1) Your AWS infrastructure has an EC2 instance that has a non-root EBS volume. The volume stores company confidential information, and you were asked to ensure the data is protected.

How can you encrypt this confidential information on this EBS volume? (Choose 2)

a) Through AWS console, change the encryption parameter setting of the volume
b) You can not protect this information on the volume since it is not an encrypted volume
c) Create a new encrypted EBS volume and mount it to the same EC2 instance, move(copy) the data to the new volume
d) Take a snapshot of the EBS volume, and use the snapshot to create a new EBS volume and attach it to the EC2 instance
e) Create a snapshot of the EBS volume, copy the snapshot and choose encryption while copying, use the encrypted snapshot copy to create a new EBS volume and mount it to the EC2 instance

2) How can you share an encrypted snapshot with another AWS account?

a) Make the snapshot public so the other accounts will access it
b) Send your CMK keys to the other AWS accounts so they can access your snapshot
c) Ensure it is not encrypted with your default CMK keys, mark the snapshot as private, and then enter the other AWS accounts, and give them permissions to the encryption key used
d) You can't share your own encrypted snapshots, you have to convert it to un-encrypted first before sharing

3) You have an EBS volume attached to an instance in one AZ and you need to move it to a new availability zone in the same region, how can you achieve this?

a) Detach the volume from the EC2 instance and re-attach it to the new EC2 instance in the new AZ
b) You can not migrate EBS volumes between AZs, you need to store your data objects on S3 and create a new EBS volume in the new AZ, then restore data from S3
c) Create a snapshot of the volume, and use that snapshot to create a new volume in the new AZ
d) Using AWS console, drag and drop the EBS volume to the new EC2 instance in the other AZ

4) You want to use the EBS volume you have in region A, in another region B, how can you migrate the volume to another region ?

a) Create a snapshot of the volume and use it to create a new volume in the new region
b) Create a snapshot of the volume, copy the snapshot and specify the new region during the copy process, create a new volume from the copied snapshot in the new region
c) You can not move EBS volumes between regions
d) Create a snapshot of the EBS volume and make it public that all regions can use it

5) How can you ensure the EBS volume data is secured when creating a snapshot which will be saved on S3?

a) EBS snapshots stored on S3 are always encrypted
b) Use of encrypted volumes ensures that any snapshots created will be encrypted too
c) Request encryption of the snapshot while you create it
d) S3 has Server Side Encryption and it will take care of this

6) Your EBS volume snapshots are stored in S3, and you can access them through:

a) Browsing your account S3 bucket created for EBS snapshots
b) Through EC2 APIs
c) You can only view them when you are creating a new volume
d) You can not access them except through contacting AWS support

7) EBS volume snapshots are: (Choose 2)

a) Created and updated asynchronously
b) Created and updated synchronously
c) Are differential
d) Are incremental

8) EBS encryption is

a) Enabled by default on all EBS volumes
b) Supported on all EC2 instance types
c) Supported on all EBS volumes types
d) Supported only by EBS snapshots

9) An EC2 instance's root EBS volume

a) Is encrypted by default
b) Can not be encrypted, you need to use 3rd party software to encrypt it
c) Can be encrypted by AWS
d) Does not support encryption

10) You have an EBS volume that is the root volume of an EC2 instance, and you want to take a snapshot, how can you do this while ensuring consistency between EBS volume and snapshots?

a) You can take the snapshot while the EC2 instance is running
b) You must stop the instance, then take the snapshot
c) You can't take a snapshot of a EBS that is an EC2 instance boot volume
d) AWS will automatically take these snapshots during maintenance windows

11) In a client meeting, as the AWS SME, the client had questions about EBS snapshots characteristics, which of the below is true regarding EBS snapshots: (Choose 5)

a) They occur synchronously
b) Snapshots of Encrypted volumes are also encrypted
c) Volumes created from encrypted snapshots are also encrypted
d) Volumes created from encrypted snapshots are unencrypted
e) Encrypted snapshots are AZ specific
f) Encrypted snapshots are Region specific
g) They occur asynchronously
h) They are differential
i) They are incremental

12) How can you ensure that your EBS volumes created during an EC2 instance launch are still available when the respective EC2 instances are terminated?

a) Change the "DeleteOnTermination" attribute of the EBS volume to false while launching the instance
b) EBS volume automatically persists after the EC2 instance is terminated
c) You can not keep the EBS volume after the EC2 instance is terminated
d) Select the detach EBS volumes option when terminating the instance

13) Encryption of EBS volumes is supported on all EC2 instance families including free tier…

a) True
b) False

14) How can you achieve EBS volume data encryption at rest? (Choose 4)

a) Use native OS encryption drivers
b) Snapshot the data and encrypt it on S3 using SSE
c) Use SSL between your EC2 instance and EBS volume
d) Use encrypted EBS volumes
e) Use 3rd party encryption tools that can encrypt EBS volumes
f) Use encrypted file system on top of your EBS volume

15) Can you access an EBS volume during the process of creating a snapshot?

a) **Yes, you can**
b) No, you can't
c) Yes, you can if the EBS volume is configured to do so.
d) EBS volume snapshot can not be accesse

16) Can an EBS snapshot be used to create a smaller size EBS volume than the one used to create the snapshot?

a) **No**
b) Yes
c) Only if data is encrypted
d) You can't create an EBS volume from another volume's snapshot

17) An encrypted EBS volumes' actual data encryption process happens

a) On S3
b) On the EBS volume itself
c) **On the EC2 instance**
d) EBS volumes can not be encrypted

18) You are trying to explain to your junior AWS Sysadmin the difference between an EC2 instance – EBS backed, and EC2 instance – Instance-Store backed, what of the below would be helpful to explain this? (Choose 3)

a) **For an EBS-backed EC2 instance, the instance can be stopped, restarted, rebooted**
b) For Instance-store backed EC2 instance, the instance can be stopped and restarted
c) **For EBS volumes on EC2 instance, the data persists when the instance is stopped or rebooted**
d) For Instance-store volumes (non boot) on EC2 instance, the data persists when the instance is stopped
e) **For Instance-store backed EC2 instance, the instance can not be stopped**

19) You were tasked to launch an EC2 instance. You have a requirement that the data on the instance's non-root volumes must be encrypted at rest and persistent. How can you achieve this?

a) Launch an instance-store backed EC2 instance under free tier and use third party tools for encryption
b) You can not achieve both volume data persistence and encryption at rest at the same time
c) Launch an EBS-backed instance that supports EBS volume encryption
d) Launch an EBS backed volume under free tier, and encrypt the non-root volumes

20) Your manager requested you to take a snapshot of a non-root EBS volume that contains sensitive corporate data, the required is to take the most accurate (consistent) snapshot of that EBS volume without disrupting the instance operation, what is the best way to achieve this?

a) Take the snapshot while the EBS volume is attached and instance is running
b) Stop the instance and take the snapshot
c) You can't take a snapshot for a non-root EBS volume
d) Un-mount the EBS volume, take the snapshot, then re-mount it again

21) An application with a 150 GB relational database runs on an EC2 Instance. While the application is used infrequently with small peaks in the morning and evening, what is the MOST cost effective storage type among the options below? Please select :

a) Amazon EBS provisioned IOPS SSD
b) Amazon EBS Throughput Optimized HDD
c) Amazon EBS General Purpose SSD
d) Amazon EFS

22) An application currently stores all its data on Amazon EBS Volumes. All EBS volumes must be backed up durably across multiple Availability Zones.
What is the MOST resilient way to backup the volumes?

a) Take regular EBS snapshots.
b) Enable EBS volume encryption.
c) Create a script to copy data to an EC2 Instance store.
d) Mirror data across 2 EBS volumes.

23) A company has opted to store their cold data on EBS Volumes. Ensuring optimal cost, which of the following would be the ideal EBS Volume type to host this type of data?

a) General Purpose SSD
b) Provisioned IOPS SSD
c) Throughput Optimized HDD
d) Cold HDD