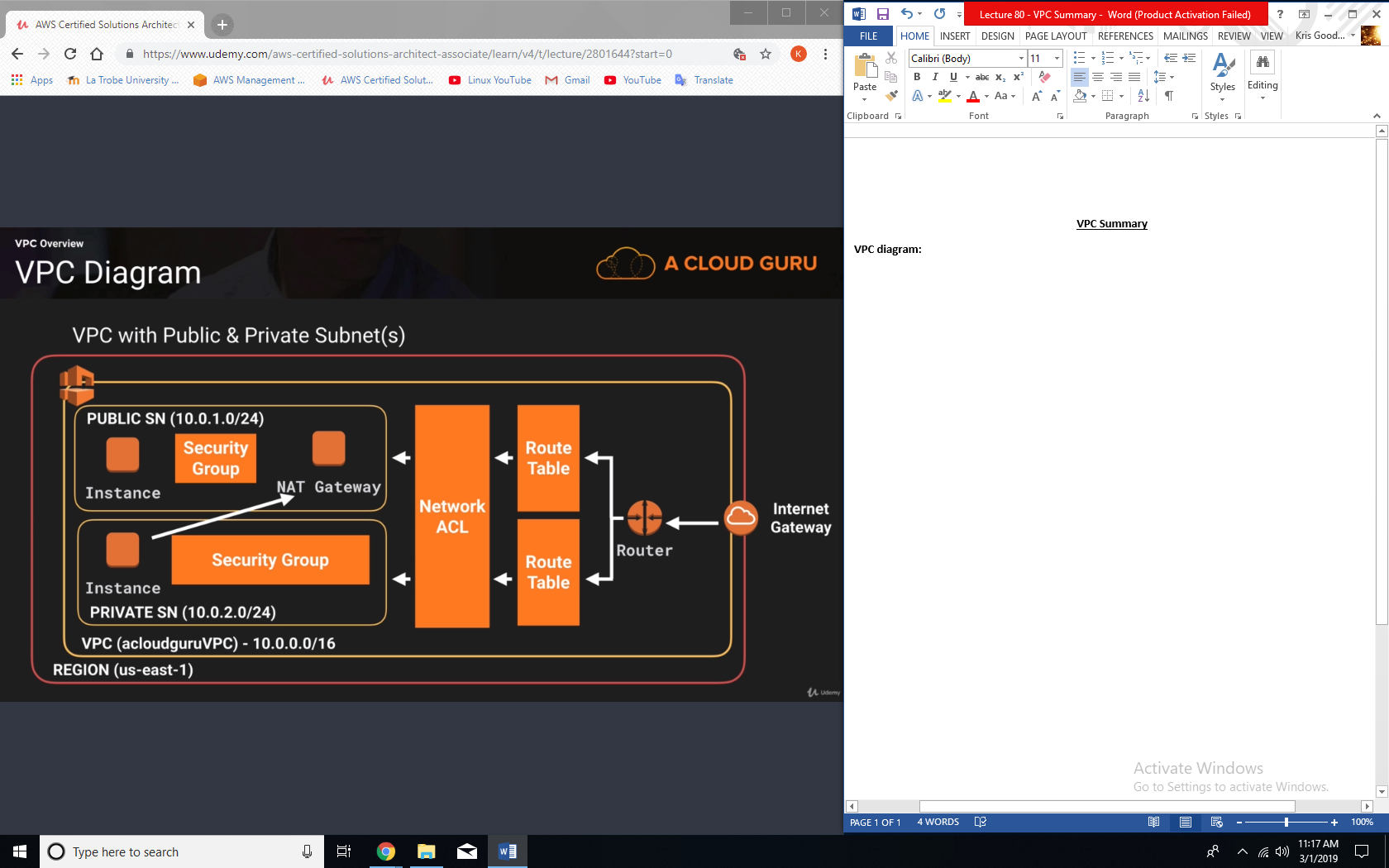
**VPC Summary**

**VPC diagram:**

**Exam Tips – NAT Instances:**

* When creating a NAT instance, Disable Source/Destination Check on the instance.
* NAT instances must be in a public subnet.
* There must be a route out of the private subnet to the NAT instance, in order for this to work.
* The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size.
* You can create high availability using Autoscaling groups, multiple subnets in different AZs, and a script to automate failover.
* They are always behind a security group

**Exam Tips – NAT Gateways:**

* Preferred by the enterprise
* Scale automatically up to 10Gbps
* No need to patch
* Not associated with security groups
* Automatically assigned a public IP address.
* Remember to update your route tables.
* No need to disable source/destination checks
* More secure than a NAT instance.

**Exam Tips – Network ACLs (Access Control Lists)**

* Your VPC automatically comes a default network ACL, and by default it allow all outbound and inbound traffic.
* You can create custom network ACLs. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
* Each subnet in your VPC must be associated with a network ACL. If you don’t explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
* You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the precious association is removed.
* Network ACLs contain a numbered list of rules that is evaluated in order, starting with the lowest numbered rule.
* Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic.
* Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).
* Block IP addresses using network ACLs, not security groups.

**Exam Tips – ALB’s:**

* You will need at least 2 public subnets in order to deploy an application load balancer.

**Exam Tips ­– VPC Flow Logs:**

* You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.
* You cannot tag a flow log.
* After you’ve created a flow log, you cannot change its configuration; for example, you can’t associate a different IAM ole with the flow log.
* Not all traffic is monitored;
  + Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
  + Traffic generated by a windows instance for Amazon Windows license activation.
  + Traffic to and from 169.254.169.254 for instance metadata.
  + DHCP traffic.
  + Traffic to the reserved IP address for the default VPC router.

**VPC Endpoints:**