Questions

1) A company is planning to lift and shift its on-premises SAP Business Suite on SAP HANA workload to AWS. The production database is 15 TB in size. The downtime for production migration is limited to a few hours. The company will use SAP HANA system replication to migrate the SAP HANA database. After migration to AWS, the company's remote workforce and business partners need to connect to this SAP Business Suite on SAP HANA instance with an internet connection and an OpenVPN-compatible client in a secure way.

   Which connectivity solution will meet these requirements?

   A) Use a direct internet connection with a single public subnet and an internet gateway during and after migration to AWS.
   B) Use an AWS Site-to-Site VPN connection during migration. Use an AWS Direct Connect connection after migration to AWS.
   C) Use an AWS Direct Connect connection during migration. Use an AWS Site-to-Site VPN connection after migration to AWS.
   D) Use an AWS Direct Connect connection during migration. Use an AWS Client VPN connection after migration to AWS.

2) A global retail company wants to move its SAP application to AWS. Currently, the company's SAProuter is in the DMZ in the company's own data center. The company wants to keep a similar architecture in the AWS Cloud.

   What is the MOST secure solution that meets these requirements?

   A) Launch the instance that the SAProuter software is installed on into a public subnet of the VPC. Assign the instance an Elastic IP address. Use the Secure Network Communications (SNC) type of internet connection. Create a specific security group for the SAProuter instance. Include rules to allow the required inbound and outbound access to the SAP support network.
   B) Launch the instance that the SAProuter software is installed on into a private subnet of the VPC. Assign the instance an Elastic IP address. Do not allow any inbound or outbound access to the SAP support network over the internet.
   C) Launch the instance that the SAProuter software is installed on into a public subnet of the VPC. Assign the instance an Elastic IP address. Use an unencrypted internet connection. Create a specific security group for the SAProuter instance. Include rules to allow all inbound and outbound access to the SAP support network.
   D) Launch the instance that the SAProuter software is installed on into a public subnet of the VPC. Assign the instance an Elastic IP address. Use the Secure Network Communications (SNC) type of internet connection. Create a specific security group for the SAProuter instance. Include rules to block all inbound and outbound access to the SAP support network.

3) An SAP solutions architect needs to design a three-system SAP landscape that consists of a development system, a quality system, and a production system. The systems will run on Amazon EC2 instances. The development system and the quality system will run for 8 hours during weekdays. The production system will run 24 hours a day, 7 days a week.

The size of the production system will increase significantly during the next year. The SAP solutions architect must create a design to ensure that production capacity is always available.

Which combination of EC2 instance purchasing options will meet these requirements MOST cost-effectively? (Select TWO.)

A) On-Demand Instances for the development system and the quality system
B) Spot Instances for the development system and the quality system
C) Spot Instances for the production system
D) EC2 Instance Savings Plan with On-Demand Capacity Reservations for the production system
E) On-Demand Instances for the production system

4) A global retail company has SAP Fiori embedded with SAP S/4HANA Finance application servers that run in a private subnet in a dedicated SAP VPC on AWS. The database tier runs on SAP HANA, which resides in the same private subnet. The company has deployed a Network Load Balancer (NLB) in a public subnet. The company has configured the NLB to send user traffic from outside the AWS network to the SAP application servers directly.

An SAP solutions architect needs to expose the user interface (UI) layer's web services for remote access through a public internet web application. The application will handle cross-domain requests such as URL redirecting, filtering, and rewriting. The whole architecture will be distributed across multiple Availability Zones with hot standby for SAP HANA database components and SAP application components. The existing NLB will work as is. During failover, the NLB will redirect user traffic to the secondary Availability Zone after SAP is installed and running.

How can the SAP solutions architect securely implement a connection between the UI layer's web services and the SAP application?

A) Use the NLB and Amazon Route 53 to send the encrypted traffic from the internet directly to the SAP Fiori application that is installed in the private subnet.
B) Install an SAP Web Dispatcher with no public IP address in the same private subnet as the SAP application. Configure the SAP Web Dispatcher to accept only HTTPS requests from the NLB. Allow the SAP Web Dispatcher IP address in the security group rule of the backend SAP application.
C) Install a third-party tool that can consume web services and the objects that contain business logic.
D) Install an SAP Web Dispatcher in the public subnet. Configure the SAP Web Dispatcher to accept only HTTPS requests from the NLB. Install SAP. Allow the SAP Web Dispatcher IP address in the security group rule of the backend SAP application.

5) An SAP technical architect is working on a high availability setup of an SAP application that is running on an SAP HANA database in the AWS Cloud. Primary and secondary SAP HANA databases are running in separate private subnets in different Availability Zones within an AWS Region. The clustering solution is using SUSE Linux Enterprise High Availability Extension.

The VPC CIDR range where these SAP systems are hosted is 10.0.0.0/16. The overlay IP address that is assigned for the ASCS/ERS cluster is 10.9.9.9. The overlay IP address that is assigned for the SAP HANA cluster is 10.0.9.9. SAP HANA system replication is configured, but the cluster solution for the SAP HANA database is not working.

What should the SAP technical architect do to resolve this issue?

A) Determine whether the SAP HANA instances have an assigned public IP address. If they do not have an assigned public IP address, assign a public IP address and try again.
B) Change the VPC CIDR range to 10.0.0.0/8 to accommodate the overlay IP address assignment.
C) Use a different overlay IP address that is outside the VPC CIDR range for the SAP HANA cluster.
D) Configure SAP HANA system replication after the cluster setup is complete.

6) A company has been using SAP S/4HANA with terabytes of data on premises to run its financial system. The company needs to migrate the SAP landscape to AWS. The on-premises data center is connected to an AWS Region through a 1 Gbps AWS Direct Connect connection. The company's networking team has ensured that the full bandwidth is available for the SAP migration project. An SAP solutions architect needs to migrate the on-premises systems by implementing a solution that minimizes downtime.

Which solution will meet these requirements?

A) Use Amazon S3 Transfer Acceleration to perform backup and restore.
B) Use SAP Software Update Manager (SUM) Database Migration Option (DMO) with System Move for migration. Use AWS Snowball to transfer the export files.
C) Use SAP HANA system replication.
D) Use SAP classical export/import (R3load based).

7) A company's SAP production workloads are running in an on-premises environment on VMs on the VMware vSphere and Microsoft Hyper-V platforms. The company needs to move its SAP workloads to AWS.

An SAP solutions architect is planning to move the on-premises SAP VMs in parallel to the AWS Cloud. The migration solution must minimize downtime and must not affect the SAP system's performance during the migration. For security purposes, no tool or agent can be installed for the migration.

Which solution meets these requirements?

A) Use AWS Application Migration Service (CloudEndure Migration) to set up a lightweight replication server. Perform cutover by launching Amazon EC2 instances based on the designed blueprint.
B) Use the AWS CLI to export the VMs into OVA files. Upload the OVA files into Amazon S3 by using S3 multipart upload. Import the OVA files by using the ec2 import-image command.
C) Use AWS Application Discovery Service with AWS Migration Hub to collect server specification information. Initiate the VM migration through the Migration Hub console.
D) Use AWS Server Migration Service (AWS SMS) to set up a replication job that replicates the on-premises VMs to AWS as AMIs.

8) A company is running its SAP workload on Oracle and VMware. The company needs to change the platform to AWS and migrate the SAP workload from Oracle to an SAP HANA database.

Which solutions can the company use to achieve this goal? (Select TWO.)

A) Change the platform and migrate the SAP workload by using SAP Software Provisioning Manager.
B) Change the platform and migrate the SAP workload by using AWS Application Migration Service (CloudEndure Migration).
C) Change the platform and migrate the SAP workload by using SAP Software Update Manager (SUM) Database Migration Option (DMO) with System Move.
D) Migrate the database by using AWS Database Migration Service (AWS DMS). Migrate the SAP workload by using AWS Application Migration Service (CloudEndure Migration).
E) Change the platform and migrate the SAP workload by using VM Import/Export on AWS.

9) As part of checks before an upgrade, an SAP solutions architect is gathering information about a production SAP instance that is running on AWS. In SAP transaction ST06, monitoring information that is related to only AWS infrastructure of the SAP system is not available. However, other SAP application-level information is present.

   What could be the cause of this issue?

   A) The AWS Data Provider for SAP agent is not installed or has an error.
   B) The Amazon CloudWatch agent is not installed or has an error.
   C) The SAP HANA monitoring agent is not installed or has an error.
   D) The AWS DataSync agent is not installed or has an error.

10) A company has been using a third-party backup tool that uses backint for data protection of SAP HANA on AWS. Because of cost and the effort that is required to maintain the dedicated backup server, the company is considering the use of AWS Backint Agent for SAP HANA.

    The SAP HANA system uses General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volumes for the SAP HANA data volumes and log volumes. Backup files are stored in an Amazon S3 bucket. An SAP solutions architect is setting up a proof-of-concept deployment for this new environment and needs to improve the speed of the database backup and restore procedures.

    Which solutions will meet these requirements? (Select TWO.)

    A) Increase the S3 bucket size. Ensure that access to the S3 bucket comes from an Amazon EC2 instance in the same AWS Region.
    B) Adjust the number of parallel backup channels by increasing the value of the parallel_data_backup_backint_channels SAP HANA parameter.
    C) Use S3 Transfer Acceleration to configure transfer of backup files.
    D) Check how much storage throughput is available to the SAP HANA EBS data volumes (/hana/data). Modify the SAP HANA EBS data volumes to a Provisioned IOPS SSD volume type, and try the backup again.
    E) Enable deduplication for the backup files.

Answers

1) D – A dedicated network connection and low latency are required for the transfer of 15 TB of data over the network in the time allocated for the migration. AWS Direct Connect meets this purpose. The company would need 3 hours to transfer 15 TB of data by using a 10 Gbps Direct Connect connection.

   AWS Client VPN provides a fully managed VPN service that can be accessed from anywhere with an internet connection and an OpenVPN-compatible client. This approach meets the requirements to allow the company's remote workforce and business partners to connect to the SAP landscape in a secure manner.

2) A – When you set up an SAP environment on AWS, you need to set up an SAP Solution Manager system and SAProuter with a connection to the SAP support network. When you set up the SAProuter and SAP support network connection, follow these guidelines:
   - Launch the instance that the SAProuter software is installed on into a public subnet of the VPC. Assign the instance an Elastic IP address.
   - Create a specific security group for the SAProuter instance with the necessary rules to allow the required inbound and outbound access to the SAP support network.
   - Use the Secure Network Communications (SNC) type of internet connection. For more information, see Remote Support in the SAP Support Portal.

   The SAP all-on-AWS architecture diagram provides an illustration of this architecture.

   In VPC security groups, it is possible to specify allow rules, but not deny rules.

3) A, D – Because the development system and the quality system will run for only 8 hours each day on weekdays, On-Demand Instances are the most cost-effective purchasing option for these systems. SAP systems are stateful and cannot be abruptly interrupted, so Spot Instances are not appropriate for this scenario.

   The production system will continue to grow in size, and capacity needs to be guaranteed. A combination of Savings Plans and On-Demand Capacity Reservations will provide the most cost-effective purchasing option for the production system while also ensuring that capacity is available when it is needed.

   For more information about purchasing recommendations for SAP systems, see SAP on AWS Pricing Fundamentals in AWS documentation.

4) D – A Network Load Balancer supports a high availability deployment of SAP Web Dispatchers across multiple Availability Zones. Network Load Balancers function at the fourth layer of the Open Systems Interconnection (OSI) model and can handle millions of requests each second. After the Network Load Balancer receives a connection request, it selects a target from the target group to route network connection requests to a destination address. This destination address can be an overlay IP address that is associated with an SAP Web Dispatcher that runs in a public subnet.

For more information, see the Load Balancing section of Architecture guidelines and decisions in AWS documentation.

5) C – An overlay IP address must be configured to use a non-VPC CIDR block to access the active SAP instance. With overlay IP routing, you can allow the AWS network to use a non-overlapping RFC1918 private IP address that resides outside a VPC CIDR range and direct the SAP traffic to any instance setup across the Availability Zone within the VPC by changing the routing entry in AWS.

   IP address assignments within a VPC cannot extend across multiple Availability Zones or be reassigned to a secondary instance in a different Availability Zone during a failover scenario.

   For more information, see SAP on AWS High Availability Setup in AWS documentation.

6) C – SAP HANA system replication will synchronize the new SAP HANA instance with the existing on-premises environment, as described in the AWS SAP migration guide. When the systems are synchronized, the company can cut over to this system without the need for the downtime that the other options would cause.

7) D – AWS Server Migration Service (AWS SMS) will minimize downtime for this migration by supporting the migration of multiple VMs from on premises. This solution is also the only answer option that will not involve the deployment of agents to the source machines.

8) A, C – SAP Software Provisioning Manager and SAP Software Update Manager (SUM) Database Migration Option (DMO) with System Move support heterogeneous migrations in which the backend database environment changes. In this case, the migration is from an anyDB environment to an SAP HANA environment. Neither AWS Application Migration Service (CloudEndure Migration) nor VM Import/Export on AWS can be used for heterogeneous migrations. AWS Database Migration Service (AWS DMS) does not support SAP HANA as a target.

9) A – The ST06 transaction depends on data from the AWS Data Provider for SAP agent to make the AWS environmental data available. The SAP HANA monitoring agent provides different information to the monitoring environment. The Amazon CloudWatch agent does not feed the SAP monitoring environment, but the CloudWatch agent makes that information available to CloudWatch. The AWS DataSync agent has nothing to do with monitoring.

10) B, D – The rate of the backup of the SAP HANA database is affected by the available throughput to and from the /hana/data volume. Two ways to improve the backup performance are to increase the IOPS available from the underlying Amazon Elastic Block Store (Amazon EBS) volumes and to increase the number of parallel backup channels. The other options will not affect the performance meaningfully. Amazon S3 bucket size does not influence available throughput, and S3 Transfer Acceleration supports performance for global users rather than the single case of the SAP backup.