1. Know what instance types can be launched from which types of AMIs, and which instance types require an HVM AMI.

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/t2-instances.html>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization_types.html>

2. Understand bastion hosts, and which subnet one might live on. Here's a good, brief summary of bastion hosts taken from http://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/ - "Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a ‘jump’ server, allowing you to use SSH or RDP to login to other instances (within private subnets) deeper within your network. When properly configured through the use of security groups and Network ACLs, the bastion essentially acts as a bridge to your private instances via the Internet."

<http://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/>

3. Know the difference between Directory Service's AD Connector and Simple AD. "Use Simple AD if you need an inexpensive Active Directory–compatible service with the common directory features. AD Connector lets you simply connect your existing on-premises Active Directory to AWS."

<http://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html>

4. Know how to enable cross-account access with IAM. "To delegate permission to access a resource, you create an IAM role that has two policies attached. The permissions policy grants the user of the role the needed permissions to carry out the desired tasks on the resource. The trust policy specifies which trusted accounts are allowed to grant its users permissions to assume the role. The trust policy on the role in the trusting account is one-half of the permissions. The other half is a permissions policy attached to the user in the trusted account that allows that user to switch to, or assume the role."

<http://docs.aws.amazon.com/IAM/latest/UserGuide/idrolesterms-and-concepts.html>

5. Have a good understanding of how Route53 supports all of the different DNS record types, and when you would use certain ones over others.

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

<https://aws.amazon.com/route53/faqs/>

6. Know which services have native encryption at rest within the region, and which do not.

<http://jayendrapatil.com/aws-storage-gateway/>

7. Know which services allow you to retain full admin privileges of the underlying EC2 instances, or conversely know which ones definitely do not.

8. Know When Elastic IPs are free or not. "If you associate additional EIPs with that instance, you will be charged for each additional EIP associated with that instance per hour on a pro rata basis. Additional EIPs are only available in Amazon VPC. To ensure efficient use of Elastic IP addresses, we impose a small hourly charge when these IP addresses are not associated with a running instance or when they are associated with a stopped instance or unattached network interface."

<https://aws.amazon.com/ec2/pricing/>

9. Know what four high level categories of information Trusted Advisor supplies.

<https://aws.amazon.com/premiumsupport/trustedadvisor/>

10. Know how to troubleshoot a connection time out error when trying to connect to an instance in your VPC. "You need a security group rule that allows inbound traffic from your public IP address on the proper port, you need a route that sends all traffic destined outside the VPC (0.0.0.0/0) to the Internet gateway for the VPC, the network ACLs must allow inbound and outbound traffic from your public IP address on the proper port," etc.

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#TroubleshootingInstancesConnectionTimeout>

11. Be able to identify multiple possible use cases and eliminate non-use cases for SWF.

<https://aws.amazon.com/swf/faqs/>

12. Understand how you might set up consolidated billing and cross-account access such that individual divisions' resources are isolated from each other, but corporate IT can oversee all of it.

<http://jayendrapatil.com/aws-consolidated-billing/>

13. Know how you would go about making changes to an Auto Scaling group, fully understanding what you can and can't change. "You can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for your Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration. When you change the launch configuration for your Auto Scaling group, any new instances are launched using the new configuration parameters, but existing instances are not affected."

<http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>

14. Know which field you use to run a script upon launching your instance.

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html#user-data-shell-scripts>

15. Know how DynamoDB (durable, and you can pay for strong consistency), Elasticache (great for speed, not so durable), and S3 (eventual consistency results in lower latency) compare to each other in terms of durability and low latency.

<https://d0.awsstatic.com/whitepapers/AWS%20Storage%20Services%20Whitepaper-v9.pdf>

16. Know the difference between bucket policies, IAM policies, and ACLs for use with S3, and examples of when you would use each. "With IAM policies, companies can grant IAM users fine-grained control to their Amazon S3 bucket or objects while also retaining full control over everything the users do. With bucket policies, companies can define rules which apply broadly across all requests to their Amazon S3 resources, such as granting write privileges to a subset of Amazon S3 resources. Customers can also restrict access based on an aspect of the request, such as HTTP referrer and IP address. With ACLs, customers can grant specific permissions (i.e. READ, WRITE, FULL\_CONTROL) to specific users for an individual bucket or object."

<https://aws.amazon.com/s3/faqs/>

17. Know when and how you can encrypt snapshots. "Public snapshots of encrypted volumes are not supported, but you can share an encrypted snapshot with specific accounts."

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

18. Understand how you can use ELB cross-zone load balancing to ensure even distribution of traffic to EC2 instances in multiple AZs registered with a load balancer.

<http://jayendrapatil.com/tag/elastic-load-balancer/>