aws training and certification

AWS 认证高级网络 — 专项
AWS Certified Advanced Networking – Specialty
（ANS-C00）考试样题

1）公司中本地网络的 IP 地址范围是 11.11.0.0/16。只有此网络范围内的 IP 才可用于服务器间的通信。IP 地址范围 11.11.253.0/24 已经分配用于云。

一名网络工程师打算在 AWS 上设计一个 VPC，并且使该 VPC 中的服务器能够通过 VPN 连接与 Internet 和本地的服务器进行通信。

以下哪些配置步骤组合能够满足这些要求？（选择两项。）

A）将 VPC 的 IP 地址范围设置为 11.11.253.0/24。

B）为 VPC 设置 RFC 1918 私有 IP 地址范围（例如，10.10.10.0/24）。设置 NAT 网关，为所有出站流量进行 10.10.10.0/24 与 11.11.253.0/24 之间的转换。

C）在虚拟专用网关与本地路由器之间设置 VPN 连接。将虚拟专用网关设置为所有流量的默认网关。配置本地路由器，将流量转发到 Internet。

D）在虚拟专用网关与本地路由器之间设置 VPN 连接。针对发往 11.11.0.0/24 的流量，将虚拟专用网关设置为默认网关。添加 VPC 子网路由，针对 Internet 流量将默认网关指向 Internet 网关。

E）为 VPC 设置 RFC 1918 私有 IP 地址范围（例如，10.10.10.0/24）。对于指向 11.11.0.0/16 的所有出站数据包，将虚拟专用网关设置为执行源 IP 转换。

2）网络工程师需要为运行在 Amazon EC2 实例上的应用程序设计一个解决方案，以连接到位于不同 VPC 和区域中的可公开访问的 Amazon RDS 多可用区数据库实例。出于安全方面的要求，流量不可通过 Internet 传输。

以下哪种配置可以确保实例能够进行私密通信而不通过 Internet 路由流量？

A）在 VPC 之间创建对等连接，并更新路由表以在 VPC 之间路由流量。为 VPC 对等连接启用 DNS 解析支持。配置应用程序以连接到数据库实例的 DNS 终端节点。

B）创建指向数据库实例的网关终端节点。更新应用程序 VPC 中的路由表，将流量路由到网关终端节点。

C）配置传输 VPC，在 VPC 之间私密地路由流量。配置应用程序以连接到数据库实例的 DNS 终端节点。

D）在 EC2 实例所处的子网中创建 NAT 网关。更新应用程序 VPC 中的路由表，通过 NAT 网关将流量路由到数据库实例的 DNS 终端节点。

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved | aws.amazon.com

3）一家公司在 AWS 上实施了关键业务环境。出于合规性目的，网络工程师需要验证 Amazon EC2 实例是否在使用经过审批的特定安全组并属于特定 VPC。实例的配置历史记录应进行记录，并在出现任何合规性问题时，应自动停止实例。

满足这些要求需要采取哪些措施？

A）启用 AWS CloudTrail 并创建自定义 Amazon CloudWatch 警报，以执行所需的检查。当 CloudWatch 警报处于失败状态时，触发停止此实例的操作以停止不合规的 EC2 实例。
B）使用 AWS CloudWatch Events 配置计划事件来调用 AWS Lambda 函数执行所需的检查。在出现不合规的资源时，可调用其他 Lambda 函数来停止 EC2 实例。
C）针对 EC2 实例状态更改通知使用 AWS CloudWatch Events 配置一个事件，用于触发 AWS Lambda 函数执行所需的检查。在出现不合规的资源时，可调用其他 Lambda 函数来停止 EC2 实例。
D）启用 AWS Config 并创建自定义 AWS Config 规则以执行所需的检查。在出现不合规的资源时，使用修正操作来执行 AWS Systems Manager 文档以停止 EC2 实例。

4）一家公司正在将其本地数据中心扩展到 AWS。预计峰值流量的范围在 1 Gbps 到 2 Gbps 之间。网络工程师必须确保 AWS 与数据中心之间有足够的带宽来处理峰值流量。该解决方案应具备高可用性且经济实惠。

应该实施什么解决方案来满足这些需求？

A）部署具有 IPsec VPN 备份的 10 Gbps AWS Direct Connect 连接。
B）在一个链路聚合组中部署两个 1 Gbps AWS Direct Connect 连接。
C）在一个链路聚合组中，部署面向两个不同 Direct Connect 位置的两个 1 Gbps AWS Direct Connect 连接。
D）部署面向两个不同 Direct Connect 位置的一个 10 Gbps AWS Direct Connect 连接。

5）网络工程师需要将公司 Amazon S3 存储桶的访问权限限制为特定的源网络。

网络工程师应该采取什么措施来实现这一点？

A）在 S3 存储桶上创建 ACL，将访问权限限制为指定网络上的 CIDR 块。
B）在 S3 存储桶上创建存储桶策略，使用条件语句将访问权限限制为指定网络上的 CIDR 块。
C）创建安全组，允许对指定网络的 CIDR 块进行入站访问，并对 S3 存储桶应用安全组。
D）创建安全组，允许对指定网络的 CIDR 块进行入站访问，创建 S3 VPC 终端节点并对 VPC 终端节点应用安全组。

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved | aws.amazon.com

6）一家公司的合规性要求指定必须收集和分析 Web 应用程序日志以确定任何恶意活动。网络工程师还需要监控更改 Web 实例的网络接口的远程尝试。

哪些服务和配置可以满足这些要求？

A) 在 Web 实例上安装 Amazon CloudWatch Logs 代理来收集应用程序日志。使用 VPC 流日志将数据发送到 CloudWatch Logs。使用 CloudWatch Logs 指标筛选条件定义日志数据中的查找模式。

B) 配置 AWS CloudTrail，将所有管理和数据事件记录到自定义 Amazon S3 存储桶和 Amazon CloudWatch Logs 中。使用 VPC 流日志将数据发送到 CloudWatch Logs。使用 CloudWatch Logs 指标筛选条件定义日志数据中的查找模式。

C) 配置 AWS CloudTrail，将所有管理事件记录到自定义 Amazon S3 存储桶和 Amazon CloudWatch Logs 中。在 Web 实例上安装 Amazon CloudWatch Logs 代理来收集应用程序日志。使用 CloudWatch Logs Insights 定义日志数据中的查找模式。

D) 启用 AWS Config 来记录对 Web 实例的所有配置更改。配置 AWS CloudTrail，将所有管理和数据事件记录到自定义 Amazon S3 存储桶中。对于在 Amazon S3 中存储的日志数据，使用 Amazon Athena 定义在其中查找的模式。

7）一家公司使用某个应用程序处理机密数据。数据当前存储在本地数据中心。网络工程师正在将工作负载迁移到 AWS，并且需要确保数据在传输到 AWS 过程中的机密性和完整性。该公司已经有 AWS Direct Connect 连接。

网络工程师应执行哪些步骤，以在本地数据中心和 AWS 之间设置最经济高效的连接？（选择两项。）

A) 将 Internet 网关附加到 VPC。

B) 在 AWS Direct Connect 连接上配置公有虚拟接口。

C) 配置指向虚拟专用网关的私有虚拟接口。

D) 在客户网关与 Amazon EC2 上的软件 VPN 之间设置 IPsec 隧道。

E) 在客户网关与虚拟专用网关之间设置站点到站点 VPN。

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved | aws.amazon.com

8）一家公司正在为其电子商务网站创建新功能。这些功能将部署为微服务，并且每个服务使用不同的域名。该公司需要为其面向公众的所有网站使用 HTTPS。应用程序需要客户端的源 IP。

应该采取哪些操作组合来达到此目的？（选择两项。）

A）使用网络负载均衡器将流量分发到各个服务。
B）使用 Application Load Balancer 将流量分发到各个服务。
C）配置应用程序，使用 X-Forwarded-For 标头检索客户端 IP。
D）配置应用程序，使用 X-Forwarded-Host 标头检索客户端 IP。
E）配置应用程序，使用 PROXY 协议标头检索客户端 IP。

9）网络工程师正在 AWS 上设计高性能计算解决方案的架构。该系统包含 Amazon EC2 实例集群，在这些实例之间需要提供低延迟通信。

以下哪种方法可以满足这些要求？

A）在单个子网中启动实例，子网的大小等于集群所需的实例数。
B）创建集群置放群组。在置放群组中启动支持 Elastic Fabric Adapter (EFA) 的实例。
C）启动具有最多可用核心数和 RAM 的 Amazon EC2 实例。连接 Amazon EBS 预配置 IOPS (PIOPS) 卷。在集群中的所有实例上实施共享内存系统。
D）选择提供增强联网功能的 Amazon EC2 实例类型。将 10 Gbps 非阻止弹性网络接口附加到实例。

10）一家公司的内部安全团队收到了请求，希望能够从公司网络内部访问 Amazon S3。所有外部流量必须经过明确允许才能通过公司防火墙。

安全团队如何授予此访问权限？

A）调度一个脚本，从 AWS 开发人员论坛公告中下载 Amazon S3 IP 前缀。相应地更新防火墙规则。
B）调度一个脚本，从 ip-ranges.json 文件下载并解析 Amazon S3 IP 前缀。相应地更新防火墙规则。
C）调度一个脚本，在 Amazon S3 终端节点上执行 DNS 查找。相应地更新防火墙规则。
D）使用 AWS Direct Connect 将数据中心连接至 VPC。创建路由，将来自数据中心的流量转发到 Amazon S3 VPC 终端节点。

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved | aws.amazon.com

答案

1) A, C — VPC 需要使用指定范围内的 CIDR 块（并且与数据中心不重叠）。未将 VPC 作为目标的所有流量路由到虚拟专用网关（假定已采用此路由），并且在到达本地后，必须随后转发到 Internet。B 和 E 不正确的原因是，它们不在指定的范围（非 RFC 1918 地址可在 VPC 中使用）内。D 不正确的原因是，它会将所有流量通过 Internet 网关定向到 Internet。

2) A — 在 VPC 对等连接上配置 DNS 解析会允许将来自应用程序 VPC 的查询解析为数据库实例的私有 IP，并防止通过 Internet 进行路由。B 不正确的原因是，网关终端节点不支持 Amazon RDS。C 和 D 不正确的原因是，数据库终端节点将解析为公有 IP，流量将流经 Internet。

3) D — AWS Config 提供用户 AWS 账户中 AWS 资源的详细配置视图。将 AWS Config 规则与 AWS Systems Manager Automation 文档配合使用可以自动修正不合规的资源。

4) C — 提供具备高可用性的充足带宽需要两个 AWS Direct Connect 连接以及两个链路聚合组，且位于两个不同的 Direct Connect 位置。如果一个 Direct Connect 位置出现故障，第二个 Direct Connect 位置的两个 Direct Connect 连接将提供备份。所有其他选项都无法在连接丢失时处理峰值流量。

5) B — 当请求源自特定范围的 IP 地址时，使用条件语句的 Amazon S3 存储桶策略将支持限制访问。A 不正确的原因是，S3 ACL 不支持 IP 限制。C 不正确的原因是安全组无法应用到 S3 存储桶。D 不正确的原因是安全组无法应用到 S3 VPC 终端节点。

6) C — Web 应用程序日志位于操作系统内部，Amazon CloudWatch Logs Insights 可用于通过 CloudWatch 代理收集和分析日志。AWS CloudTrail 监控所有 AWS API 活动，并可用于监控特定 API 调用以确定更改 Web 实例的网络接口的远程尝试。

7) B, E — 在 AWS Direct Connect 连接上设置 VPN 可保护传输中的数据。所要执行的步骤为：设置公有虚拟接口，并使用公有虚拟接口在数据中心和虚拟专用网关之间创建站点到站点 VPN。A 不正确的原因是，它会通过公有 Internet 发送流量。C 无法实现的原因是，公告 VPN 隧道 IP 需要公有虚拟接口。D 不正确的原因是，它不会利用现有的 Direct Connect 连接。

8) B, C — Application Load Balancer 支持主机托管的路由，这是基于域名将流量路由到不同微服务所必需的。X-Forwarded-For 是正确的请求标头，可以标识客户端的源 IP 地址。

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved | aws.amazon.com

9) B — 集群置放群组和 Elastic Fabric Adapters (EFA) 对于可从低延迟和/或高网络吞吐量中获益的高性能计算应用程序，这是推荐之选。A 不正确的原因是，子网的大小对网络性能没有影响。C 不正确的原因是，Amazon EBS 卷无法在 Amazon EC2 实例之间共享。D 仅解决了一半问题，因为增强网络功能影响 EC2 实例的网络行为，但不影响实例之间的网络基础设施。

10) B — ip-ranges.json 文件包含 AWS 使用的最新 IP 地址列表。AWS 不再通过开发人员论坛公告发布 IP 前缀。DNS 查找无法提供详尽的可用 IP 前缀列表。D 需要传递路由，这无法实现。

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved | aws.amazon.com