Draw.io Offline

<https://github.com/jgraph/drawio-desktop/releases/download/v14.4.3/draw.io-14.4.3-windows-installer.exe>  
  
[draw.io](http://draw.io/) offline for windows can be downloaded using above link.  
----------------------------------------------------------  
  
AWS QA:  
- Difference between public n private subnet  
- How private subnet routes traffic to internet.  
- What is vpc peering and after accepting the vpc peering request what aws does?  
- IAM roles: ec2 to s3bucket  
- Explain S3 website hosting and configuration  
- Difference between nacl and sg = 100% Question  
- Explain Stateful and Stateless with an example.  
- How to communicate/ssh to ec2 that are in different region as well as different Azs.  
- Difference between EBS and EC2, and how pricing works for both.  
- How to restrict access of s3 in folder level.  
- VPC - how vpc works, cidr block formula, peering, endpoint  
- IAM best practices  
- What is Application LB?  
- What is Lifecycle Management?  
- why application LB is deployed in two or three AZs.  
- what is ssh and how it works, troubleshoot Network Timeout error and public key authentication failed.  
- What is Assume Role in IAM.  
- How to connect to EC2 instance using a custom ssh key pair.  
- How to connect to an EC2 instance if the Private Key used to connect to that instance is lost.  
- What are the possible options when an error occurs "public key authentication failed"  
----------------------------------------------------------  
  
Access S3 Buckets using VPC Endpoint for S3 Service from Private Instance  
1. Create a new VPC, IGW and attach to VPC, Create two subnets in your VPC: one private and one public.  
2. Launch one instance, the bastion instance, in the public subnet. Launch another instance, the private instance, in the private subnet. You will use the bastion instance to reach the private instance. The private instance will be used to access Amazon S3.  
3. Configure security groups such that the bastion instance to be accessible over SSH 22 from your IP address only. The private instance should be accessible over SSH 22 from the bastion instance only.  
4. Create a route table for both the private and public subnet. Associate the route tables  
with their respective subnets. Associate IGW route for Public Route Table.  
5. Create an Amazon S3 bucket, Upload an object such as a text file into the bucket.  
6. Use Secure Shell (SSH) to access the bastion instance. Access S3 bucket from Public Instance and this should work as you are using the Internet to access the Amazon S3 endpoint. SSH to private instance,You should not be able to access the Amazon S3 file from the private instance.  
7. Create VPC Endpoint Gateway for S3 and Specify the private subnet in your VPC that will use the endpoint.Check the route table entries for the private subnet. It should now include a route to the endpoint for the Amazon S3 prefix list.  
8. Access the Amazon S3 object from your private instance.  
  
An Architecture Diagram using [draw.io](http://draw.io/) for above setup is to be created and shared here.  
----------------------------------------------------------  
  
S3 Bucket Policies Use Cases:  
Create a Bucket Policy on below scenarios:  
1)Everyone including anonymous, is allowed to List the bucket and perform GET Object operations on all objects in the bucket  
- Only users belonging the IAM Group BI-Team in the specified account are allowed full access.  
- Users inside this Group should only be able to Upload,Delete Objects from specified Organization's Public IP(This can be your IP)  
  
2)User should be able to access the S3 Objects only from a particular Domain:  
- Like only users accessing [www.flipkart.com](http://www.flipkart.com/), Objects should be accessible when access is tried from this domain only.  
  
3) Only Root user should be able to delete objects or buckets in S3.  
  
Acceptance Criteria:  
- Apply the policy and test all the positive and negative cases to be sure that Policy Works in all scenarios.