**Security Token Service (STS)**

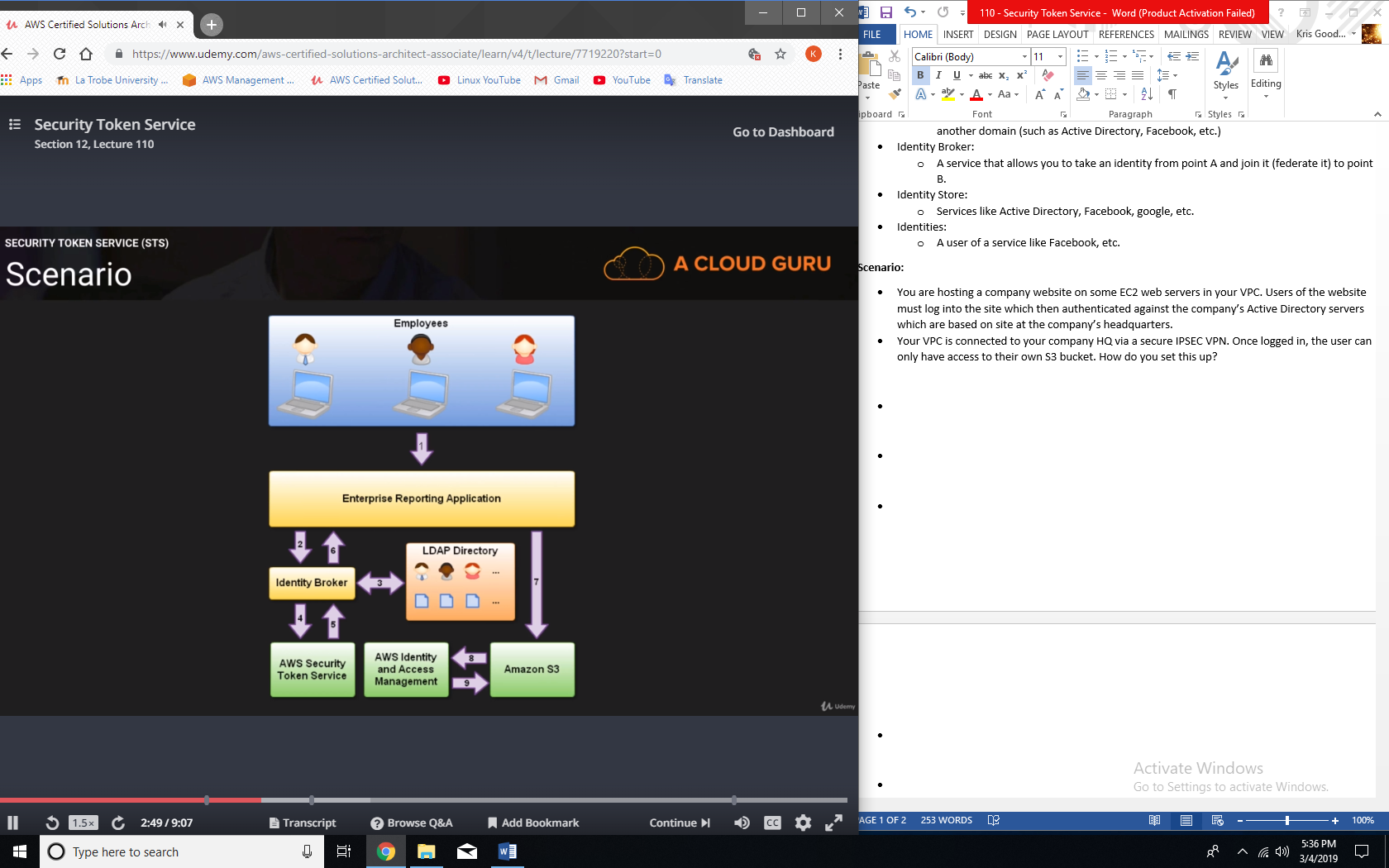
**What is Security Token Service?**

* Grants users limited and temporary access to AWS resources. Users can come from three sources;
  + Federation (typically Active Directory):
    - Uses Security Assertion Markup Language (SAML).
    - Grants temporary access based off the users Active Directory credentials. Does not need to be a user in IAM.
    - Single sign on allows users to log in to AWS console without assigning IAM credentials.
  + Federation with Mobile Apps:
    - Use Facebook/Amazon/Google or other OpenID providers to log in.
  + Cross Account Access:
    - Let’s users from one AWS account access resources in another.

**Understanding the Key Terms:**

* Federation:
  + Combining or joining a list of users in one domain (such as IAM) with a list of users in another domain (such as Active Directory, Facebook, etc.)
* Identity Broker:
  + A service that allows you to take an identity from point A and join it (federate it) to point B.
* Identity Store:
  + Services like Active Directory, Facebook, google, etc.
* Identities:
  + A user of a service like Facebook, etc.

**Scenario:**

* You are hosting a company website on some EC2 web servers in your VPC. Users of the website must log into the site which then authenticated against the company’s Active Directory servers which are based on site at the company’s headquarters.
* Your VPC is connected to your company HQ via a secure IPSEC VPN. Once logged in, the user can only have access to their own S3 bucket. How do you set this up?  
  

1. Employee enters their username and password.
2. The application calls an identity broker. The broker captures the username and password.
3. The identity broker uses the organization’s LDAP directory to validate the employee’s identity.
4. The identity broker calls the new GetFederationToken function using IAM credentials. The call must include an IAM policy and a duration (1 to 36 hours), along with a policy that specifies the permissions to be granted to the temporary security credentials.
5. The Security Token Service confirms that the policy of the IAM user making the call to GetFederationToken gives permission to create new tokens and then returns four values to the application: an access key, a secret access key, a token, and a duration (the token’s lifetime).
6. The identity broker returns the temporary security credentials to the reporting application.
7. The data storage application uses the temporary security credentials (including the token) to make requests to Amazon S3.
8. Amazon S3 uses IAM to verify that the credentials allow the requested operation on the given S3 bucket and key.
9. IAM provides S3 with the go-ahead to perform the requested operation.

**In the exam:**

1. Develop an identity broker to communicate with LDAP and AWS STS.
2. Identity broker always authenticates with LDAP first, then with AWS STS.
3. Application then gets temporary access to AWS resources.