Go through the demo and speak on each area (high level):

- Regions and AZ
  - What is a Region?
    - An isolated geographically distributed number of AZs. Provides tolerance against localized catastrophes
  - What is an AZ?
    - Cluster of data centers within a few miles connected by high speed networks
- Networking (VPC and subnets)
  - What is a VPC? Virtual Private Cloud or VPC is a Software Defined Network (SDN)…
  - What is a Subnet? subset of a VPC, that maps to an AZ
- Compute
  - What is EC2? EC2 == VM == VMware
  - Different instance type use cases?
    - Must be determined based on testing, or previous knowledge
    - Briefly, Cx is for compute focused workload, Mx is balanced, Tx is for burstable compute workloads, Rx is for large memory requirements, etc.
  - Use cases for instance purchase options, i.e. Spot Instance, Reserved Instances, On-Demand
    - Spot Instances: Cost savings where large number of instances is involved, and workloads can be restarted. Can be combined with On-Demand to have minimum number of guaranteed instances.
  - What is “capacity reservation”?
    - Customer asking AWS to reserve or guarantee number of instances within an AZ
- Storage (EBS)
  - Provide certain guidances:
    - separate volume for application data to reduce blast radius (improve data recovery, avoid app causing OS issues or vice versa such as file system full)
    - Use appropriate EBS volume type
- Security (IAM)
  - What is IAM?
    - Identity and Access Management or IAM provides access for groups, users, or services to AWS services and capabilities.
  - What is an IAM Role?

        - The permissions allowed (or denied) as defined by an IAM JSON policy document for AWS service actions
    - What is an IAM Profile?
        - The IAM policy permissions defined for a trusted service
- Load Balancing
    - Gateway Load Balancer or GWLB fronts 3rd party appliances providing easier scale, and manage.
    - What is use case differences for ALB, NLB, GWLB?
        - GWLB for 3rd party appliances such as firewall (e.g. Palo Alto Networks)
        - ALB is for applications (http/https) offering various routing and feature capabilities
        - NLB is for low level communications (tcp/udp), offering better scale, and static IP address
    - ALB will provide its own IP address, so does not preserve client IP address by default. Must enable `X-Forwarded-For HTTP header` setting to capture client IP address, the backend has to process header
    - NLB with Target Group using Instance ID with preserve client IP. Target Group using IPv2 will need to enable "activate proxy protocol version 2 " setting on the NLB
    - Security Groups (SGs)
        - NLB does not have associated SG and backend resource SG must allow client IPs for preserve client IP, or NLB IPs when not preserving client IPs
        - ALB has associated SG and backend resource SG must allow ALB IPs

References

- AWS Global Infrastructure: <https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi&loc=1>
- Load Balancer comparison: <https://aws.amazon.com/elasticloadbalancing/features/?nc=sn&loc=2&dn=1>
- How do I capture client IP addresses in the web server logs behind an ELB?
- <https://aws.amazon.com/premiumsupport/knowledge-center/elb-capture-client-ip-addresses/>
- How do I attach a security group to my Elastic Load Balancer?

- <https://aws.amazon.com/premiumsupport/knowledge-center/security-group-load-balancer/>
- Instance purchasing options: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html>
- AWS Systems Manager Session Manager
- Cloudcraft, diagramming AWS infrastructure and other benefits