return traffic flows back to the GWLB endpoint and out to the internet through the internet gateway. • Step 1: Correct. The spoke VPC route table points default (or other relevant prefixes) to the GWLB endpoint. • Step 2: Correct. The GWLB endpoint is an interface endpoint that privately and securely forwards packets to the GWLB in the appliance VPC. • Step 3: Correct. The GWLB passes traffic to the attached virtual appliance (e.g., a firewall) for inspection. • Step 4: Correct. After inspection, the traffic returns to the spoke VPC through the GWLB endpoint and finally exits via the spoke VPC's internet gateway.

ashk123456 11 months, 4 weeks ago

Selected Answer: A

Traffic from the spoke VPC is first directed to the GWLB endpoint (which resides in the spoke VPC) via route table configurations

https://zhangxuetu.online

[202610]

Question #233 Topic 1

A network engineer needs to provide a list of IP addresses that are sending traffic to an Amazon EC2 instance. VPC flow logs are enabled. The EC2 instance has a single network interface and two assigned IP addresses. However, the flow logs are logging traffic only for the primary IP address. The network engineer needs to determine whether any traffic is being sent to the second IP address of the EC2 instance.

What should the network engineer do to locate the traffic flow for the second IP address?

A. Create a new flow log that includes the pkt-dstaddr field to capture the original destination IP address of the traffic. **Most Voted**

B. Create a new flow log that includes the dstaddr field to capture the original destination IP address of the traffic.

C. Create a new flow log that includes the pkt-srcaddr field to capture the original destination IP address of the traffic.

D. Create a new flow log that includes the srcaddr field to capture the original destination IP address of the traffic.

Correct Answer: A

Community vote distribution

A (100%)

Comments

woorkim **Highly Voted** 1 year, 3 months ago

Selected Answer: A

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-limitations.html If your network interface has multiple IPv4 addresses and traffic is sent to a secondary private IPv4 address, the flow log displays the primary private IPv4 address in the dstaddr field. To capture the original destination IP address, create a flow log with the pkt-dstaddr field.

exampb007 1 year, 2 months ago

Selected Answer: A

A is the correct one

makanju 1 year, 3 months ago

Selected Answer: A

Amazon VPC Flow Logs are used to capture network traffic information for interfaces in a VPC. By default, flow logs capture data for the primary private IP address of the network interface. However, to capture traffic for secondary IP addresses assigned to an interface, additional fields such as pkt-dstaddr are necessary.

https://zhangxuetu.online

[202610]

Question #234 Topic 1

A company has configured an AWS Cloud WAN core network with edge locations in the us-east-1 Region and the us-west-1 Region. Each edge location has two segments: development and staging. The segments use the default core network policy.

The company has attached VPCs to the core network. A development VPC is attached to the development segment in us-east-1 and is configured to use the 10.0.0.0/16 CIDR block. A staging VPC is attached to the staging segment in us-west-1 and is configured to use the 10.5.0.0/16 CIDR block. The company has updated the route tables for both VPCs with a route that directs any traffic for 0.0.0.0/0 to the core network.

The company's network team needs to establish communication between the two VPCs by using the AWS Cloud WAN core network. The network team is not receiving a response during tests of communication between the VPCs. The network team has verified that security groups and network ACLs are not blocking the traffic.

What should the network team do to establish this communication?

A. Update both VPC route tables to have a new static route. Configure a route on the development VPC to direct the traffic for 10.0.0.0/16 to the development VPC attachment. Configure a route on the staging VPC to direct the traffic for 10.5.0.0/16 to the staging VPC attachment.

B. Update the segment filter to allow traffic on the development and staging segments.

C. Set the isolate-attachments parameter to False for the development and staging segments.

D. Update the core network policy to add a static route for each segment. Configure a route to direct the traffic for 10.0.0.0/16 to the development VPC attachment. Configure a route to direct the traffic for 10.5.0.0/16 to the staging VPC attachment. Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Comments

ArunRav Highly Voted 1 year, 4 months ago

Selected Answer: D

You need to update the core network policy to enable communication between the VPCs.

woorkim Highly Voted 1 year, 3 months ago

Selected Answer: D

A. Adding static routes to VPC route tables wouldn't help because the segments themselves are isolated B. Segment filters control what attachments can join a segment, not inter-segment communication C. The isolate-attachments parameter controls isolation within a segment, not between segments D. Updating the core network policy with static routes would define how traffic should flow between segments

https://zhangxuetu.online

[202610]

Question #235 Topic 1

A company has VPCs in the us-east-1 Region that are connected to each other through a transit gateway. A network engineer needs to establish an AWS Direct Connect connection between the company's on-premises data center and the transit gateway for the migration of a workload.

The Direct Connect connection is UP according to the ConnectionState metric in Amazon CloudWatch. However, the VIF is DOWN. The network engineer has verified the transit VIF and BGP configurations on the on-premises router and has found no issues. However, the network engineer is unable to ping the Amazon peer IP address.

Which combination of steps should the network engineer take to troubleshoot this issue? (Choose three.)

A. Verify that the correct IP address and subnet mask are in use for the subinterface on the router. Most Voted

B. Ensure that VLAN trunking is disabled on the router.

C. Verify that the router has a MAC address entry from the AWS endpoint in the Address Resolution Protocol (ARP) table. Most Voted

D. Verify that the optical signal that is received over the cross connect is optimal.

E. Ensure that the correct VLAN tag is applied on the subinterface configuration on the router. Most Voted

F. Ensure that TCP port 179 is not being blocked at the on-premises router.

Correct Answer: ACE

Community vote distribution



Comments

intp75 1 year ago

Selected Answer: ACE

https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html

dspd 1 year, 1 month ago

Selected Answer: ACE

A. Correct IP address and subnet mask: This is crucial for establishing the connection. If these are incorrect, the VIF won't be able to establish a connection with the AWS side. C. MAC address entry in ARP table: If the router doesn't have the MAC address of the AWS endpoint in its ARP table, it won't be able to communicate at the link layer. This

could explain why the network engineer is unable to ping the Amazon peer IP address. E. Correct VLAN tag: The VLAN tag must match between the AWS configuration and the router's subinterface. If this is misconfigured, the traffic won't be properly tagged and routed.

secdaddy 1 year, 1 month ago

Selected Answer: ACE

Ping fails so it is lower level than port 179. Connect is up so have light. We have subinterface twice and if there is a subinterface trunking must already be disabled. Could be wrong IP/mask (A), arp failure - maybe cabling to wrong por (C), or wrong vlan tag (E).

jfedotov 1 year, 2 months ago

Selected Answer: AEF

Answers: AEF

meseerie 1 year, 1 month ago

F is at layer 3, the issue report as at layer2. F is wrong

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #236 Topic 1

A logistics company has multiple VPCs in an AWS Region. The company uses a transit gateway to connect the VPCs. The company has several on-premises offices that connect to the transit gateway by using AWS Site-to-Site VPN connections over the internet. The company has configured one transit gateway VPN attachment for each office.

Route propagation is enabled on all route tables. Each Site-to-Site VPN connection uses two tunnels in an active-passive configuration. The company configured each office with appropriate static routes on both the Site-to-Site VPN connection and the office's customer gateway.

The company wants to use both IPsec tunnels of every office to maximize the overall VPN connection bandwidth.

Which design changes are necessary to meet these requirements?

A. Create an AWS Transit Gateway Connect attachment for each office Use the existing VPN attachments as the transport for the new Connect attachments. Set up a Generic Routing Encapsulation (GRE) tunnel on each customer gateway that terminates on the Connect attachment for each office. Move the static routes from the transit gateway VPN attachment to the customer gateway for the transit gateway Connect attachment.

B. Enable equal-cost multi-path (ECMP) routing on the transit gateway. Ensure ECMP is supported by and enabled on the customer gateways. Enable ECMP on the Site-to-Site VPN connection. Ensure static routes on the customer gateways have equal metrics and administrative distance.

C. Enable equal-cost multi-path (ECMP) routing on the transit gateway. (Ensure ECMP is supported by and enabled on the customer gateways. Change the routing configuration between the transit gateway and the customer gateways from static routing to BGP. Remove related static routes from the customer gateways. **Most Voted**

D. Enable equal-cost multi-path (ECMP) routing on the transit gateway. Ensure ECMP is supported by and enabled on the customer gateways. Change the routing configuration between the transit gateway and the customer gateways from static routing to BGP. Ensure the customer gateway applies the correct community strings to give the transit gateway the ability to perform ECMP forwarding.

Correct Answer: C

Community vote distribution

C (100%)

Comments

maddyr 3 months ago

Selected Answer: C

ECMP + BGP to optimise bw

jfedotov 1 year, 2 months ago

Selected Answer: C

C is the answer

https://zhangxuetu.online

[202610]

Question #237 Topic 1

A finance company runs multiple applications on Amazon EC2 instances in two VPCs that are within a single AWS Region. The company uses one VPC for stock trading applications. The company uses the second VPC for financial applications. Both VPCs are connected to a transit gateway that is configured as a multicast router.

In the stock trading VPC, an EC2 instance that has an IP address of 10.128.10.2 sends trading data over a multicast network to the 239.10.10.10 IP address on UDP Port 5102. The company recently launched two new EC2 instances in the financial application VPC. The new EC2 instances need to receive the multicast stock trading data from the EC2 instance that is in the stock trading VPC.

Which combination of steps should the company take to meet this requirement? (Choose three.)

A. Add the elastic network interfaces of the two new EC2 instances as members of the multicast group by using the group IP address of 239.10.10.10. Most Voted

B. Add an inbound rule to the security groups that are attached to the multicast receiver instances. Configure the rule as follows:
Protocol: IGMP Version 2. Port: 5102, and Source: 239 10.10.10/32

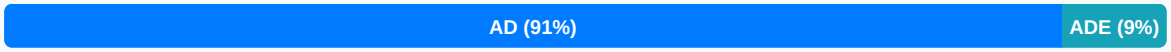
C. Create associations to two EC2 instance IDs on the financial application VPC transit gateway attachment under the transit gateway multicast domain.

D. Create an association to EC2 instance subnets on the financial application VPC transit gateway attachment under the transit gateway multicast domain.
D. Add an inbound rule to the security groups that are attached to the multicast receiver instances. Configure the rule as follows:
Protocol: IGMP Version 2. Port: All, and Source: 0 0.0.0/32 Most Voted

E. Add an inbound rule to the security groups that are attached to the multicast receiver instances. Configure the rule as follows.
Protocol: UDP, Port: 5102, and Source: 10.128.10.2/32

Correct Answer: AD

Community vote distribution



Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: AD

ADF is correct

Sudeepshiv 12 months ago

Selected Answer: ADE

1. A: Register the receiver ENIs to the multicast group. 2. D: Associate the receiver subnets with the multicast domain. 3. E: Allow the sender's UDP traffic in the receiver’s security group.

dspd 1 year, 1 month ago

Selected Answer: AD

ADF : The best combination of steps to meet this requirement is: A. Add the elastic network interfaces of the two new EC2 instances as members of the multicast group by using the group IP address of 239.10.10.10. D. Create an association to EC2 instance subnets on the financial application VPC transit gateway attachment under the transit gateway multicast domain. F. Add an inbound rule to the security groups that are attached to the multicast receiver instances. Configure the rule as follows: Protocol: UDP, Port: 5102, and Source: 10.128.10.2/32

meseerie 1 year, 2 months ago

Selected Answer: AD

Correct answers: ADF A. Add the elastic network interfaces of the two new EC2 instances as members of the multicast group by using the group IP address of 239.10.10.10. - same IP as the existing Group D.Create an association to EC2 instance subnets on the financial application VPC transit gateway attachment under the transit gateway multicast domain. -when you select Multicast Domain creation, choose the attachment you have made, and the subnet where the EC2 instances were launched to associate. F.Add an inbound rule to the security groups that are attached to the multicast receiver instances. Configure the rule as follows. Protocol: UDP, Port: 5102, and Source: 10.128.10.2/32

c1193d4 1 year, 2 months ago

Selected Answer: AD

Issue on my side regarding answers numbering: ADF A. Add the elastic network interfaces of the two new EC2 instances as members of the multicast group by using the group IP address of 239.10.10.10. D. Create an association to EC2 instance subnets on the financial application VPC transit gateway attachment under the transit gateway multicast domain. F. Add an inbound rule to the security groups that are attached to the multicast receiver instances. Configure the rule as follows. Protocol: UDP, Port: 5102, and Source: 10.128.10.2/32

https://zhangxuetu.online

[202610]

Question #238 Topic 1

A company runs workloads in multiple VPCs in the us-east-1 Region. The VPCs are connected to a transit gateway. An AWS Direct Connect connection provides private connectivity between a data center that is in the US and the transit gateway. A Direct Connect gateway is associated with the transit gateway.

The company has recently opened a new office location in London. The company plans to launch cloud services in multiple VPCs in the eu-west-2 Region. Users in the new London office must have private access to the workloads that run in us-east-1. Users in the US data center must have access to any workloads that are created in eu-west-2. A network engineer must implement a flexible solution that provides users the required access. The solution must be able to accommodate future growth.

Which solution will meet these requirements with the LEAST operational effort?

A. Create an AWS Site-to-Site VPN connection from the London office to the Direct Connect gateway in us-east-1.

B. Establish a new Direct Connect connection for the London office. Attach the new Direct Connect connection to the existing Direct Connect gateway. Create a transit gateway in eu-west-2. Associate the new transit gateway with the existing Direct Connect gateway. Create a peering connection between the transit gateways in us-east-1 and eu-west-2. **Most Voted**

C. Create an AWS Site-to-Site VPN connection from the London office to each of the VPCs that are in us-east-1.

D. Establish a new AWS Direct Connect connection for the London office Create a new Direct Connect gateway and a transit gateway in eu-west-2. Attach the new Direct Connect connection to the new Direct Connect gateway. Create a peering connection between the transit gateways in us-east-1 and eu-west-2.

Correct Answer: B

Community vote distribution

B (100%)

Comments

woorkim 1 year, 1 month ago

Selected Answer: B

Since the Direct Connect gateway (DXGW) is global, it can be used to connect the new DX connection in London to the existing transit gateway in us-east-1. This simplifies routing and minimizes operational complexity.

secdaddy 1 year, 1 month ago

Selected Answer: B

No need for another DXGW as it's global. VPNs as described don't meet the connectivity requirements.

https://zhangxuetu.online

[202610]

Question #239 Topic 1

A company has 10 Amazon EC2 instances that run web server software in a production VPC. The company also has 10 web servers that run in an on-premises data center. The company has a 10 Gbps AWS Direct Connect connection between the on-premises data center and the production VPC. The data center uses the 10.100.0.0/20 CIDR block.

The company needs to implement a load balancing solution that receives HTTPS traffic from thousands of external users. The solution must distribute the traffic across the web servers on AWS and the web servers in the data center. Regardless of the location of the web servers, HTTPS requests must go to the same web server for the duration of the session.

Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) in the production VPC. Create one target group for the EC2 Instances and a second target group for the on-premises servers. Specify IP as the target type. Register the EC2 instances and the on-premises servers with the target groups. Enable connection draining on the NLB.

B. Deploy an Application Load Balancer (ALB) in the production VPC. Create one target group for the EC2 Instances and a second target group for the on-premises servers. Specify IP as the target type. Register the EC2 instances and the on-premises servers with the target groups. Enable application-based sticky sessions on the ALB. **Most Voted**

C. Deploy a Network Load Balancer (NLB) in the production VPCreate one target group for the EC2 Instances and a second target group for the on-premises servers. Specify instance as the target type. Register the EC2 instances and the on-premises servers with the target groups. Enable sticky sessions on the NLB.

D. Deploy an Application Load Balancer (ALB) in the production VPC. Create one target group for the EC2 Instances and a second target group for the on-premises servers. Specify instance as the target type. Register the EC2 instances and the on-premises servers with the target groups. Enable application-based sticky sessions on the ALB.

Correct Answer: B

Community vote distribution

B (100%)

Comments

zanhsieh 1 year ago

Selected Answer: B

NLB can't handle HTTPS directly and no sticky session nor session persistence, so AC are out. EC2 target group can't register on-prem servers, so CD dropped. Therefore only B left.

secdaddy 1 year, 1 month ago

Selected Answer: B

ALB for sticky https & IP not instance type as have onprem

https://zhangxuetu.online

[202610]

Question #240 Topic 1

A global company is establishing network connections between the company's primary and secondary data centers and a VPC. A network engineer needs to maximize resiliency and fault tolerance for the connections. The network bandwidth must be greater than 10 Gbps.

Which solution will meet these requirements MOST cost-effectively?

A. Set up a 100 Gbps connection at the primary data center that terminates at an AWS Direct Connect location. Set up a second 100 Gbps connection at the secondary data center that terminates at a second Direct Connect location. Ensure the connections are managed by separate providers.

B. Set up a 10 Gbps connection at the primary data center that terminates at an AWS Direct Connect location. Set up a second 10 Gbps connection at the secondary data center that terminates at a second Direct Connect location. Ensure the connections are managed by separate providers.

C. Set up two 10 Gbps connections at the primary data center that terminate at one AWS Direct Connect location. Ensure the connections are managed by separate providers. Set up two 10 Gbps connections at the secondary data center that terminate at a second Direct Connect location. Ensure the connections are managed by separate providers. **Most Voted**

D. Set up a 10 Gbps connection at the primary data center that terminates at an AWS Direct Connect location. Set up an AWS Site-to-Site VPN connection at the secondary data center that terminates at a virtual private gateway in the same Region as the company's VPC.

Correct Answer: C

Community vote distribution



Comments

AtomicNuke 1 year, 2 months ago

Selected Answer: C

C is correct - In order to maximize resiliency and fault tolerance for the connections, two DX connections are established for each AWS DX location https://aws.amazon.com/directconnect/resiliency-recommendation/

djangoGroup 1 year, 2 months ago

Selected Answer: C

B) Using 10 Gbps connections: ✗ Barely meets bandwidth requirement (no redundancy) ✓ Good resiliency (separate locations and providers) ✓ More cost-effective than A C) Using dual 10 Gbps connections: ✓ Meets bandwidth

requirements (20 Gbps per site with redundancy) ✓ Excellent resiliency (separate providers and locations) ✓ More cost-effective than A, slightly more expensive than B but with better redundancy

woorkim 1 year, 2 months ago

Selected Answer: C

The answer is C. Provides >10 Gbps bandwidth through multiple 10 Gbps connections Maximizes resiliency with redundant connections at separate locations Uses separate providers for additional fault tolerance More cost-effective than 100 Gbps connections while meeting requirements

meseerie 1 year, 2 months ago

Selected Answer: B

B) the bandwidth must be greater overall, combined 10+10 is the most cost-efficient setup.

https://zhangxuetu.online

[202610]

Question #241 Topic 1

A company's data center is connected to a single AWS Region by an AWS Direct Connect dedicated connection. The company has a single VPC in the Region. The company stores logs for all its applications locally in the data center.

The company must keep all application logs for 7 years. The company decides to copy all application logs to an Amazon S3 bucket.

Which solution will meet these requirements?

A. Create a public VIF on the Direct Connect connection. Create an Amazon S3 gateway endpoint in the VPC.

B. Create a private VIF on the Direct Connect connection. Create an Amazon S3 gateway endpoint in the VPC.

C. Create a private VIF on the Direct Connect connection. Create an Amazon S3 interface endpoint in the VPC. **Most Voted**

D. Create a public VIF on the Direct Connect connection. Create an Amazon S3 interface endpoint in the VPC.

Correct Answer: C

Community vote distribution



Comments

matanasov 10 months, 1 week ago

Selected Answer: C

Private VIF - Used to access VPC resources (including VPC endpoints) over private IPs from on-premises. Interface endpoints for Amazon S3 - Allow access from on premises

1a17d1e 7 months, 3 weeks ago

The Q doesn't say that the Direct Connect was set up using private addressing, can we default to thinking that private addressing is in place?

ashk123456 11 months, 4 weeks ago

Selected Answer: B

Private Virtual Interface (VIF): A private VIF is used to access AWS services like Amazon S3 through your VPC. It enables private connectivity between your on-premises data center and your VPC over Direct Connect. S3 Gateway

Endpoint: This is the appropriate endpoint type for Amazon S3. Gateway endpoints are the recommended way to connect to S3 from a VPC as they use route tables to direct traffic over the AWS private network to S3 without traversing the internet.

siheom 1 year ago

Selected Answer: B

vote B

zanhsieh 1 year ago

Selected Answer: B

I pick B. All options can access S3. GW endpoint is free but interface endpoint isn't. Security wise we will pick private VIF not public VIF, and pick GW endpoint not interface endpoint.

secdaddy 1 year, 1 month ago

Selected Answer: A

How about (A) that has an S3 gateway (preferred as free) endpoint providing S3 for inside the VPC and the public VIF providing S3 service for the DC across DX.

woorkim 1 year, 2 months ago

Selected Answer: C

https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html you allow in-VPC applications to continue accessing Amazon S3 through the gateway endpoint, which is not billed. Then, only your on-premises applications would use interface endpoints to access Amazon S3.

secdaddy 1 year, 1 month ago

Private VIF doesn't provide S3 to onprem ?

kowal_001 1 year, 2 months ago

Selected Answer: C

Interface Endpoint for Amazon S3: Unlike gateway endpoints, interface endpoints (using AWS PrivateLink) are accessible from both inside the VPC and from external sources such as an AWS Direct Connect connection or VPN. This makes the interface endpoint the right choice when the application logs stored locally in the data center need to be uploaded to S3 over the Direct Connect connection.

c1193d4 1 year, 2 months ago

Selected Answer: C

C: because gateway endpoints are not accessible from sources outside the VPC (like DX)

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #242 Topic 1

A company is planning to host a secure web application across multiple Amazon EC2 instances. The application will have an associated DNS domain in an Amazon Route 53 hosted zone.

The company wants to protect the domain from DNS poisoning attacks. The company also wants to allow web browsers to authenticate into the application by using a trusted third party.

Which combination of actions will meet these requirements?

A. Configure the Route 53 hosted zone to use DNS Security Extensions (DNSSEC). Install self-signed X.509 certificates on the EC2 instances.

B. Configure a Name Authority Pointer (NAPTR) record in the Route 53 hosted zone. Install X 509 certificates that are signed by a public certificate authority on the EC2 instances.

C. Configure the Route 53 hosted zone to use DNS Security Extensions (DNSSEC). Install X.509 certificates that are signed by a public certificate authority on the EC2 instances. Most Voted

D. Configure a Name Authority Pointer (NAPTR) record in the Route 53 hosted zone. Install self-signed X.509 certificates on the EC2 instances.

Correct Answer: C

Community vote distribution

C (100%)

Comments

woorkim 1 year, 2 months ago

Selected Answer: C

• A protocol for securing DNS traffic, verifies DNS data integrity and origin • Works only with Public Hosted Zones

c1193d4 1 year, 2 months ago

Selected Answer: C

C: DNSSEC will protect against DNS poisoning NAPTR is not relevant for this usage

https://zhangxuetu.online

[202610]

Question #243 Topic 1

A company is planning to use an AWS Transit Gateway hub and spoke architecture to migrate to AWS. The current on-premises multi-protocol label switching (MPLS) network has strict controls that enforce network segmentation by using MPLS VPNs. The company has provisioned two 10 Gbps AWS Direct Connect connections to provide resilient, high-speed, low-latency connectivity to AWS.

A security engineer needs to apply the concept of network segmentation to the AWS environment to ensure that virtual routing and forwarding (VRF) is logically separated for each of the company's software development environments. The number of MPLS VPNs will increase in the future. On-premises MPLS VPNs will have overlapping address space. The company's AWS network design must support overlapping address space for the VPNs.

Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy a software-defined WAN (SD-WAN) head-end virtual appliance and an SD-WAN controller into a Transit Gateway Connect VPC. Configure the company's edge routers to be managed by the new SD-WAN controller and to use SD-WAN to segment the traffic into the defined segments for each of the company's development environments.

B. Configure IPsec VPNs on the company edge routers for each MPLS VPN for each of the company's development environments. Attach each IPsec VPN tunnel to a discrete MPLS VPN. Configure AWS Site-to-Site VPN connections that terminate at a transit gateway for each MPLS VPN. Configure a transit gateway route table that matches the MPLS VPN for each Transit Gateway VPN attachment.

C. Create a transit VPC that terminates at the AWS Site-to-Site VRF-aware IPsec VPN. Configure IPsec VPN connections to each VPC for each of the company's development environment VRFs.

D. Configure a Transit Gateway Connect attachment for each MPLS VPN between the company's edge routers and Transit Gateway. Configure a transit gateway route table that matches the MPLS VPN for each of the company's development environments. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

woorkim 1 year, 2 months ago

Selected Answer: D

Transit Gateway Connect: Directly integrates with Direct Connect Native support for VRF separation Minimal operational overhead Easy to scale with new MPLS VPNs Supports overlapping IP addresses Uses existing Direct Connect infrastructure Simple route table management

c1193d4 1 year, 2 months ago

Selected Answer: D

D: see Pattern 3 at https://aws.amazon.com/blogs/networking-and-content-delivery/design-patterns-for-interconnecting-a-telco-data-center-to-an-amazon-vpc/

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #244 Topic 1

A company is planning to migrate to AWS and use multiple VPCs in multiple AWS Regions. A network engineer must connect the eu-west-1 and eu-central-1 Regions to the company headquarters and branch office, respectively.

The network engineer created a production VPC, named Prod A, with a CIDR block of 10.0.0.0/16. Prod A runs in an account in eu-west-1. The network engineer then created another production VPC, named Prod B, with a CIDR block of 10.1.0.0/16. Prod B runs in a different account in eu-central-1.

The network engineer performed the following steps to try to achieve the required connectivity:
1. Created one transit gateway in each Region
2. Shared and accepted the transit gateways with the production accounts in both Regions
3. Configured the peering attachment between both transit gateways
4. Attached both VPCs to the respective Region transit gateway
5. Created both transit gateway route tables and associated the attachments with the route tables
6. Configured a static route in both transit gateway route tables to send traffic to the remote VPC in the other Region
7. Activated route propagation on the VPC route tables in each Region

After the configuration, the network engineer tried to connect from Prod A to Prod B. However, the connection was unsuccessful.

What should the network engineer do to achieve the required connectivity?

A. Modify the IP address of the peering attachment to a wider range.

B. Delete the static routes that were in the transit gateway route table to send traffic to the remote VPC and enable route propagation instead.

C. Create a new route destined to 10.0.0.0/8 in both production VPC route tables with the Region transit gateway as the target. **Most Voted**

D. Modify the transit gateway route tables from the production accounts to propagate routes dynamically between the production VPCs.

Correct Answer: C

Community vote distribution

C (100%)

Comments

secdaddy 1 year, 1 month ago

Selected Answer: C

A Eliminate TGW peering attachments don’t have IP addresses. B Eliminate TGW peering requires static routes; propagation is not supported. C ⚠ Technically Valid (but bad design) Broad CIDR route (10.0.0.0/8) works but is ugly. D Eliminate Cannot propagate routes dynamically between VPCs.

woorkim 1 year, 2 months ago

Selected Answer: C

C is correct because: Adding a route for 10.0.0.0/8 in both VPC route tables pointing to the transit gateway will: Enable traffic to flow between the VPCs Cover both VPC CIDR ranges (10.0.0.0/16 and 10.1.0.0/16) Complete the routing path in both directions

c1193d4 1 year, 2 months ago

Selected Answer: C

C: because TGW routes are NOT propagated to VPC route tables (manual update as to take place)

https://zhangxuetu.online

[202610]

Question #245 Topic 1

A company hosts an application on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are part of an Amazon EC2 Auto Scaling group.

To comply with new security standards, the company must capture all application access data, including server response codes, request paths, latency, and client IP addresses. The company also needs to query the captured data for performance analysis.

Which solution will meet these requirements?

A. Enable VPC flow logs on the ALB subnets. Store the logs to an Amazon S3 bucket. Query the logs in the S3 bucket by using Amazon Athena.

B. Configure Amazon VPC Traffic Mirroring on all EC2 elastic network interfaces. Deploy a third-party monitoring appliance from AWS Marketplace in a private subnet. Use Amazon Data Firehose to send all mirrored traffic to the monitoring appliance. Query the logs directly from the monitoring appliance.

C. Configure Amazon CloudWatch detailed monitoring on the EC2 instances Include all available logs. Use Amazon Data Firehose to send all the collected logs to an Amazon S3 bucket. Query the data directly from the S3 bucket.

D. Enable access logs on the ALB. Store the logs in an Amazon S3 bucket. Query the logs in the S3 bucket by using Amazon Athena. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: D

These logs can be stored directly in S3 and then queried using Amazon Athena, which provides SQL-like querying capabilities for log analysis and performance troubleshooting.

dspd 1 year, 1 month ago

Selected Answer: D

D - Enable access logs on the ALB. Store the logs in an Amazon S3 bucket. Query the logs in the S3 bucket by using Amazon Athena. This is the best solution because: Comprehensive Data Capture: ALB access logs capture detailed

information about requests sent to the load balancer, including: Client IP addresses Request paths Server response codes Latency Additional details like request and response headers, SSL cipher, SSL protocol

https://zhangxuetu.online

[202610]

Question #246 Topic 1

A company has five VPCs in the us-east-1 Region. The company hosts an internal web application in us-east-1. One of the company's VPCs. named VPC-A, needs to connect to an external partner's AWS environment. The partner's environment is in the same AWS Region where the partner hosts a new version of the company's web application. The partner hosts its version of the application in a VPC named VPC-B.

The company has Amazon EC2 instances in VPC-A that need to connect to the web application in VPC-B A network engineer notices that the partner's VPC-B and the company's VPC-A use the same IP space. The network engineer needs a solution to allow the EC2 instances to connect to the web application. The solution must not negatively affect the exiting environment of the company or the partner.

Which combination of steps should the network engineer take meet these requirements? (Choose two.)

A. Establish a VPC peering connection between VPC-A to VPC-B.

B. Ensure the partner creates a VPC endpoint service that uses a Network Load Balancer in VPC-B. Most Voted

C. Deploy a VPC endpoint in VPC-A that uses a VPC endpoint service that is shared by the partner. Most Voted

D. Deploy a new routable VPC CIDR block as a secondary CIDR block to both VPC-A and VPC-B. Deploy a public NAT gateway in VPC-A.

E. Establish an AWS Site-to-Site VPN connection between VPC-A and VPC-B.

Correct Answer: BC

Community vote distribution

BC (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: BC

AWS PrivateLink (which uses VPC endpoint services) is specifically designed to connect services across VPCs without requiring overlapping CIDR ranges to be routable between them. This solves the IP overlap problem without requiring IP address changes. The partner would create a VPC endpoint service backed by a Network Load Balancer that fronts their web application in VPC-B. The company would then create a VPC endpoint in VPC-A that connects to the partner's endpoint service, allowing EC2 instances to access the application using a private DNS name that resolves to a private IP within VPC-A's address space.

woorkim 1 year, 2 months ago

Selected Answer: BC

Handles overlapping IP ranges Doesn't require network changes Provides secure connectivity Uses AWS PrivateLink, which is designed for this scenario Maintains isolation between environments

c1193d4 1 year, 2 months ago

Selected Answer: BC

B and C: see https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/

https://zhangxuetu.online

[202610]

Question #247 Topic 1

A company has a hybrid environment that connects an on-premises data center to the AWS Cloud. The hybrid environment uses a 10 Gbps AWS Direct Connect dedicated connection. The Direct Connect connection has multiple private VIFs that terminate in multiple VPCs.

To comply with regulations, the company must encrypt all WAN traffic, regardless of the underlying transport. The company needs to implement an encryption solution that will not affect the company's bandwidth capacity.

Which solution will meet these requirements?

A. Create a public VIF. Configure a new AWS Site-to-Site VPN connection to use the new public VIF.

B. Configure MAC security (MACsec) support on the port of the existing Direct Connect connection. Change the encryption mode to must_encrypt.

C. Configure a new Direct Connect connection that supports MAC security (MACSec) Associate the existing VIFs to the new Direct Connect connection. **Most Voted**

D. Create a public VIF. Configure a new private IP VPN that uses the Direct Connect connection.

Correct Answer: C

Community vote distribution

C (100%)

Comments

c1193d4 **Highly Voted** 1 year, 2 months ago

Selected Answer: C

C: because it's NOT possible to activate MacSec on an existing connection - see https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

dspd 1 year, 1 month ago

Selected Answer: C

To enable the Direct Connect MACsec feature, you must migrate to a MACsec capable Direct Connect circuit.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #248 Topic 1

A company needs to capture and log traffic for Nitro-based Amazon EC2 instances to comply with regulations. The company's network team has prepared a solution that enables VPC traffic mirroring and sends traffic to a second set of EC2 instances in an Auto Scaling group.

The network team has added a Network Load Balancer (NLB) in front of the EC2 instances the traffic will be sent to. However, the solution does not send any mirrored traffic to the EC2 instances that are behind the NLB.

How should the network team configure traffic mirroring to use the NLB endpoint?

A. Select the NLB as a source for traffic mirroring. Use a UDP listener.

B. Select the NLB as a target for traffic mirroring. Use a TCP listener and a UDP listener.

C. Select the NLB as a target for traffic mirroring. Use a TCP listener.

D. Select the NLB as a target for traffic mirroring. Use a UDP listener. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

c1193d4 **Highly Voted** 1 year, 2 months ago

Selected Answer: D

D: VxLAN UDP Port 4789 is used for traffic mirroring

ashk123456 11 months, 4 weeks ago

Selected Answer: D

Amazon VPC Traffic Mirroring allows you to capture and inspect network traffic from Nitro-based EC2 instances by sending mirrored traffic to a monitoring system. The mirrored traffic is always sent using UDP encapsulation. Since the Network Load Balancer (NLB) is being used as a target, the correct listener configuration should be UDP.

woorkim 1 year, 2 months ago

Selected Answer: D

he answer is D because: Traffic mirroring requires UDP for VXLAN encapsulation NLB must be configured as target, not source Single UDP listener is sufficient Matches AWS traffic mirroring architecture requirements

https://zhangxuetu.online

[202610]

Question #249 Topic 1

A US-based company is expanding its business to Europe. A network engineer needs to extend the company's network infrastructure by setting up a new hub and spoke architecture in the eu-west-1 Region. The network engineer uses a transit gateway peering connection to connect the new resources in eu-west-1 to an existing environment in the us-east-1 Region.

The hub and spoke architecture in each AWS Region includes an inspection VPC that uses AWS Network Firewall to centralize traffic inspection for each Region. To reduce costs, the network engineer decides to inspect inter-Region traffic by using the inspection VPC in the Region that originates the traffic. The network engineer configures the transit gateway route tables accordingly for each Region.

When the network engineer tests the new architecture, communication within each Region works as expected. However, the network engineer finds that inter-Region communication is not working. The network engineer must resolve the inter-Region communication issue.

Which solution will meet this requirement?

A. Configure Open Shortest Path First (OSPF) routing on the transit gateway peering connection to propagate the VPC CIDR blocks from each Region to the remote peer.

B. Use AWS Resource Access Manager (AWS RAM) to share access between the transit gateways. Enable the Allow sharing with anyone setting.

C. Prevent asymmetric routing in the inspection VPCs by ensuring that both requests and responses are inspected by the same inspection VPC

D. Enable Appliance mode on both the transit gateway attachments for the inspection VPC. **Most Voted**

Correct Answer: D

Community vote distribution

D (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: D

In a hub-and-spoke architecture using AWS Transit Gateway, when traffic is routed to an inspection VPC (which contains AWS Network Firewall), the traffic path must remain symmetric—meaning that both request and response traffic must pass through the same inspection VPC. By default, AWS Transit Gateway performs packet routing optimally, which can sometimes lead to asymmetric routing issues when using an inspection VPC.

woorkim 1 year, 2 months ago

D is correct! A (Configure OSPF routing): AWS Transit Gateway does not support dynamic routing protocols like OSPF. Instead, it uses static routes or BGP for route propagation in Direct Connect scenarios. B (Use AWS RAM to share access): AWS RAM is used to share transit gateways across accounts, not for enabling inter-Region communication or fixing routing issues. C (Prevent asymmetric routing in the inspection VPCs): While preventing asymmetric routing is important, the root cause here is the lack of appliance mode. Simply ensuring symmetry without enabling appliance mode will not resolve the issue.

kowal_001 1 year, 2 months ago

Selected Answer: D

Enable Appliance Mode on the transit gateway attachments for both inspection VPCs in the us-east-1 and eu-west-1 Regions. This ensures that bidirectional traffic passes through the same inspection VPC, resolving the asymmetric routing issue and enabling inter-Region communication.

https://zhangxuetu.online

[202610]

Question #250 Topic 1

A company runs applications in two VPCs that are in separate AWS Regions. One VPC is in the us-east-1 Region. The second VPC is in the us-west-1 Region. The company needs to establish connectivity between the two VPCs. The company also needs to connect the VPCs to applications that run in an on-premises data center.

The current traffic requirement between the VPCs is 50 TB per month. The company expects traffic volume between the VPCs to increase. The traffic requirement from the VPCs to the on-premises data center is 10 TB per month. The company expects the traffic between the VPCs and the data center to remain constant.

Which solution will meet these requirements MOST cost-effectively?

A. Create a transit gateway in each Region. Create VPN connections from the transit gateways to the on-premises firewall. Create a peering connection between the transit gateways.

B. Create a virtual private gateway in each Region. Create VPN connections from the on-premises firewall to the virtual private gateways. Configure the on-premises firewall to route the traffic between the two VPCs.

C. Create a virtual private gateway in each Region. Create VPN connections from the on-premises firewall to the virtual private gateways. Create a VPC peering connection between the two VPCs. **Most Voted**

D. Create a virtual private gateway in each Region. Create VPN connections from the on-premises firewall to the virtual private gateways. Create a VPN connection between the virtual private gateways.

Correct Answer: C

Community vote distribution

C (75%) A (25%)

Comments

Nouwara 10 months, 4 weeks ago

Selected Answer: C

it is between A and C but as it is asked for the most cost effective so it should be C as vpc peering is less expensive than TGW

ashk123456 11 months, 4 weeks ago

Selected Answer: A

C is incorrect: VPC peering is not cost-effective for 50 TB/month because AWS charges per GB for inter-Region traffic. No centralized management: Unlike Transit Gateway, VPC Peering requires manual route table updates.

kaerarune 12 months ago

Selected Answer: A

The amount of traffic between VPCs is expected to increase, while the amount of traffic between VPCs and on-premises is expected to remain constant, so wouldn't a TGW configuration be more cost-effective in the future?

victian 1 year ago

Selected Answer: C

actually, Inter-region TGW peering data transfer fees are higher than inter-region VPC peering data transfer fees

46f094c 1 year, 1 month ago

Selected Answer: C

Inter-region VPC peering is supported. No need to add the cost of a TGW

secdaddy 1 year, 1 month ago

Selected Answer: A

D. AWS does not support VPN connections directly between VGWs and B. seems unlikely due to the increasing VPC-VPC traffic requirement. C. Inter-region VPC peering is not free. A. Inter-region TGW peering data transfer fees are lower than inter-region VPC peering data transfer fees.

victian 1 year ago

actually, Inter-region TGW peering data transfer fees are higher than inter-region VPC peering data transfer fees

woorkim 1 year, 2 months ago

Selected Answer: C

Transit Gateways + VPN + TGW peering Higher base cost due to TGW hourly charges Additional data processing charges More expensive than necessary

kowal_001 1 year, 2 months ago

Selected Answer: C

C. There is no info about extra VPCs in the future. A will work and would be better if we consider more VPCs. But it this case, we have only 2 of them , so peering is xenough.

c1193d4 1 year, 2 months ago

Selected Answer: C

C: because it's the less expensive solution and because a 1.25 Gbps VPN is enough to transfer 10TB over 1 month (around 2h30 / 1 TB)

https://zhangxuetu.online

[202610]

Question #251 Topic 1

A company runs workloads in multiple VPCs. The company needs to securely access a workload in one of the VPCs, named VPC-A, from an on-premises data center. A network engineer sets up an AWS Site-to-Site VPN connection to a transit gateway. The network engineer configures dynamic routing for the connection, and communication works properly.

Recently, the owner of VPC-A added another CIDR range to the VPC. The VPC-A owner created workloads that use the additional CIDR range.

The company's on-premises network is unable to reach the new workloads. The network engineer needs to resolve the network connectivity issue and ensure that connectivity will not be affected if additional VPC CIDR ranges are added to the VPC in the future.

Which solution will meet these requirements with the MOST operational efficiency?

A. Configure route propagation for VPC-A to the VPN attachment route table. **Most Voted**

B. Manually update the VPN attachment route table to include the new CIDR range.

C. Configure an Amazon EventBridge rule to invoke an AWS Lambda function when the rule to matches an update to the VPC-A CIDR range. Configure the Lambda function to update the VPN attachment route table.

D. Configure an Amazon CloudWatch alarm to invoke an AWS Lambda function when there is an update to the VPC-A CIDR range. Configure the Lambda function to update the VPN attachment route table. Restart the VPN tunnels.

Correct Answer: A

Community vote distribution



Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: A

When VPC-A adds a new CIDR, the route should automatically propagate to the VPN attachment route table, ensuring that the on-premises network learns the new CIDR without manual updates.

woorkim 1 year, 2 months ago

Selected Answer: A

By enabling route propagation for VPC-A to the VPN attachment route table, any new CIDR ranges added to VPC-A will automatically be propagated to the VPN attachment route table. This ensures that on-premises networks can

reach the new workloads in VPC-A without manual updates.

c1193d4 1 year, 2 months ago

Selected Answer: A

The 2nd CIDR will be automatically added to the VPC-A and will be propagated to the VPN attachment RT.

https://zhangxuetu.online

[202610]

Question #252 Topic 1

A company is migrating its internet VPN connections to dedicated AWS Direct Connect connections. The company needs to set up the Direct Connect connections so that all network communications are encrypted in transit.

Which combination of steps will meet this requirement? (Choose three.)

A. Create new Direct Connect connections while requesting MACsec ports. Most Voted

B. Create a MACsec Connectivity Association Key Name (CKN) and Connectivity Association Key (CAK) pair. Associate the pair with each new connection. Most Voted

C. Update the on-premises routers to use MACsec and the shared Connectivity Association Key Name (CKN) and Connectivity Association Key (CAK) pair. Most Voted

D. Create a shared key for an IPsec connection.

E. Configure a new Direct Connect gateway. Associate the shared key with the new Direct Connect gateway.

F. Set up IPsec on the on-premises router. Associate the shared key with the IPsec configuration.

Correct Answer: ABC

Community vote distribution

ABC (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: ABC

ABC is correct

woorkim 1 year, 1 month ago

Selected Answer: ABC

to encrypt network communications over AWS Direct Connect connections are A, B, and C. These steps ensure that MACsec is enabled and properly configured for the Direct Connect connections, providing encryption in transit.

kowal_001 1 year, 2 months ago

Selected Answer: ABC

ABC MACsec combination.

https://zhangxuetu.online

[202610]

Question #253 Topic 1

A company has an application VPC and a networking VPC that are connected through VPC peering. The networking VPC contains a Network Load Balancer (NLB). The application VPC contains Amazon EC2 instances that run an application. The EC2 instances are part of a target group that is associated with the NLB in the networking VPC.

The company configures a third VPC and peers it to the networking VPC. The new VPC contains a new version of the existing application. The new version of the application runs on new EC2 instances in an application subnet. The new version of the application runs in a different Availability Zone than that original version of the application.

The company needs to establish connectivity between the NLB and the new version of the application.

Which combination of steps will meet this requirement? (Choose three.)

A. Register the new application EC2 instances with the NLB by using the instance IDs.

B. Register the new application EC2 instances with the NLB by using instance IP addresses. Most Voted

C. Configure the NLB in the Availability Zone where the new application EC2 instances run. Most Voted

D. Configure the NLB to use zonal shift.

E. Configure the network ACL for the application subnet in the new VPC to allow outbound connections.

F. Configure the network ACL for the application subnet in the new VPC to allow inbound connections and outbound connections. Most Voted

Correct Answer: BCF

Community vote distribution

BCF (100%)

Comments

woorkim Highly Voted 1 year, 2 months ago

Selected Answer: BCF

A. Register the new application EC2 instances with the NLB by using the instance IDs: Instance ID registration is not supported across VPC peering connections because the NLB cannot resolve private DNS names or directly communicate with instances in a different VPC. D. Configure the NLB to use zonal shift: Zonal shift is a feature of AWS Elastic Disaster Recovery (DRS) for mitigating zonal outages, not for enabling communication with targets in different Availability Zones. E. Configure the network ACL for the application subnet in the new VPC to allow outbound

connections: Outbound-only configuration is insufficient. Both inbound and outbound rules are required for full communication between the NLB and the EC2 instances.

c1193d4 1 year, 2 months ago

Selected Answer: BCF

BCF: When registering targets by instance ID, instances must be in the same Amazon VPC as the Network Load Balancer. See https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#target-type

https://zhangxuetu.online

Question #254 Topic 1

A company uses AWS Site-to-Site VPN connections to encrypt traffic between the company's on-premises location and a single VPC. The Site-to-Site VPN connections use two 1 Gbps AWS Direct Connect connections with public VIFs. The company plans to add 15 additional VPCs in the same AWS Region.

The company must maintain the same level of encryption that the Site-to-Site VPN connections currently provide for each connection between the on-premises location and the new VPCs. The new connections must not use public IP addresses. The bandwidth of the Site-to-Site VPN connections will remain less than the current provisioned speed.

Which combination of steps will meet these requirements with LEAST operational overhead? (Choose three.)

A. Create a transit gateway and a Direct Connect gateway. Associate the transit gateway with the Direct Connect gateway. Attach all the new VPCs to the transit gateway. Most Voted

B. For each new VPC, create a new Direct Connect private VIF to a Direct Connect gateway. Associate all VPCs with the Direct Connect gateway.

C. Assign a private IP CIDR block to the transit gateway. Most Voted

D. Assign a public IP CIDR block to the transit gateway.

E. Create a transit VIF to the Direct Connect gateway. Create a Site-to-Site VPN private IP VPN connection. Most Voted

F. Create a public VICreate a Site-to-Site VPN public IP VPN connection.

Correct Answer: ACE

Community vote distribution

ACE (100%)

Comments

c1193d4 1 year, 2 months ago

Selected Answer: ACE

ACE: see https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway-vpn.html

[202610]

Question #255 Topic 1

A company hosts application servers on premises and on Amazon EC2 instances in a VPC. The application servers access data that is hosted in an Amazon S3 bucket through the public internet. The EC2 instances in the VPC use an AWS Site-to-Site VPN for connectivity with the on-premises application servers.

New company regulations state that all traffic between the application servers and the S3 bucket must remain private and must not use public IP addresses.

Which solution will meet these requirements MOST cost-effectively?

A. Configure an S3 gateway endpoint Modify the route table with the appropriate route for the endpoint. Access the S3 bucket through the gateway endpoint from the EC2 instances.

B. Configure an S3 interface endpoint. Update the on-premises servers and EC2 instances to use the interface endpoint DNS name to access the S3 bucket.

C. Configure an S3 interface endpoint. Update the on-premises servers to use the interface endpoint DNS name to access the S3 bucket. Configure an S3 gateway endpoint. Modify the route table so that the EC2 instances use the gateway endpoint. Most Voted

D. Configure an S3 gateway endpoint. Modify the route table with the appropriate route for the endpoint. Use an S3 bucket policy to restrict access to the gateway endpoint. Configure a proxy server fleet behind a Network Load Balancer in the VPC so that the on-premises servers can access the S3 bucket.

Correct Answer: C

Community vote distribution



Comments

Nouwara 10 months, 4 weeks ago

Selected Answer: C

S3 Gateway Endpoint (for EC2 instances): This will allow EC2 instances within the VPC to access the S3 bucket via private IP addresses, bypassing the public internet. The traffic will stay within the AWS network, maintaining privacy. S3 Interface Endpoint (for on-premises servers): Since the on-premises servers cannot access S3 via the VPC gateway endpoint, the interface endpoint provides a way for the on-premises servers to connect to S3 through the private network using a private IP. By using the DNS name associated with the interface endpoint, the on-premises servers will route traffic through the VPC interface endpoint, keeping the traffic private.

TechAwesome 1 year ago

Selected Answer: B

Both B and C make sense. Depends how do you understand "must not use public IP addresses". Even with Gateway endpoint, you are still accessing S3's public IP address..The question is not clear.

jfedotov 1 year, 2 months ago

Selected Answer: C

C is correct S3 Interface Endpoint with the option "Enable private DNS only for inbound endpoint" S3 Gateway for EC2

jfedotov 1 year, 2 months ago

Selected Answer: B

B is correct "A company hosts application servers on-premises and on Amazon EC2 instances" Both onprem and ec2 send traffic to S3, so it should be S3 Interface.

woorkim 1 year, 2 months ago

Selected Answer: C

most cost-effective solution because: Gateway endpoints are free and perfect for EC2 instances in the VPC Interface endpoints, while having a cost, are necessary for on-premises servers Each type of server uses the most appropriate endpoint type No unnecessary components like proxy fleets or load balancers

meseerie 1 year, 2 months ago

Selected Answer: B

B. traffic is sourced from On-Prem to S3 in private. So Interface endpoint is needed.

c1193d4 1 year, 2 months ago

Selected Answer: C

C: see this architecture in https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

nico73 1 year, 2 months ago

Selected Answer: C

because gateway endpoints are not accessible from sources outside the VPC

jfedotov 1 year, 2 months ago

B is correct, no need to create routes for the interface

jfedotov 1 year, 2 months ago

C is correct, mislook the answer, the route is needed for gateway.

https://zhangxuetu.online

[202610]

Question #256 Topic 1

A company uses AWS Network Firewall to protect outgoing traffic for multiple VPCs that are in the same AWS account. Each VPC contains Amazon EC2 instances that host the company's applications. Each EC2 instance is tagged with the name of the application it hosts. The EC2 instances are in Auto Scaling groups.

A Network Firewall stateful rule group must remain up-to-date, even when an Auto Scaling group launches and terminates EC2 instances.

Which solution will meet this requirement with the LEAST implementation and administrative effort?

A. Create a network ACL for each application. Reference the network ACL in the stateful rule group.

B. Create a prefix list for each application. Reference the prefix list in the stateful rule group.

C. Create an AWS Lambda function that queries the EC2 instance tags for each application name and then updates the stateful rule group with the IP address of each instance.

D. Create a resource group for each application name. Reference the Amazon Resource Name (ARN) for the resource groups in the stateful rule group. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

a0e6696 7 months ago

Selected Answer: D

https://docs.aws.amazon.com/network-firewall/latest/developerguide/resource-group-creating.html use a resource group, include the resource group's Amazon Resource Name (ARN) in a stateful rule's IP set reference. For information about using resource groups in IP set references

Nouwara 10 months, 4 weeks ago

Selected Answer: B

D cannot be the anser as AWS Network Firewall does not support resource groups or ARNs as rule group match criteria.

ashk123456 11 months, 4 weeks ago

Selected Answer: B

Prefix lists in AWS are dynamic collections of IP address ranges (CIDR blocks) that can be referenced within Network Firewall rules. When you maintain and update a prefix list to include the subnets where your Auto Scaling groups

operate, the Network Firewall rules automatically apply to any new instances launched in those subnets. D. Resource groups cannot be referenced in firewall rule groups. ----AWS Network Firewall does not support referencing resource groups in rule groups.

woorkim 1 year, 2 months ago

Selected Answer: D

because: Resource groups automatically update membership based on tags No ongoing maintenance required once set up Handles Auto Scaling events automatically Minimal implementation effort (just create groups and reference ARNs) No custom code or manual updates needed Works with Network Firewall's native capabilities

c1193d4 1 year, 2 months ago

Selected Answer: D

D: because a tag-based resource group can be created : see https://docs.aws.amazon.com/network-firewall/latest/developerguide/resource-groups.html

kvf 5 months, 1 week ago

But you cannot reference the ARN of the resource group in the rule https://docs.aws.amazon.com/network-firewall/latest/developerguide/resource-group-settings.html

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #257 Topic 1

A company has multiple AWS Site-to-Site VPN connections between an on-premises environment and multiple VPCs. The Site-to-Site VPN connections use virtual private gateways and are configured with IPv4 addresses. The company hosts several internal applications in the VPCs.

Application users have reported that the applications are performing slowly. A network engineer notices excessive latency in the network path that the VPN connections use. The network engineer needs to resolve the excessive latency.

Which solution will meet this requirement?

A. Use AWS Global Accelerator to deploy an accelerator on the existing Site-to-Site VPN connections.

B. Deploy a transit gateway and a new accelerated Site-to-Site VPN connection. **Most Voted**

C. Replace the existing Site-to-Site VPN connections with new Site-to-Site VPN connections that use IPv6.

D. Replace the existing Site-to-Site VPN connections with AWS PrivateLink connections.

Correct Answer: B

Community vote distribution

B (100%)

Comments

c1193d4 **Highly Voted** 1 year, 2 months ago

Selected Answer: B

B: Acceleration is only supported for Site-to-Site VPN connections that are attached to a transit gateway. See https://docs.aws.amazon.com/vpn/latest/s2svpn/accelerated-vpn.html

https://zhangxuetu.online

[202610]

Question #258 Topic 1

A company has a transit gateway in a single AWS account. The company sends flow logs for the transit gateway to an Amazon CloudWatch Logs log group.

The company created an AWS Lambda function to analyze the logs. The Lambda function sends a notification to an Amazon Simple Notification Service (Amazon SNS) topic when a VPC generates traffic that is dropped by the transit gateway. Each notification contains the account ID. VPC ID, and total amount of dropped packets.

The company wants to subscribe a new Lambda function to the SNS topic. The new Lambda function must automatically prevent the traffic that is identified in each notification from leaving a VPC by applying a network ACL to the transit gateway attachment subnets in the VPC that generates the traffic.

Which solution will meet these requirements?

A. Configure the existing Lambda function to add the destination IP addresses of the dropped traffic to each SNS notification. Configure the new Lambda function to create an outbound rule by using the destination IP addresses in the network ACL. **Most Voted**

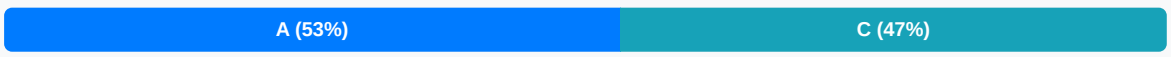
B. Configure the existing Lambda function to add the source IP addresses of the dropped traffic to each SNS notification. Configure the new Lambda function to create an inbound rule by using the source IP addresses in the network ACL.

C. Configure the existing Lambda function to add the source IP addresses of the dropped traffic to each SNS notification. Configure the new Lambda function to create an outbound rule by using the source IP addresses in the network ACL.

D. Configure the existing Lambda function to add the destination IP addresses of the dropped traffic to each SNS notification. Configure the new Lambda function to create an inbound rule by using the destination IP addresses in the network ACL.

Correct Answer: A

Community vote distribution



Comments

woorkim **Highly Voted** 1 year, 2 months ago

Selected Answer: A

It uses destination IP addresses, which identify where the problematic traffic is trying to go It creates outbound rules, which prevent traffic from leaving the VPC This combination will effectively block traffic to the identified problematic

destinations The solution maintains proper traffic flow direction matching between the identified problems and the blocking mechanism It can be automated through Lambda based on the SNS notifications

Ohnet 3 months, 3 weeks ago

Selected Answer: A

There is no option to specify source IPs in outbound NACL rule.

0xab3d 8 months, 3 weeks ago

Selected Answer: C

Logs are captured at the TGW.

Nouwara 10 months, 4 weeks ago

Selected Answer: C

cant b A as destination is outside the VPC, and NACLs operate at subnet level. we can't block external destinations with NACLs directly. correct answer is C. Source IP + outbound rule

ashk123456 11 months, 4 weeks ago

Selected Answer: C

The goal is to prevent traffic identified in SNS notifications from leaving the VPC. The correct approach is to: 1. Identify the source IP addresses of the unwanted traffic. 2. Use a network ACL (NACL) to block outbound traffic from these source IPs in the transit gateway attachment subnets.

youonebe 1 year ago

Selected Answer: C

Answer is C. Traffic is going out from EC2, need to identify the source and attach outbound constrain to the subnet ACL.

c1193d4 1 year, 2 months ago

Selected Answer: A

A: add a NACL outbound rule to stop the traffic from the VPC where it's generated - use the destination address (only IP settable for outbound rules)

https://zhangxuetu.online

[202610]

Question #259 Topic 1

A company has multiple VPCs with subnets that use IPv4. Traffic from the VPCs to the internet uses a NAT gateway. The company wants to transition to IPv6.

A network engineer creates multiple IPv6-only subnets in an existing testing VPC. The network engineer deploys a new Amazon EC2 instance that has an IPv6 address into one of the subnets. During testing, the network engineer discovers that the new EC2 instance is not able to communicate with an IPv4-only service through the internet. The network engineer needs to enable the IPv6 EC2 instance to communicate with the IPv4-only service.

Which solution will meet this requirement?

A. Enable DNS64 for the IPv6-only subnets. Update the route tables for the IPv6-only subnets to send traffic through the NAT gateway. **Most Voted**

B. Enable NAT64 for the testing VPC. Reconfigure the existing NAT gateway to support IPv6.

C. Enable DNS64 for the new EC2 instance. Create a new egress-only internet gateway that supports IPv6.

D. Enable NAT64 for each route table. Create a new NAT gateway that supports both IPv4 and IPv6.

Correct Answer: A

Community vote distribution

A (100%)

Comments

c1193d4 **Highly Voted** 1 year, 2 months ago

Selected Answer: A

A: DNS64 must be activated at the subnet level - NAT64 is available by default on a NAT GW

ashk123456 11 months, 4 weeks ago

Selected Answer: A

NAT64 is available by default on an AWS NAT Gateway when used with an IPv6-enabled subnet. However, DNS64 must be explicitly enabled at the subnet level for it to work properly.

https://zhangxuetu.online

[202610]

Question #260 Topic 1

A company deployed an application in two AWS Regions in one AWS account. The company has one VPC in each Region. The VPCs use non-overlapping private CIDR ranges.

The company needs to connect both VPCs to a single on-premises data center to test the application. The application requires up to 800 Mbps of throughput. A network engineer needs to establish connectivity between the VPCs and the on-premises data center.

Which solution will meet this requirement with the LEAST operational overhead?

A. Order a 2 Gbps Direct Connect connection for the data center. Configure a virtual private gateway in each VPC. Create a private VIF for each virtual private gateway, and associate the virtual private gateways with the Direct Connect connection. Configure static routes in the VPC route tables and in the data center router.

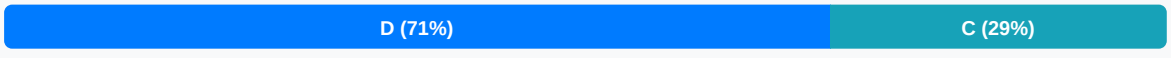
B. Order a 2 Gbps Direct Connect connection for the data center. Configure a virtual private gateway in each VPC. Create a private VIF for each virtual private gateway, and associate the virtual private gateways with the Direct Connect connection. Configure Open Shortest Path First (OSPF) routing between the private VIF and the data center.

C. Configure a customer gateway and a virtual private gateway in each VPConfigure an AWS Site-to-Site VPN connection between the data center and each VPConfigure static routes in each VPC route table to point to the subnets in the data center.

D. Configure a customer gateway and a virtual private gateway in each VPC. Configure an AWS Site-to-Site VPN connection between the data center and each VPC. Configure BGP routing between the VPCs and the data center. **Most Voted**

Correct Answer: D

Community vote distribution



Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: D

Option D provides the quickest implementation with the most automated routing management through BGP, making it the solution with the least operational overhead while meeting all requirements. A and B both require ordering and provisioning a physical Direct Connect connection,

Sudeepshiv 12 months ago

Selected Answer: D

• AWS Site-to-Site VPN is fast to set up, cost-effective, and ideal for temporary or test connectivity. • You can easily establish VPN tunnels to each VPC using virtual private gateways (VGWs) and customer gateways (CGWs). • Using BGP (Border Gateway Protocol) provides dynamic route exchange between your on-premises network and AWS — this reduces manual route configuration and simplifies scaling as new networks are added. • It provides adequate throughput (up to 1.25 Gbps) per VPN connection with ECMP and accelerated VPN — enough for the required 800 Mbps throughput.

jfedotov 1 year, 1 month ago

Selected Answer: C

isn't it easier to configure static routes for 2 VPC and on-prem DC, than configuring BGP? C or D ?

woorkim 1 year, 2 months ago

Selected Answer: D

answer is D. Using Site-to-Site VPN connections with BGP routing provides: Automatic route propagation Dynamic routing updates Sufficient throughput Lower cost than Direct Connect Minimal operational overhead for maintenance Simpler setup compared to Direct Connect options

c1193d4 1 year, 2 months ago

Selected Answer: D

D: a VPN is enough for 800 Mbps and for testing

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #261 Topic 1

A company runs a workload in a single VPC on AWS. The company's architecture contains several interface VPC endpoints for AWS services, including Amazon CloudWatch Logs and AWS Key Management Service (AWS KMS). The endpoints are configured to use a shared security group. The security group is not used for any other workloads or resources.

After a security review of the environment, the company determined that the shared security group is more permissive than necessary. The company wants to make the rules associated with the security group more restrictive. The changes to the security group rules must not prevent the resources in the VPC from using AWS services through interface VPC endpoints. The changes must prevent unnecessary access.

The security group currently uses the following rules:

• Inbound - Rule 1

Protocol: TCP -

Port: 443 -

Source: 0.0.0.0/0 -

• Inbound - Rule 2

Protocol: TCP -

Port: 443 -

Source: VPC CIDR -

• Outbound - Rule 1

Protocol: All -

Port: All -

Destination: 0.0.0.0/0 -

Which rule or rules should the company remove to meet with these requirements?

A. Outbound - Rule 2

B. Inbound - Rule 1 and Outbound - Rule 1 **Most Voted**

C. Inbound - Rule 2 and Outbound - Rule 1

D. Outbound - Rule 1

Correct Answer: B

Community vote distribution



Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: B

Corrected answer

kaerarune 12 months ago

Selected Answer: B

"Outbound - Rule 2" is missing. Write it.

secdaddy 1 year, 1 month ago

Selected Answer: B

Inbound rule 2 allows traffic from the VPC CIDR to the endpoints incoming so can delete inbound rule 1 which is wider than the VPC CIDR and as SGs are stateful and automatically allow return traffic can delete the outbound rule. No need to add anything.

woorkim 1 year, 1 month ago

Selected Answer: B

Keep Inbound Rule 2 (VPC CIDR) so that only resources in the VPC can connect to the endpoints. Replace the removed outbound rule with a more restrictive rule that allows outbound traffic only to the AWS service VPC endpoints.

kowal_001 1 year, 2 months ago

Selected Answer: A

question is not complete. Correct answer should be inbound rule 1. inbound rule 2 is not complete but i assume there are some network cidrs provided so only this inbound should stay. There is also one outbound rule so it doesn't make sense to remove outbound rule 2

https://zhangxuetu.online

[202610]

Question #262 Topic 1

A company uses transit gateways to route traffic between the company's VPCs. Each transit gateway has a single route table. Each route table contains attachments and routes for the VPCs that are in the same AWS Region as the transit gateway. The route tables in each VPC also contain routes to all the other VPC CIDR ranges that are available through the transit gateways. Some VPCs route to local NAT gateways.

The company plans to add many new VPCs soon. A network engineer needs a solution to add new VPC CIDR ranges to the route tables in each VPC.

Which solution will meet these requirements in the MOST operationally efficient way?

A. Create a new customer-managed prefix list. Add all VPC CIDR ranges to the new prefix list. Update the route tables in each VPC to use the new prefix list ID as the destination and the appropriate transit gateway ID as the target. **Most Voted**

B. Turn on default route table propagation for the transit gateway route tables. Turn on route propagation for each route table in each VPC.

C. Update the route tables in each VPC to use 0.0.0.010 as the destination and the appropriate transit gateway ID as the target.

D. Turn on default route table association for the transit gateway route tables. Turn on route propagation for each route table in each VPC.

Correct Answer: A

Community vote distribution

A (100%)

Comments

woorkim 1 year, 1 month ago

answer is A Route propagation — A VPC, VPN connection, or Direct Connect gateway can dynamically propagate routes to a transit gateway route table. With a Connect attachment, the routes are propagated to a transit gateway route table by default. With a VPC, you must create static routes to send traffic to the transit gateway. With a VPN connection, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP). With a Direct Connect gateway, allowed prefixes are originated to your on-premises router using BGP. With a peering attachment, you must create a static route in the transit gateway route table to point to the peering attachment.

jfedotov 1 year, 2 months ago

Selected Answer: A

A https://docs.aws.amazon.com/vpc/latest/tgw/create-prefix-list-reference.html

kowal_001 1 year, 2 months ago

Selected Answer: A

A. b -> won't work here c - > can break internet facing VPCs d -> also won't work

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #263 Topic 1

A company has several AWS Site-to-Site VPN connections between an on-premises customer gateway and a transit gateway. The company's application uses IPv4 to communicate through the VPN connections.

The company has updated the VPC to be dual stack and wants to transition to using IPv6-only for new workloads. When the company tries to communicate through the existing VPN connections, IPv6 traffic fails.

Which solution will provide IPv6 support with the LEAST operational overhead?

A. Create a new Site-to-Site VPN connection that supports IPv6. **Most Voted**

B. Create a new Site-to-Site VPN connection to a self-managed Amazon EC2 instance that runs open source software.

C. Update the existing Site-to-Site VPN connections to support IPv6.

D. Update the on-premises customer gateway's public IP address from IPv4 to IPv6.

Correct Answer: A

Community vote distribution

A (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: A

AWS Site-to-Site VPN does not support IPv6 over existing VPN connections that were established using IPv4. IPv6 traffic will not work through an IPv4-based VPN connection. The best solution with the least operational overhead is to create a new Site-to-Site VPN connection that supports IPv6. AWS now supports IPv6 for Site-to-Site VPN, allowing the company to set up a dual-stack VPN connection.

dspd 1 year, 1 month ago

Selected Answer: A

AWS Site-to-Site VPN connections cannot be updated from IPv4 to IPv6. They need to be recreated.

https://zhangxuetu.online

掌学兔
ZHANGXUETU

[202610]

Question #264 Topic 1

A company has two teams: Team A and Team B. Team A has VPCs that run in Account A. The team uses a transit gateway (TGW-A) to route traffic between workloads that run in the different VPCs. Similarly, Team B has VPCs that run in Account B. Team B uses a different transit gateway (TGW-B) to route traffic between workloads that run in the different VPCs.

The company's network team manages the routing for Team A and Team B. The network team wants to retire TGW-B and use a single transit gateway to manage routing for the VPCs of both teams.

Which solution will meet this requirement with the LEAST operational overhead?

A. Create a resource share for TGW-A Share TGW-A with Account B. Create VPC attachments for the VPCs in Account B. Configure routing for the VPCs in TGW-A route tables. Update the route tables of the VPCs in Account B to forward traffic to TGW-Delete TGW-B attachments and TGW-B. **Most Voted**

B. Create a resource share for TGW-A. Share TGW-A with Account B. Replicate the TGW-B configuration to TGW-A to automatically start routing changes for the VPCs in Account B. Delete TGW-B when routing changes are complete.

C. Create a new transit gateway (TGW-C) in Account A. Create a resource share for TGW-Share TGW-C with Account B. Create VPC attachments for the VPCs in Account A and Account B. Configure routing for all the VPCs in TGW-C route tables. Update the route tables for the VPCs in Account A and Account B to forward traffic to TGW-Delete TGW-A attachments and TGW-B attachments. Delete TGW-A and TGW-B.

D. Create a new transit gateway (TGW-C) in a new account (Account C). Create a resource share for TGW-C. Share TGW-C with Account A and Account B. Create VPC attachments for the VPCs in Account A and Account B. Configure routing for all the VPCs in TGW-C route tables. Update the route tables for the VPCs in Account A and Account B to forward traffic to TGW-C. Delete TGW-A attachments and TGW-B attachments. Delete TGW-A and TGW-B.

Correct Answer: A

Community vote distribution

A (100%)

Comments

tushar321 10 months, 2 weeks ago

Selected Answer: A

A looks to be good

ashk123456 11 months, 4 weeks ago

Selected Answer: A

1. Resource Sharing with AWS RAM: • AWS Resource Access Manager (RAM) allows TGW-A to be shared with Account B, enabling Team B's VPCs to attach to it. 2. Reusing TGW-A: • Since TGW-A is already handling routing, adding Account B's VPCs is straightforward. 3. Simple Routing Updates: • Account B's VPCs just need to update their route tables to forward traffic through TGW-A. 4. Retirement of TGW-B: • Once Team B's VPCs are fully connected to TGW-A, TGW-B can be safely decommissioned.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #265 Topic 1

A company has an AWS environment that includes multiple VPCs that are connected by a transit gateway. The company wants to use a certificate-based AWS Site-to-Site VPN connection to establish connectivity between an on-premises environment and the AWS environment. The company does not have a static public IP address for the on-premises environment.

Which combination of steps should the company take to establish VPN connectivity between the transit gateway and the on-premises environment? (Choose two.)

A. Create a public certificate in AWS Certificate Manager (ACM).

B. Create a private certificate in AWS Certificate Manager (ACM). Most Voted

C. Configure the Site-to-Site VPN tunnels to use the pre-shared key (PSK).

D. Create a customer gateway. Specify the current dynamic IP address of the customer gateway device's external interface.

E. Create a customer gateway. Do not specify the IP address of the customer gateway device. Most Voted

Correct Answer: BE

Community vote distribution

BE (100%)

Comments

AWSLoverLoverLoverLoverLover 11 months, 2 weeks ago

Selected Answer: BE

Answer: B & E

ashk123456 11 months, 4 weeks ago

Selected Answer: BE

Why B (Create a private certificate in ACM) is correct: • AWS requires a private certificate from AWS Certificate Manager (ACM) for certificate-based authentication. • The certificate is used to authenticate the VPN connection instead of a pre-shared key (PSK). Why E (Create a customer gateway without specifying an IP address) is correct: • If the on-premises IP address is dynamic, you must create a customer gateway without an IP address. • This allows the VPN to function with BGP (Border Gateway Protocol), which dynamically updates the connection when the on-premises IP changes.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #266 Topic 1

A company operates in multiple AWS Regions. The company has deployed transit gateways in each Region. The company uses AWS Organizations to operate multiple AWS accounts in one organization.

The company needs to capture all VPC flow log data when a new VPC is created. The company needs to send flow logs to a specific Amazon S3 bucket.

Which solution will meet these requirements with the LEAST administrative effort?

A. Update IAM permissions for each user to include a condition that ensures users can create VPCs only when VPC Flow Logs is enabled and configured correctly.

B. Create a custom AWS Config rule with automatic remediation that verifies VPC Flow Logs is enabled and configured correctly. Apply the AWS Config rule to the organization. Most Voted

C. Enable VPC Flow Logs on each transit gateway. Configure VPC Flow Logs to send flow logs to the specified S3 bucket.

D. Deploy a serverless application that uses AWS CloudTrail to monitor for VPC creation events in each account. Configure the application to apply the correct VPC Flow Logs configuration.

Correct Answer: B

Community vote distribution

B (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: B

 AWS Config supports organization-wide governance – The rule can be applied to all accounts in AWS Organizations without requiring manual intervention in each account. Automatic enforcement – AWS Config can automatically remediate non-compliant VPCs by enabling flow logs and configuring them correctly. Least administrative effort – Once the rule is set up, it automatically applies to new VPCs without requiring ongoing manual work.

Sudeepshiv 12 months ago

Selected Answer: B

The requirement is to automatically capture VPC flow log data when a new VPC is created and send it to a specific S3 bucket with minimal administrative effort.

https://zhangxuetu.online

[202610]

Question #267 Topic 1

A company wants to analyze TCP internet traffic. The traffic originates from Amazon EC2 instances in the company's VPC. The EC2 instances initiate connections through a NAT gateway.

The company wants to capture data about the traffic including source and destination IP addresses ports, and the first 8 bytes of the TCP segments of the traffic. The company needs to collect, store, and analyze all the required data points.

Which solution will meet these requirements?

A. Configure the EC2 instances to be VPC traffic mirror sources. Deploy software on the traffic mirror target to forward the data to Amazon CloudWatch Logs. Analyze the data by using CloudWatch Logs Insights

B. Configure the NAT gateway to be a VPC traffic mirror source. Deploy software on the traffic mirror target to forward the data to an Amazon S3 bucket. Analyze the data by using Amazon Athena. **Most Voted**

C. Turn on VPC Flow Logs for the EC2 instances. Specify the default format and set Amazon CloudWatch Logs as the log destination. Analyze the flow log data by using CloudWatch Logs Insights.

D. Turn on VPC Flow Logs for the EC2 instances. Specify a custom format and set Amazon S3 as the log destination. Analyze the flow log data by using Amazon Athena.

Correct Answer: B

Community vote distribution



Comments

1a17d1e 7 months ago

Selected Answer: A

This is a messed up question. A: EC2 is the way to go to capture 8 bytes, but CloudWatch Logs Insights cannot analyze the first 8 bytes of TCP segments> B: NAT Gateway cannot be a mirroring source. C & D: VPC Flow Logs cannot capture the first 8 bytes of TCP segments Hopefully the actual Q is worded differently. As is, I'm choosing A because at least that answer made it past its initial configuration action as mirroring via EC2 is indeed possible to obtain the needed capture info.

AnsonCert 8 months ago

Selected Answer: A

By Amazon Q: B. NAT Gateway cannot be used as a source for Traffic Mirroring in AWS. Traffic Mirroring is designed to copy network traffic from specific sources to designated targets for analysis and monitoring purposes. The supported sources for Traffic Mirroring include: Elastic Network Interfaces (ENIs) attached to EC2 instances Network

Load Balancers Transit Gateway attachments A. For data analysis: If using CloudWatch Logs as the destination, use CloudWatch Logs Insights for analysis. If using S3 as the destination, use Amazon Athena for SQL-based analysis. C and D. Capture additional data: VPC Flow Logs don't capture packet payload data (like the first 8 bytes of TCP segments)

Gafa255 10 months ago

Selected Answer: B

definitively B, because need capture TCP data

AWSLoverLoverLoverLoverLover 11 months, 2 weeks ago

Selected Answer: B

The correct answer is: B. Requirements: Analyze TCP internet traffic initiated by EC2 instances via a NAT gateway. Capture: Source and destination IP addresses Ports First 8 bytes of the TCP segments. Collect, store, and analyze the data. A. CloudWatch Logs isn't a suitable destination for raw packet data—it’s structured log storage. Not designed for analyzing binary packet data; difficult to analyze packet-level data in CloudWatch Logs Insights.

ashk123456 11 months, 4 weeks ago

Selected Answer: B

 Using the NAT gateway as a VPC traffic mirror source ensures all outbound traffic is captured. Forwarding traffic to S3 and analyzing it with Athena provides an efficient storage and analysis pipeline. A. Incorrect – This would capture traffic at the instance level, but it does not efficiently aggregate traffic from multiple instances.

https://zhangxuetu.online

[202610]

Question #268 Topic 1

A media company is planning to host an event that the company will live stream to users. The company wants to use Amazon CloudFront.

A network engineer creates a primary origin and a secondary origin for CloudFront. The engineer needs to ensure that the primary origin can fail over to the secondary origin within 15 seconds if a disruption occurs.

Which solution will meet this requirement with the LEAST operational overhead?

A. Configure a Lambda@Edge function to check the health status of both origins every 10 seconds. Reroute incoming requests when the origin health status is unhealthy.

B. Create a Network Load Balancer (NLB) in front of both origins Configure the NLB as the origin in CloudFront.

C. Set the CloudFront origin connection timeout value to 5 seconds Set the origin connection attempts value to 2. **Most Voted**

D. Configure a Lambda@Edge function to monitor incoming requests for an origin response. Reroute incoming requests if no response is received from the primary origin within 10 seconds.

Correct Answer: C

Community vote distribution

C (100%)

Comments

AWSLoverLoverLoverLoverLover 11 months, 3 weeks ago

Selected Answer: C

Amazon CloudFront supports origin failover natively for primary and secondary origins. It can automatically fail over to the secondary origin if the primary is unhealthy. To control how quickly failover happens, you use: Origin connection timeout: Time CloudFront waits to establish a connection. Origin connection attempts: Number of retry attempts before declaring failure. If you set timeout to 5 seconds and attempts to 2, the total failover time is 10 seconds. CloudFront will try the primary origin twice, each with a 5-second timeout. If both fail, it moves to the secondary origin — all within 15 seconds, satisfying your requirement.

ashk123456 11 months, 4 weeks ago

Selected Answer: C

CloudFront determines origin health based on timeout and retry settings: Origin connection timeout: The time CloudFront waits before considering the origin unresponsive. Setting this to 5 seconds minimizes failover delay. Origin connection attempts: The number of retry attempts before marking the origin as unhealthy. Setting this to 2

attempts ensures failover within (5 sec * 2) = 10 seconds, well within the 15-second requirement. B.□ Incorrect – An NLB does not provide failover between different origins in the way CloudFront does. CloudFront's origin failover feature is simpler and requires less management.

Sudeepshiv 12 months ago

Selected Answer: C

CloudFront Failover Mechanism: • CloudFront allows you to configure multiple origins with automatic failover when the primary origin is unavailable. Connection timeout and retry attempts control how quickly CloudFront will attempt to use a secondary origin if the primary origin fails to respond.

https://zhangxuetu.online

[202610]

Question #269 Topic 1

AnyCompany deploys and manages networking resources in its AWS network account, named Account-A. AnyCompany acquires Example Corp, which has an application that runs behind an Application Load Balancer (ALB) in Example Corp's AWS account, named Account-B.

Example Corp needs to use AWS Global Accelerator to create an accelerator to publish the application to users. AnyCompany's networking team will manage the accelerator.

Which solution will meet these requirements with the LEAST management overhead?

A. Create an accelerator in Account-B. Use a cross-account role from Account-A to grant the networking team access to manage the accelerator.

B. Deploy a Network Load Balancer (NLB) in Account-A to route traffic to the ALB in Account-B. Create an accelerator, and set the NLB as the endpoint in Account-A.

C. Create a cross-account Global Accelerator attachment in Account-B for the Account-A principal. Create an accelerator in Account-A by using the shared attachment. **Most Voted**

D. Create an accelerator in Account-A. Use AWS Resource Access Management (AWS RAM) to share the accelerator with Account-B. Associate the ALB in Account-B with the accelerator in Account-A.

Correct Answer: C

Community vote distribution



Comments

matanasov 10 months, 1 week ago

Selected Answer: C

https://aws.amazon.com/blogs/networking-and-content-delivery/announcing-cross-account-support-for-aws-global-accelerator/

Nouwara 10 months, 3 weeks ago

Selected Answer: C

AWS Global Accelerator cannot be shared via AWS RAM.

Nouwara 10 months, 4 weeks ago

Selected Answer: C

D is uncorrect as Global Accelerator is not a resource we share via AWS RAM

ashk123456 11 months, 4 weeks ago

Selected Answer: D

 Minimal management overhead – AWS RAM enables cross-account resource sharing without requiring custom configurations or additional infrastructure. Global Accelerator supports ALBs in other accounts – By sharing access, Account-A can add Account-B's ALB as an endpoint. Centralized network management – The networking team in Account-A can manage everything related to traffic routing and failover policies.

Sudeepshiv 12 months ago

Selected Answer: D

AnyCompany's networking team (Account-A) is responsible for managing AWS Global Accelerator. Example Corp (Account-B) owns the ALB where the application is hosted. The solution should have minimal management overhead and enable cross-account Global Accelerator integration.

https://zhangxuetu.online

[202610]

Question #270 Topic 1

A company has two AWS Direct Connect connections between Direct Connect locations and the company's on-premises environment in the US. The company uses the connections to communicate with AWS workloads that run in the us-east-1 Region. The company has a transit gateway that connects several VPCs. The Direct Connect connections terminate at a Direct Connect gateway and the transit VIFs to the transit gateway.

The company recently acquired a smaller company that is based in Europe. The newly acquired company has only on-premises workloads. The newly acquired company does not expect to run workloads on AWS for the next 3 years. However, the newly acquired company requires connectivity to the parent company's AWS resources in us-east-1 and to the parent company's on-premises environment in the US. The parent company wants to use two new Direct Connect connections in Europe to provide the required connectivity.

Which solution will meet these requirements with the LEAST operational overhead for the newly acquired company?

A. Associate new transit VIFs to the existing Direct Connect gateway. Configure the new transit VIFs to use Direct Connect SiteLink. **Most Voted**

B. Associate new transit VIFs to a new Direct Connect gateway and to a new transit gateway in the eu-west-1 Region. Use transit gateway peering to connect the transit gateways.

C. Associate new private VIFs to the existing Direct Connect gateway. Configure the existing transit VIFs and the new private VIFs to use Direct Connect SiteLink.

D. Associate new private VIFs to a new Direct Connect gateway and to a new VPC in us-east-1. Configure the existing transit VIFs and the new private VIFs to use Direct Connect SiteLink and AWS PrivateLink endpoints in the new VPC.

Correct Answer: A

Community vote distribution

A (100%)

Comments

ashk123456 11 months, 4 weeks ago

Selected Answer: A

 Direct Connect SiteLink enables low-latency, global private networking between on-premises sites. Using the existing Direct Connect gateway avoids additional operational overhead (no need for new transit gateways, VPCs, or peering). Transit VIFs are the correct choice for connecting to a Direct Connect gateway when using SiteLink.

https://zhangxuetu.online

[202610]

Question #271 Topic 1

A company is establishing hybrid cloud connectivity from an on-premises environment to AWS in the us-east-1 Region. The company is using a 10 Gbps AWS Direct Connect dedicated connection. The company has two accounts in AWS. Account A has transit gateways in four AWS Regions. Account B has transit gateways in three Regions. The company does not plan to expand.

To meet security requirements the company's accounts must have separate cloud infrastructure.
Which solution will meet these requirements MOST cost-effectively?

A. Create one Direct Connect gateway in us-east-1. Use AWS Resource Access Manager (AWS RAM) to share the Direct Connect gateway with each account. Create a transit VIF for Account Associate the four transit gateways in Account A to the Direct Connect gateway. Create a transit VIF for Account B. Associate the three transit gateways in Account B to the Direct Connect gateway.

B. Create one Direct Connect gateway in us-east-1 for Account A. Create a second Direct Connect gateway in us-east-1 for Account Create a transit VIF for Account A. Associate the four transit gateways in Account A to the Direct Connect gateway in Account A. Create a transit VIF for Account Associate the three transit gateways in Account B to the Direct Connect gateway in Account B. **Most Voted**

C. Create one Direct Connect gateway in us-east-1. Use AWS Resource Access Manager (AWS RAM) to share the Direct Connect gateway with each account. Create a transit VIF for Account A. Associate the four transit gateways in Account A to the Direct Connect gateway. Order a new 10 Gbps Direct Connect dedicated connection for Account B. Create a transit VIF on the new Direct Connect connection for Account B. Associate the three transit gateways in Account B to the Direct Connect gateway.

D. Create one Direct Connect gateway in us-east-1 for Account A. Create a second Direct Connect gateway in us-east-1 for Account B. Create a transit VIF for Account A. Associate the four transit gateways in Account A to the Direct Connect gateway in Account A. Order a new 10 Gbps Direct Connect dedicated connection for Account B. Create a transit VIF on the new Direct Connect connection for Account B. Associate the three transit gateways in Account B to the Direct Connect gateway in Account B.

Correct Answer: B

Community vote distribution



Comments

Wardove Highly Voted 11 months ago

Selected Answer: B

https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html Transit gateways per AWS Direct Connect gateway limitation is 6 Overall you cannot associate 7 tgws with 1 DXGW so u need 2

a0e6696 7 months ago

Selected Answer: B

max limit is 6.. only 6 tgw we can attach to the one DGW

ashk123456 11 months, 3 weeks ago

Selected Answer: A

 Using a single Direct Connect Gateway (DXGW) reduces costs. AWS RAM allows sharing the DXGW across multiple accounts securely. Each account gets its own transit VIF to ensure separation. No need for additional Direct Connect circuits or gateways, reducing complexity.

https://zhangxuetu.online

[202610]

Question #272 Topic 1

A company runs an application across multiple AWS Regions and multiple Availability Zones. The company needs to expand to a new AWS Region. Low latency is critical to the functionality of the application.

A network engineer needs to gather metrics for the latency between the existing. Regions and the new Region. The network engineer must gather metrics for at least the previous 30 days.

Which solution will meet these requirements?

A. Configure an AWS Network Access Analyzer Network Access Scope, and use the analysis to review the latency.

B. Set up AWS Network Manager Infrastructure Performance. Publish network performance metrics to Amazon CloudWatch. **Most Voted**

C. Use an Amazon VPC Reachability Analyzer path to review the latency.

D. Set up VPC Flow Logs. Publish log metrics to Amazon CloudWatch.

Correct Answer: B

Community vote distribution

B (100%)

Comments

ashk123456 11 months, 3 weeks ago

Selected Answer: B

 AWS Network Manager Infrastructure Performance can monitor and log latency metrics between Regions. It publishes network performance data to CloudWatch, allowing historical analysis for at least 30 days. Minimal setup effort, built-in AWS solution for inter-region latency measurement.

Franck12az31 12 months ago

Selected Answer: B

AWS Network Manager Infrastructure Performance allows latency monitor between AWS region and can gather metrics to 30 days.

Sudeepshiv 12 months ago

Selected Answer: B

The company needs to: Measure latency between AWS Regions before expanding. Analyze historical latency data for the past 30 days. AWS Network Manager Infrastructure Performance is designed for this use case.

https://zhangxuetu.online

[202610]

Question #273 Topic 1

A company operates in the us-east-1 Region and the us-west-1 Region. The company is designing a solution to connect an on-premises data center to the company's AWS environment in us-east-1. The solution uses two AWS Direct Connect connections.

Traffic from us-west-1 to the data center needs to traverse the Direct Connect connections. A network engineer needs to set up active-passive functionality across the two Direct Connect connections by using a Direct Connect gateway to influence inbound traffic from VPCs that are in us-west-1 to the data center.

Which solution will meet these requirements?

A. At the data center, set the local preference for the primary connection to be higher than the local preference for the secondary connection.

B. Use AS path prepending to set the AS path on the primary connection to be longer than the AS path on the secondary connection.

C. Use local preference BGP community tags to apply the 7224:7300 local preference BGP community tag to the prefixes for the primary connection. Apply the 7224:7100 local preference BGP community tag to the prefixes for the secondary connection. **Most Voted**

D. Use local preference BGP community tags to apply the 7224:9300 local preference BGP community tag to the prefixes for the primary connection. Apply the 7224:9100 local preference BGP community tag to the prefixes for secondary connection. **Most Voted**

Correct Answer:

Community vote distribution

C (100%)

Comments

Fox_Mulder 2 weeks, 5 days ago

Selected Answer: C

7224:7300 = High Preference. 7224:7200 = Medium Preference. 7224:7100 = Low Preference.

Anderson01 2 weeks, 5 days ago

Selected Answer: C

Local Preference Communities: AWS provides specific BGP community tags for Private and Transit VIFs to control this behavior. AWS evaluates these tags before other BGP attributes like AS Path length. 7224:7300: High Preference (Active). 7224:7200: Medium Preference. 7224:7100: Low Preference (Passive)

[202610]

Question #274 Topic 1

A company has multiple firewalls and ISPs for its on-premises data center. The company has a single AWS Site-to-Site VPN connection from the company's on-premises data center to a transit gateway. A single ISP services the Site-to-Site VPN connection. Multiple VPCs are attached to the transit gateway.

A customer gateway that the Site-to-Site VPN connection uses fails. Connectivity is completely lost, but the company's network team does not receive a notification.

The network team needs to implement redundancy within a week in case a single customer gateway fails again. The team wants to use an Amazon CloudWatch alarm to send notifications to an Amazon Simple Notification Service (Amazon SNS) topic if any tunnel of the Site-to-Site VPN connection fails.

Which solution will meet these requirements MOST cost-effectively?

A. Replace the existing customer gateway with a new router. Create a new Site-to-Site VPN connection to the transit gateway. For each VPN connection, set up a CloudWatch TunnelState alarm for the VPN connection. Use a value of 0 for the alarm.

B. Use a second customer gateway and a second ISP. Create a new Site-to-Site VPN connection to the transit gateway. For each VPN connection, set up a CloudWatch TunnelState alarm for the VPN connection. Use a value of less than 1 for the alarm. Most Voted

C. Add an AWS Direct Connect connection to the existing Site-to-Site VPN connection to the transit gateway. For each VPN connection, set up a CloudWatch TunnelState alarm for the VPN connection. Use a value of failed for the alarm.

D. Use a second customer gateway with the existing ISP. Create a new Site-to-Site VPN connection to the transit gateway. For each VPN connection, set up a CloudWatch TunnelState alarm for the VPN connection. Use a value of unavailable for the alarm.

Correct Answer:

Question #275 Topic 1

A gaming company operates in one AWS Region. The company's architecture includes an Application Load Balancer (ALB) and Amazon EC2 instances in an Auto Scaling group that support a frontend application. The company uses AWS WAF integrated with the ALB. The ALB has one security group attached to it. The company uses AWS Network Firewall with stateful rules. The company has set up Network ACLs.

The company wants to automatically block access for game users who violate specific rules. The company wants to temporarily block access for problematic users for 1 to 2 hours. The company's software can identify the source IP addresses of problematic users. The company has created a serverless solution to store the IP addresses in Amazon DynamoDB.

The company wants to use its existing serverless architecture to automatically block the problematic users.

Which solution will meet these requirements in the MOST scalable way? (Choose two.)

A. Create a new AWS WAF IP set that the serverless solution updates. Introduce an AWS WAF deny rule to block traffic from any address in the IP set. Most Voted

B. Configure the serverless solution to modify the network ACLs to block traffic from the IP addresses of the problematic users.

C. Configure the serverless solution to modify the ALB security group to block traffic from the IP addresses of the problematic users.

D. Create a new AWS WAF IP set that is updated by the serverless solution. Create an AWS WAF rule to redirect traffic from sources that match the IP set to a new API for the serverless solution.

E. Create an AWS Network Firewall stateless rule to drop traffic from the IP addresses of the problematic users. Configure the serverless solution to update the new rule with the IP addresses of the problematic users. Most Voted

Correct Answer:

掌学兔
ZHANGXUETU

Question #276 Topic 1

A company is setting up an AWS Direct Connect connection between the company's on-premises data center and AWS. The company currently has a single VPC in its AWS account. The on-premises data center uses the 172.16.0.0/16 CIDR block, and the VPC uses the 10.1.1.0/24 CIDR block. The company associates the Direct Connect connection to one private VIF.

A network engineer receives reports that SSH communication from hosts that are in the company's on-premises data center to Amazon EC2 instances that are deployed in the company's VPC is failing. The network engineer investigates and finds that the VIF is up and a BGP peering session has been established properly.

Which steps should the engineer take to troubleshoot this issue? (Choose three.)

A. Ensure that the advertised route for the on-premises network is present in the VPC route tables. Ensure that the VPC's subnets are present in the route tables of the on-premises network equipment. Most Voted

B. Ensure that BGP community tags announcements from the customer gateway router are configured properly.

C. Ensure that the customer gateway router accepts BGP community tags in the prefixes the router receives.

D. Ensure that the VPC network ACLs allow inbound and outbound traffic for the on-premises network prefix. Most Voted

E. Ensure that the security groups for the EC2 instances allow inbound SSH communication from the on-premises network prefix. Most Voted

F. Ensure that the security groups for the EC2 instances allow outbound SSH communication from the on-premises network prefix.

Correct Answer:

Question #277 Topic 1

A company needs to connect its on-premises network to a VPC in the us-east-1 Region. The connection must support a maximum transmission unit (MTU) of 9,000 bytes and must be highly available.

Which solution will meet these requirements MOST cost-effectively?

A. Use AWS Site-to-Site VPN to create two VPNs. Use two connections to two virtual private gateways that are in the same VPC.

B. Use AWS Site-to-Site VPN to create two VPNs. Use two connections to a single transit gateway that has a VPC attachment.

C. Create a multi-site, nonredundant AWS Direct Connect deployment. Use two Direct Connect connections to two separate Direct Connect locations. **Most Voted**

D. Create a multi-site, redundant AWS Direct Connect deployment. Use two Direct Connect connections to one Direct Connect location and two connections to a second Direct Connect location.

Correct Answer:

掌学兔
ZHANGXUETU
[202610]

Question #278 **Topic 1**

A network engineer maintains a company's AWS infrastructure. The network engineer used AWS Transit Gateway to set up a hub and spoke architecture. The network engineer created a shared services VPC to centralize access to interface VPC endpoints.

The company uses AWS Organizations to manage AWS accounts for multiple teams in a single organization. Each team in the company has a separate account and VPC. All the team accounts require access to the interface VPC endpoints.

The network engineer needs a solution to grant each account the minimum required access. Each team's account must have access only to a list of authorized interface VPC endpoints. The solution must have minimal effect on the current architecture.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a separate shared services VPC for each team account. Include the interface VPC endpoints that the team is authorized to use in each VPC. Use a unique transit gateway route table to connect each team's spoke VPC to the team's shared services VPC.

B. Apply security groups to the interface VPC endpoints that are in the shared services VPC. Configure each security group to allow only the CIDR block of the team spoke VPCs that are authorized to use the endpoints included in the security group.

C. Create a unique interface VPC endpoint for each team that is authorized to access a service. Update routing for the shared services VPC so that the CIDR block for each team can access only the set of endpoints the team is authorized to access.

D. Associate an endpoint policy with each interface VPC endpoint. In each policy, deny all the traffic except for traffic from accounts that are authorized to access the corresponding service. Most Voted

Correct Answer:

https://zhangxuetu.online

Question #279 Topic 1

A global network service provider deploys managed AWS Direct Connect connections for its customers. The company wants to integrate monitoring for the connections into its existing ticketing system. The ticketing system runs in the company's VPC on multiple EC2 instances. The ticketing system uses a REST API.

The ticketing system must receive events with minimal latency. The company expects to receive an average of 1 event each day. The company wants to use its existing infrastructure as code (IaC) tooling to configure the monitoring integration solution.

Which solution will meet these requirements in the MOST cost-effective way?

A. Configure an Amazon EventBridge rule to send events to an AWS Lambda function. Configure the Lambda function to process the events and to send events to the ticketing system's REST API. Most Voted

B. Configure a scheduled event in Amazon CloudWatch to run an AWS Lambda function once every minute. Configure the function to poll the AWS API to detect changes in the Direct Connect connection state. Configure the function to submit tickets to the ticketing system's REST API when the function detects state changes.

C. Write a script to poll the AWS API to detect changes in Direct Connect connection state and to submit tickets to the ticketing system's REST API. Deploy the script to the ticketing system's EC2 instance. Schedule the script to run once every minute by using the operating system configuration.

D. Configure an Amazon EventBridge rule to send events directly to an Amazon DynamoDB table. Use Amazon DynamoDB Streams to send the events to an AWS Lambda function. Configure the function to process the events and to send the events to the ticketing system's REST API.

Correct Answer:

Question #280 Topic 1

A network engineer deploys an Application Load Balancer (ALB) in two Availability Zones. There is one target group. There are four Amazon EC2 instance targets in the first Availability Zone and six EC2 instance targets in the second Availability Zone.

During testing, the network engineer notices that the targets in the first Availability Zone receive 40% of the traffic. The targets in the second Availability Zone receive 60% of the traffic. The network engineer needs to update the configuration to prevent traffic from crossing Availability Zones. The network engineer wants to achieve a 50% traffic split across the Availability Zones.

Which solution will meet these requirements?

A. Disable cross-zone load balancing for the target group.

B. Disable cross-zone load balancing for the ALB. Most Voted

C. Disable cross-zone load balancing for all the targets in the first Availability Zone.

D. Disable cross-zone load balancing for all the targets in the second Availability Zone.

Correct Answer:

掌学兔
ZHANGXUETU

Question #281 Topic 1

A company hosts a corporate website on Amazon EC2 instances behind a Network Load Balancer (NLB). The NLB has one TLS listener.

The company wants to use AWS WAF to enhance security for the website.

Which solution will meet this requirement?

A. Attach an Elastic IP address to the NLB. Associate an AWS WAF web ACL with the Elastic IP address.

B. Replace the NLB with an Application Load Balancer (ALB). Associate an AWS WAF web ACL with the ALB. Most Voted

C. Associate an AWS WAF web ACL with the NLB.

D. Associate an AWS WAF web ACL with the EC2 instances that are behind the NLB.

Correct Answer:

掌学兔
ZHANGXUETU
[202610]

Question #282 **Topic 1**

A security company has a domain that stores DNS records in an Amazon Route 53 public hosted zone. The company has configured DNS Security Extensions (DNSSEC) signing for the domain. The domain has no subdomains.

A network engineer must disable DNSSEC signing for the domain. The network engineer must not cause any DNS outage.

Which solution will meet these requirements?

A. Disable DNSSEC signing. Delete the resource record signature (RRSIG) records. Wait for the TTL of the RSIG records to elapse. Deactivate the key-signing keys (KSKs).

B. Deactivate the key-signing keys (KSKs). Wait for the TTL of the KSK records to elapse. Disable DNSSEC signing.

C. Delete the designated signer (DS) record in the parent domain. Wait for the TTL of the DS record to elapse. Disable DNSSEC signing. Deactivate the key-signing keys (KSKs). Most Voted

D. Deactivate the key-signing keys (KSKs). Delete the designated signer (DS) record of the domain. Wait for the TTL of the DS record to elapse. Disable DNSSEC signing.

Correct Answer:

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #283 Topic 1

A company needs to build an integration with its internal ticketing system. The integration will require an AWS Lambda function.

The Lambda function needs to query a REST API that is part of the internal ticketing system. The ticketing system's REST API is accessible only through an Application Load Balancer (ALB) that is in a private subnet in the company's VPC.

The company deploys the Lambda function with the following infrastructure as code (IaC):

```
resource "aws_lambda_function" "this_function" {
  function_name = var.this_name
  role          = aws_iam_role.lambda_role.arn
  handler       = "lambda_code.main.lambda_handler"
  filename      = "code.zip"
  runtime       = "python3.11"
  environment {
    variables = {
      "TS_URL" = var.ticket_system_url
    }
  }
}
```

The IaC deployment succeeds, but the deployed Lambda function times out when it tries to access the ticketing system.

How can the company give the Lambda function the ability to access the ticketing system?

A. Create an AWS PrivateLink endpoint service. Expose the service to the Lambda function.

B. Attach the Lambda function to the ALB's target group by creating a new aws_lb_target_group_attachment resource. Configure the resource to reference both the ALB's ARN and the Lambda function's ARN.

C. Update the Lambda function's security group to include appropriate inbound rules that permit traffic from the VPC.

D. Add a vpc_config section to the Lambda function resource. Configure the vpc_config section to include one or more security group IDs and one or more private subnet IDs that permit access to the ALB. **Most Voted**

Correct Answer:

https://zhangxuetu.online

[202610]

Question #284 Topic 1

A company has several application accounts that include dual-stack VPCs. The company wants to implement a centralized DNS solution that supports IPv6.

A network engineer deploys a shared services VPC. The network engineer sets up network connectivity between the company's application VPCs, the shared services VPC, and the company's on-premises environment with support for IPv4 and IPv6 traffic.

The network engineer is using Amazon Route 53 to implement a centralized DNS solution. The network engineer needs to ensure that resources in the application VPCs have the ability to perform DNS queries against an on-premises DNS resolver.

Which solution will meet this requirement?

A. Create a Route 53 Resolver outbound endpoint in the shared services VPC within a dual-stack subnet. Use AWS Resource Access Manager (AWS RAM) to share the resolver rules to the application accounts. Most Voted

B. Create a Route 53 Resolver inbound endpoint in the shared services VPC within a subnet that supports only IPv6. Use AWS Resource Access Manager (AWS RAM) to share the endpoint to the application accounts.

C. Create a Route 53 Resolver outbound endpoint within a dual-stack subnet in each application VPUse AWS Resource Access Manager (AWS RAM) to share the resolver rules to the application accounts.

D. Create a Route 53 Resolver inbound endpoint within a subnet that supports only IPv4 in each application VPC. Use AWS Resource Access Manager (AWS RAM) to share the resolver rules to the shared services account.

Correct Answer:

https://zhangxuetu.online

Question #285 Topic 1

A company uses an organization in AWS Organizations to manage many AWS accounts that host many VPCs and workloads. The company has an AWS Direct Connect connection between a data center and AWS. The company uses a transit gateway in a central network account to connect the workload VPCs to the data center.

The company wants to tag each transit gateway attachment automatically with information from tags that are attached to each requester account VPC. The company provisions an IAM role in every account. The company assigns the IAM role permissions to retrieve the required tag data from the VPCs and a trust policy that allows principals in the central network account to invoke the IAM role.

Which solution will meet these requirements?

A. Configure AWS Identity and Access Management Access Analyzer to monitor the transit gateway for new attachments. Configure IAM Access Analyzer to invoke an AWS Systems Manager runbook that assumes the IAM role in the requester account and tags the attachment with the required information.

B. Configure an SCP to monitor the transit gateway for new attachments. Configure the SCP to invoke an AWS CloudFormation stack template in the account that requests an attachment to tag the attachment.

C. Configure Amazon VPC IP Address Manager (IPAM) and register the transit gateway. Configure IPAM to run an AWS CDK function when a new IP address is requested from the transit gateway for a new attachment. Configure the CDK function to assume the IAM role in the requester account and to tag the attachment with the required information.

D. Configure AWS Network Manager and register the transit gateway. Create an Amazon EventBridge rule to receive attachment notifications from Network with the required information. Manager and to invoke an AWS Lambda function that assumes the IAM role in the requester account. Configure the Lambda function to tag the attachment. Most Voted

Correct Answer:

掌学兔
ZHANGXUETU

Question #286 Topic 1

A company is using AWS Fargate to deploy many containerized web applications to a VPC. The applications must all be reachable through various DNS names on the standard port for HTTPS traffic. The company uses an Application Load Balancer (ALB) to handle traffic to each of the applications.

The company uses the AWS Cloud Development Kit (AWS CDK) to automate the deployment process. The company uses two types of CDK stacks. The company uses one common stack to build the VPC itself and other shared infrastructure. The company also uses a set of application-specific stacks that contain details and logic for each application.

The company needs to correctly allocate ALB-related resources between the two types of stacks.

Which combination of solutions will provide a repeatable allocation of resources to the common stack and application-specific stacks? (Choose three.)

A. ALB listener in the common stack **Most Voted**

B. ALB listener in the application-specific stacks

C. ALB listener host header rule in the common stack

D. ALB listener host header rule in the application-specific stacks **Most Voted**

E. ALB target group in the common stack

F. ALB target group in the application-specific stacks **Most Voted**

Correct Answer:

掌学兔
ZHANGXUETU
[202610]

Question #287 Topic 1

A company runs applications across multiple AWS accounts. The company uses an organization in AWS Organizations to manage all the accounts. The company runs the applications in VPCs. The applications must be able to communicate with each other.

The company establishes an AWS Direct Connect connection between an on-premises data center and AWS. The company needs to be able to access the VPCs from the on-premises location. The company plans to add more than 100 new applications and VPCs to its AWS environment. The connectivity solution must allow for future growth and simplify the connectivity process from the data center to AWS.

Which solution will meet these requirements?

A. Attach all VPCs that host applications to the Direct Connect connection by using private VIFs. Create a virtual private gateway in each application VPC. Connect a hardware VPN in the data center to the virtual private gateway in each VPC. Configure static routes in all VPCs. Use the data center VPN appliance to route traffic.

B. Create a new AWS account and deploy a network transit VPC. Deploy Amazon EC2 instances that run open source VPN software. Create a virtual private gateway in each application VPC. Configure connections between the instance that runs the VPN software in the network transit VPC and each virtual private gateway, and update the route tables. Connect the open source VPN to a hardware VPN in the data center and configure routing.

C. Create a transit gateway in a new networking account. Use AWS Resource Access Manager (AWS RAM) to create a resource share that has the transit gateways source type. Enter the organization ID share the ID with the transit gateway. Create a private IP VPN that connects to a customer gateway in the data center. Attach the VPN to the transit gateway and configure dynamic routing. Most Voted

D. Create a Direct Connect gateway and associate it with the Direct Connect connection. Attach all VPCs that host applications to the Direct Connect gateway. Create a public VIF and attach it to the gateway. Create an AWS Site-to-Site VPN connection by using the public VIF. Connect to a hardware VPN appliance in the data center and configure dynamic routing.

Correct Answer:

https://zhangxuetu.online

Question #288 Topic 1

A company notices VPC flow log data that shows some company traffic is going to malicious websites. The company identifies the Amazon EC2 instance that is sending traffic to the malicious websites and determines that the application that runs on the instance is compromised.

Similar security events have happened multiple times at the company in the past. The company reacted to previous security events by blocking the malicious websites. The company needs a scalable solution to prevent similar security events in the future.

Which solution will meet this requirement with the LEAST operational overhead?

A. Set up an EC2 instance to run firewall software in the VPC. Route all traffic through the firewall EC2 instance. Maintain a list of known malicious websites on the firewall instance. Disable the source and destination checks for the firewall instance.

B. Set up an Application Load Balancer (ALB) in front of the problematic EC2 instance. Enable AWS WAF on the EC2 instance.

C. Set up an Application Load Balancer (ALB) in front of the problematic EC2 instance. Enable AWS WAF on the ALB.

D. Set up an Amazon Route 53 DNS Firewall rule group. Create a domain list that contains only the domains the application must communicate with to function. Add the domain list to the rule group. Associate the rule group with the VPC. Most Voted

Correct Answer:

掌学兔
ZHANGXUETU
[202610]

Question #289 Topic 1

A company has a hybrid environment. The company uses AWS Direct Connect with a transit VIF attached to a transit gateway to connect its on-premises location to the AWS Cloud. The company operates from a single AWS account in the us-east-1 Region. The company has a legacy application that runs on premises with the corp.example.com DNS name. The company has created an Amazon Route 53 Resolver outbound endpoint and a Resolver rule in us-east-1 in the AWS account.

As part of an expansion, the company creates one more AWS account for a new business unit that operates in us-east-1. The new account has VPCs that are attached to the transit gateway. The new account uses the existing Direct Connect connection to connect to the on-premises location. Applications that run in the new account's VPCs also need to access the on-premises location by using the corp.example.com DNS name.

A network engineer needs to identify a solution to resolve the corp.example.com DNS name from the new account.

Which solution will meet these requirements MOST cost-effectively?

A. Create a hosted transit VIF for the new account on the existing Direct Connect connection. In the new account, create a new Route 53 Resolver outbound endpoint. Also in the new account, create a new Resolver rule that specifies FORWARD as the value for RuleType. Associate the new rule with the VPCs in the new account.

B. Share the Resolver rule from the existing account with the new account by using AWS Resource Access Manager (AWS RAM). Associate the shared rule with the VPCs in the new account. Most Voted

C. Share the Route 53 Resolver outbound endpoint from the existing account with the new account by using AWS Resource Access Manager (AWS RAM). In the new account, create a new Resolver rule that specifies FORWARD as the value for RuleType. Associate the new rule with the VPCs in the new account.

D. Create an AWS Site-to-Site VPN connection between the new account and the on-premises location. Attach the Site-to-Site VPN connection to the existing transit gateway. In the new account, create a new Route 53 Resolver outbound endpoint. Also in the new account, create a new Resolver rule that specifies FORWARD as the value for RuleType. Associate the rule with the VPCs in the new account.

Correct Answer:

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #290 Topic 1

A company has many VPCs in the us-east-1 Region. The company uses a transit gateway to connect the VPCs to one another. The company recently acquired a smaller company that has a single VPC named VPC-Z.

A network engineer needs to onboard VPC-Z to the existing transit gateway. The network engineer notices an IP address overlap between VPC-Z and VPC-A. The network engineer must establish outbound connectivity from VPC-Z to all the company's other VPCs, including VPC-A.

Which combination of solutions will meet this requirement? (Choose two.)

A. Create a new non-overlapping CIDR block in VPC-Z. Create two subnets that use the new CIDR block. Most Voted

B. Create a new non-overlapping CIDR block in VPC-A. Create two subnets that use the new CIDR block.

C. Create a private NAT gateway in VPC-Z in a non-overlapping subnet. Advertise only the non-overlapping VPC-Z CIDR block to the transit gateway route table. Most Voted

D. Create a private NAT gateway in VPC-A in a non-overlapping subnet. Advertise only the non-overlapping VPC-A CIDR block to the transit gateway route table.

E. Create a VPC peering connection between VPC-A and VPC-Z.

Correct Answer:

掌学兔
ZHANGXUETU
[202610]

Question #291 Topic 1

A company has two on-premises data center locations named Data Center 1 and Data Center 2. Each data center has a company-managed customer router. Both data centers have a dedicated AWS Direct Connect connection to the same Direct Connect gateway that uses a private VIF. The company enabled Direct Connect SiteLink when the company created each private VIF. The company uses SiteLink to send data from one Direct Connect location to the other, bypassing AWS Regions.

Data Center 2 hosts an application that a partner company needs to access. The partner wants to access the application from the partner's own data center by using the Direct Connect network. The company's network engineer needs to create a separate isolated network for the partner to establish connectivity between Data Center 2 and the partner's data center.

Which combination of steps will meet these requirements? (Choose two.)

A. Create a new Direct Connect gateway for the partner in an AWS account. Share the account number with the partner to allow the partner to create a hosted VIF to the account. Accept and associate the partner's hosted VIF with the new Direct Connect gateway. Most Voted

B. Provision a separate transit VIF for the partner on the Direct Connect connection at Data Center 2. Connect the transit VIF to the partner-specific Direct Connect gateway.

C. Share the company's AWS account number with the partner to allow the partner to create a hosted VIF to the account. Accept and associate the partner's hosted VIF with the existing Direct Connect gateway.

D. Provision a separate private VIF for the partner on the Direct Connect connection at Data Center 2. Connect the private VIF to the partner-specific Direct Connect gateway. Enable SiteLink. Most Voted

E. Provision a separate public VIF for the partner on the Direct Connect connection at Data Center 2. Connect the public VIF to the partner-specific Direct Connect gateway. Enable SiteLink.

Correct Answer:

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #292 Topic 1

A company wants to use SSL/TLS certificates that are issued by AWS Certificate Manager (ACM) to secure the company's social media web application. The application runs on backend Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses Amazon Route 53 to manage DNS records. The company needs to integrate ACM with the EC2 instances and Route 53.

Which solution will meet this requirement?

A. Request a public certificate from ACM for the domain name that is configured in Route 53. Configure the ALB to use the public certificate Configure the A record in Route 53 to point to the ALB alias. **Most Voted**

B. Request a private certificate from ACM for the domain name that is configured in Route 53. Configure the ALB to use the private certificate. Configure the A record in Route 53 to point to the ALB domain name.

C. Request two private certificates from ACM for the domain name that is configured in Route 53. Configure the ALB to use one private certificate. Configure the A record in Route 53 to point to the ALB alias. Configure the backend EC2 instances to use the second private certificate.

D. Request a private certificate and a public certificate from ACM for the domain name that is configured in Route 53. Configure the ALB to use the public certificate. Configure the A record in Route 53 to point to the ALB domain name. Configure the backend EC2 instances to use the private certificate.

Correct Answer: A

Comments

Gramterre 2 weeks, 2 days ago

Correct answer is A. You need to present a certificate signed by a public authority to the web application clients. The route53 record should point to the ALB Alias.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #293 Topic 1

A company has an AWS Direct Connect connection between an on-premises data center and a single private VIF in the company's VPC. The VPC contains resources that the company has secured by using security groups and network ACLs.

A network engineer adds a subnet in the company's data center during a maintenance period. The network engineer notices that the BGP status for the private VIF is down after the maintenance activity. The Direct Connect connection was fully operational before the maintenance period. The network team verifies that layer 2 connectivity is working between the company's router and the Direct Connect router.

The networking engineer must resolve this issue.

Which solution will meet this requirement?

A. Use route filters or aggregation on the company's router to limit the routes that are advertised from the company's router. **Most Voted**

B. Add a route policy to the company's router to ensure that all routes that are advertised from the company's router are tagged with a correct BGP community string that begins in "7224".

C. Revalidate the physical and logical path between the company's router and the Direct Connect router, including any Direct Connect Partner.

D. Ensure that security groups and network ACLs allow TCP communications to port 179.

Correct Answer: A

Community vote distribution

A (100%)

Comments

gonzales 1 month, 3 weeks ago

Selected Answer: A

The key clues are: * The Direct Connect connection worked before maintenance. * Layer 2 connectivity is still working. * BGP went down immediately after a new on-premises subnet was added. A private VIF can receive at most 100 IPv4 routes and 100 IPv6 routes from the customer router. If the router advertises more than the limit, AWS places the BGP session into an idle state and reports it as down. The new subnet likely caused the number of advertised prefixes to exceed this quota.

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #294 Topic 1

A company uses AWS Cloud WAN as a primary connectivity solution to establish communication between VPCs in a multi-account and multi-Region environment. The company has created an attachment policy statement in the AWS Cloud WAN core network policy. The attachment policy requires acceptance for new VPC attachments, regardless of the segment that the new VPC attachment needs to be associated with.

The company wants to automate acceptance for new VPC attachments based on specific conditions. The company creates an AWS Lambda function to check for the specific conditions. A network engineer must integrate the Lambda function with the company's existing architecture.

Which solution will meet these requirements in the MOST cost-effective way?

A. Update the AWS Cloud WAN core network policy to create a network function group. Select the require acceptance option. Create a service insertion segment action that targets the Lambda function.

B. Create an Amazon EventBridge rule to match AWS Network Manager events for the VPC attachments. Configure the EventBridge rule to invoke the Lambda function when the rule matches. Most Voted

C. Use Amazon CloudWatch logs to stream AWS CloudTrail logs to an Amazon Kinesis data stream. Configure an event source mapping to target the Lambda function to process the event stream.

D. Configure AWS Network Manager as a source for a pipe in Amazon EventBridge Pipes. Create a filter in the pipe for new VPC attachments. Set the Lambda function as the target of the pipe.

Correct Answer: B

Community vote distribution

B (100%)

Comments

gonzales 1 month, 3 weeks ago

Selected Answer: B

D is incorrect: Network Manager doesn't have a queue of events that a Pipe can read.

https://zhangxuetu.online

[202610]

Question #295 Topic 1

A company hosts multiple workloads in a single VPC that has public subnets and private subnets. The company establishes an AWS Direct Connect connection to provide connectivity between the company's on-premises network and the VPC.

The company purchases a domain in its AWS account. The domain needs to resolve to a private Application Load Balancer (ALB) for requests that originate from the company's network. The domain needs to resolve to a public ALB for requests that originate from the internet.

Which solution will meet these requirements?

A. Create an Amazon CloudFront distribution for the domain. Create an AWS Lambda@Edge function that inspects each request and routes requests from the internet to the public ALB. Configure the Lambda@Edge function to route requests from the company's network to the private ALB. Create an Amazon Route 53 public hosted zone for the domain. Include an A record that is configured as an alias that points to the CloudFront distribution.

B. Create an Amazon Route 53 public hosted zone for the domain. Include an alias record that points to the public ALCreate a Route 53 private hosted zone for the domain. Include an alias record that points to the private ALConfigure a Route 53 inbound resolver endpoint on the VPC. Configure the company's network DNS to forward queries for the domain to the endpoint. **Most Voted**

C. Create an Amazon Route 53 public hosted zone for the domain. Include an alias record that points to the public ALB. Create an additional alias record for the domain that routes to the private ALB. Associate a geolocation routing policy with the CIDR range of the company's network.

D. Deploy new Amazon EC2 instances that host DNS servers in each of the private subnets. Configure the DNS servers to return the IP address of the public ALB for requests from the internet. Configure the DNS servers to return the IP address of the private ALB for requests from the company's network. Configure a public Amazon Route 53 inbound resolver to forward all requests for the domain to the EC2 instances. Enable client IP preservation.

Correct Answer: B

Community vote distribution

B (100%)

Comments

gonzales 1 month, 3 weeks ago

Selected Answer: B

This is a split-horizon DNS design: * Internet users resolve the domain through a public hosted zone and receive the public ALB. * On-premises users forward DNS queries over Direct Connect to a Route 53 Resolver inbound endpoint in the VPC. Route 53 answers from the private hosted zone and returns the private ALB. AWS supports public and private hosted zones with the same domain name for this purpose.

https://zhangxuetu.online

掌学兔 ZHANGXUETU
[202610]

Question #296 Topic 1

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company is centralizing VPC endpoint access in a shared services VPC that is in the company's networking AWS account. The company uses a transit gateway to connect the shared services VPC in the networking account to spoke VPCs that are in separate AWS accounts. A network engineer tests the connectivity from the spoke VPCs to the central VPC endpoints and finds that everything works as expected.

The company expects to create new VPC endpoints in the shared services VPC. The network engineer wants to reduce the operational overhead for other teams to configure DNS resolution in an Amazon Route 53 private hosted zone when the other teams add new centralized VPC endpoints. The network engineer plans to use AWS CloudFormation as an infrastructure as code (IaC) solution.

Which combination of actions will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Create a Route 53 Profile. From the networking account, use AWS Resource Access Manager (AWS RAM) to share the Route 53 Profile with the organization. **Most Voted**

B. In a CloudFormation stack set, create an Amazon EventBridge rule that invokes an AWS Lambda function any time a user creates a new private hosted zone.

C. Create an AWS Lambda function that has cross-account permissions. Configure the Lambda function to associate a private hosted zone with each of the spoke VPCs.

D. Create the VPC endpoint, private hosted zone, and private hosted zone association to the Route 53 Profile resources in the same AWS CloudFormation stack in the networking AWS account. **Most Voted**

E. Create an AWS Lambda function that associates the new private hosted zone with the Route 53 Profile.

Correct Answer: AD

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #297 Topic 1

A company is developing a new video streaming application that runs on three Amazon EC2 instances in a VPC across two Availability Zones named AZ-A and AZ-B. Two of the EC2 instances are in AZ-A. The third EC2 instance is in AZ-B. The EC2 instances are part of a target group that is associated with a Network Load Balancer (NLB).

During load testing, the company observes that traffic is not equally distributed across the three instances. The two instances in AZ-A each receive 25% of the traffic. The instance in AZ-B receives 50% of the traffic. There is no latency SLA for the application.

The company wants traffic to be evenly distributed across all three instances.

Which solution will meet this requirement?

A. Ensure that the AZ-A and AZ-B subnet route tables have routes for all targets.

B. Enable cross-zone load balancing on the NLB target group. Most Voted

C. Deploy an Application Load Balancer (ALB) to each Availability Zone. Register the ALBs as targets for the NLB.

D. Replace the NLB with a Gateway Load Balancer (GWLB). Enable cross-zone load balancing for the GWLB.

Correct Answer: B

掌学兔
ZHANGXUETU
[202610]

Question #298 Topic 1

A company is using AWS to deliver applications and services to its employees and customers around the world. Currently, the company has a presence in the us-east-1 Region with multiple VPCs. The company's network team has established a transit gateway in us-east-1 to connect all the VPCs. The transit gateway is associated with an AWS Direct Connect gateway that connects a transit VIF provisioned from Direct Connect. The Direct Connect connection exists between a co-location facility and an on-premises data center in us-east-1.

The network team needs to build out AWS capabilities for employees and customers that are located in the eu-west-2 Region. Some of the employee applications need to access resources in us-east-1 by using the resources' IP addresses. The network connection must be encrypted, and traffic must not use publicly routable IP addresses. The solution must be able to scale to new VPCs that require this connection.

Which solution will meet these requirements with the LEAST operational overhead?

A. Establish a Direct Connect connection in eu-west-2. Establish a public VIF with an IPsec tunnel to connect to virtual private gateways that are attached to the VPCs in eu-west-2 and us-east-1. Route traffic between the VPCs in the two Regions by using the IPsec tunnels.

B. Set up an AWS Global Accelerator endpoint for applications in us-east-1 that the employee applications in eu-west-2 require connectivity with. Change the application code for resources in eu-west-2 to send traffic to the applications in us-east-1 through an internet gateway and the Global Accelerator endpoint.

C. Establish a transit gateway with a different Autonomous System Number (ASN) in eu-west-2. Create attachments to the VPCs in eu-west-2. Create a transit gateway peering attachment between the transit gateway in us-east-1 and the transit gateway in eu-west-2. Update the route tables with static routes between the two Regions. Most Voted

D. Create an inter-Region peering connection between each VPC in eu-west-2 and the target VPCs in us-east-1. Accept the peering attachments in each VPC in us-east-1. Update the route tables with static routes between the two Regions.

Correct Answer: C

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #299 Topic 1

A company creates web applications in multiple AWS accounts in the us-east-2 Region. The company creates Amazon Route 53 public hosted zones in each of the accounts to serve DNS queries for the web applications.

The company needs a solution to log all DNS queries to the public hosted zones for further analysis.

Which solution will meet this requirement?

A. Create an Amazon CloudWatch Logs log group in the us-east-1 Region in each account. Configure query logging for the public hosted zones. **Most Voted**

B. Create an Amazon S3 bucket in us-east-2. Update the public hosted zone in each account to publish logs to the S3 bucket.

C. Create an Amazon CloudWatch Logs log group in us-east-2 in one AWS account. Configure query logging for the public hosted zones.

D. Create an Amazon S3 bucket in the us-east-1 Region. Update the public hosted zone in each account to publish logs to the S3 bucket.

Correct Answer: A

https://zhangxuetu.online

掌学兔
ZHANGXUETU

Question #300 Topic 1

A company establishes an AWS Site-to-Site VPN connection between an on-premises data center and the company's VPC. Users report a loss of connectivity after the company moves a VPN device behind a new firewall. A network engineer investigates the connectivity issue and confirms that the AWS Region that the Site-to-Site VPN connection connects to is reachable through the internet.

What is the likely cause of this connectivity issue?

A. Dead Peer Detection (DPD) timeout expired after the company moved the VPN device.

B. The new firewall is blocking UDP port 4500. Most Voted

C. The network engineer needs to include the new firewall IP address in the security group.

D. The network engineer needs to update a tunnel initiation option.

Correct Answer: B

Question #301 Topic 1

A company has an existing AWS Site-to-site VPN connection between a transit gateway and an on-premises data center for IPv4 traffic. The data center is migrating to IPv6. A network engineer must update existing VPCs on AWS to IPv6.

The network engineer starts with a test VPC by associating IPv6 with the test VPC. The network engineer deploys test Amazon EC2 instances to an IPv6-only subnet.

What should the network engineer do next to test connectivity between the test VPC and the data center by using IPv6?

A. Create a new Site-to-Site VPN connection that supports IPv6. Configure the customer gateway in the data center.

B. Enable IPv6 support on the existing Site-to-Site VPN connection. Reconfigure the customer gateway in the data center.

C. Create a new dual-stack Site-to-Site VPN connection. Configure the customer gateway in the data center. Most Voted

D. Enable dual-stack support on the existing Site-to-Site VPN connection. Reconfigure the customer gateway in the data center.

Correct Answer: C

掌学兔
ZHANGXUETU
[202610]

Question #302 Topic 1

A company deploys a set of applications on Amazon EC2 instances. The company applies a security group named sg-all to every EC2 instance to allow communication between the instances.

The company plans to use an AWS CloudFormation stack to launch more EC2 instances. The stack contains an AWS::EC2::SecurityGroup CloudFormation resource. The stack also contains all elements of the necessary infrastructure except for an element that references the sg-all security group. The company needs to configure the security group in CloudFormation.

Which solution will meet this requirement MOST quickly?

A. Add the security group resource to the Outputs section of the stack. Deploy the stack. Copy the CloudFormation stack to a new file, edit the file, and add a rule to the existing security group. Use a reference to the security group from the Outputs section of the deployed stack. Use the new file to update the deployed stack.

B. Create an AWS::Lambda::Function resource that includes a DependsOn attribute that is equal to the name of the security group CloudFormation resource. Add the AWS Lambda function resource to the stack. Include API calls to add the security group's name to the security group. Deploy the stack.

C. Add an AWS::EC2::SecurityGroupIngress Cloud Formation resource to the stack. Include a reference to the name of the security group resource in the Properties section of the resource. Deploy the stack. Most Voted

D. Add a duplicate of the existing AWS::EC2::SecurityGroup CloudFormation resource to the stack. Configure the duplicate security group resource to include the name of the existing security group resource. Apply the duplicate security group resource on the new EC2 instances. Deploy the stack.

Correct Answer: C

https://zhangxuetu.online

掌学兔
ZHANGXUETU
[202610]

Question #303 Topic 1

A company is migrating an internal application to the AWS Cloud. The company deploys an SSL VPN service on a group of Amazon EC2 instances. The company will use the SSL VPN service to allow users to access the application from remote locations worldwide. The company must minimize latency between users and the application.

Which solution will meet these requirements?

A. Create an Amazon CloudFront distribution. Add the SSL VPN EC2 instances as the content origin.

B. Deploy AWS Direct Connect private VIFs with SiteLink to connect remote locations to the AWS Region that hosts the application.

C. Deploy multiple SSL VPN EC2 instances in the same AWS Region. Use a Network Load Balancer (NLB) to distribute traffic across the instances.

D. Create an accelerator in AWS Global Accelerator. Add the SSL VPN EC2 instances to the endpoint group of the accelerator. Most Voted

Correct Answer: D

https://zhangxuetu.online

Question #304 Topic 1

A company runs workloads in multiple VPCs. A pair of Amazon EC2 instances are experiencing issues when the instances attempt to communicate with one another. A network engineer suspects that the issue is in the application layer. The network engineer needs to troubleshoot the issue.

The network engineer configures VPC flow logs for one of the EC2 instances. The VPC flow logs display correct headers for the packets from the instance. The network engineer is unable to check the validity of the application layer.

What should the network engineer do next to troubleshoot this issue?

A. Configure VPC flow logs for the second EC2 instance. Analyze the information in the VPC flow logs.

B. Configure VPC flow logs for the source VPC and the destination VPC. Analyze the information in the VPC flow logs.

C. Configure Amazon VPC Traffic Mirroring on the EC2 instance interfaces. Configure a new monitoring instance as the mirror target. Analyze the packets for application layer correctness. Most Voted

D. Configure Amazon VPC Traffic Mirroring on the VPCs where the EC2 instances are deployed. Configure a new monitoring instance as the mirror target. Analyze the packets for application layer correctness.

Correct Answer: C

掌学兔
ZHANGXUETU
[202610]

Question #305 Topic 1

A company uses on-premises DNS servers. The company has Amazon Route 53 private hosted zones in a single VPC. The company wants to query the Route 53 private hosted zones from the on-premises location.

Which combination of steps will meet this requirement? (Choose three.)

A. Create a Route 53 Resolver inbound endpoint. Most Voted

B. Create a Route 53 Resolver outbound endpoint.

C. Configure a conditional forwarder on the on-premises DNS servers. Set the Route 53 Resolver endpoint as the destination. Most Voted

D. Configure an AWS PrivateLink endpoint service, and set the VPC resolver as the target.

E. Set up private connectivity between the on-premises location and the company's VPC. Most Voted

F. Create Route 53 Resolver rules for each private hosted zone.

Correct Answer: ACE

https://zhangxuetu.online

Question #306 Topic 1

A company deploys a centralized inspection architecture that uses Gateway Load Balancers (GWLBs) and a transit gateway. The company uses a VPC attachment to connect spoke VPCs to the transit gateway. The company must inspect network traffic for the spoke VPCs. The spoke VPCs have a default route that uses the transit gateway as the next hop. The company deploys GWLBs and virtual appliances to each Availability Zone in a centralized appliance VPC. The company connects the appliance VPC to the transit gateway by using a VPC attachment.

A network engineer discovers that HTTP traffic from an Amazon EC2 instance that is located in Availability Zone 1 in Spoke VPC 1 to an EC2 instance in Availability Zone 2 in Spoke VPC 2 is not reaching its destination. Security appliance logs do not show any established sessions. When the network engineer forwards traffic between EC2 instances in the same Availability Zone from Spoke VPC 1 to Spoke VPC 2, the traffic arrives and security appliance logs show established sessions. The network engineer checks the configuration and finds that both the security group and the network ACL are configured correctly. Neither the security group nor the network ACL are blocking any cross-Availability Zone traffic.

Which solution will fix the connectivity failure?

A. Configure each spoke VPC to have a static route entry that points the CIDR block of the EC2 instances to the transit gateway.

B. Configure the virtual appliances to send traffic with a maximum transmission unit (MTU) of 9,000 bytes.

C. Set the TCP keep-alive setting to less than 350 seconds in the operating system of the virtual appliances.

D. Enable appliance mode for the VPC attachment for the centralized appliance VPC. Most Voted

Correct Answer: D