Mini Project 17: Cloud Security Part 1

Mini-Project Overview Time Estimate: 2 hours

Context: Read through this brief about cloud security from Attack Solutions, Inc., a provider of cybersecurity service, before proceeding to

Project Submission Steps:

Operating in the cloud undoubtedly delivers significant advantages and security improvements for most organizations… [However,] when scoping a move to the cloud, businesses need to assess security in the context of this environment and evaluate Cloud Service Providers (CSPs) accordingly. Moving to the cloud means adopting a partnership approach to security that requires high levels of trust and transparency between all parties. These should be established at the start of the relationship. Partnering with a CSP allows you to access the security expertise of a business whose success depends on providing the most advanced levels of protection. Cloud providers have economies of scale. This allows your company to invest far more into talent and adoption of the latest innovative infrastructure protection and defense technology than any single organization could commit financially. Due diligence around your CSP is important when entrusting core systems to a third party. Therefore, it is critical to take the time to work with them to ensure that your cloud instance is secure and well maintained.

(Tombs, G. (2020, October 31). Why cloud security is more important than ever. Attack Solutions. http://attacksolutions.com/why-cloud-security-is-more-important-than-ever/.)

Project Submission Steps

One of the major security concerns of cloud-based information assets is access control.

Read the scenario below and perform the required task.

Scenario

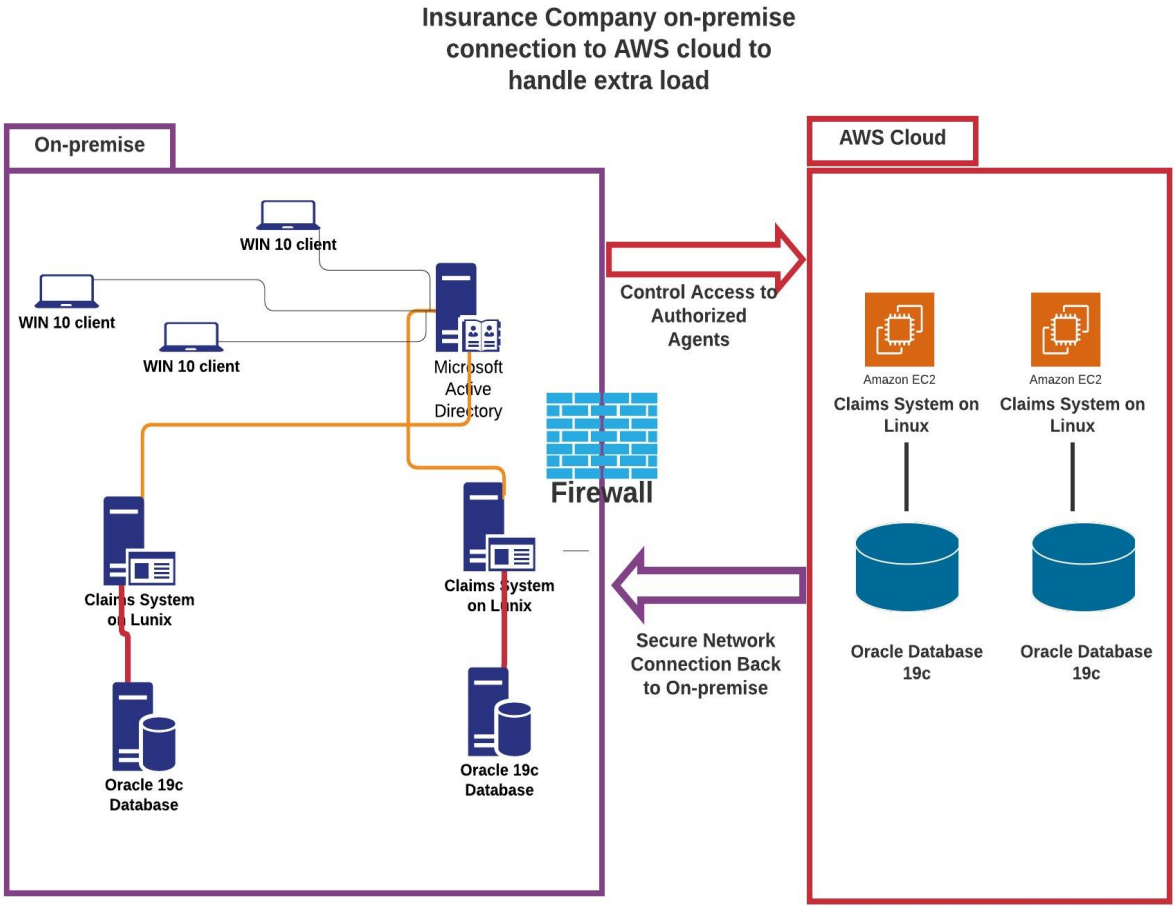
An insurance company has a claims application used to capture data about their policyholders and any property damage they suffer. A hurricane is projected to strike the Gulf Coast region of the US, likely causing massive property damage. This will create a huge spike in claims which will in turn create an enormous load on the corporate IT infrastructure. The company's decision is to use a public cloud provider to deliver virtual machines to handle the expected demand. The company must control access between the enterprise system and the virtual machines hosted by the cloud provider, limiting access to only authorized agents of the company. The company must securely transmit any data created by cloud-based instances of the application back inside the corporate firewall. The cloud provider must ensure that no traces of the application or its data remain whenever a virtual machine is shut down. The insurance company is based in the U.S. and only has domestic offices (there are no operations outside of the U.S.). The company

is using Microsoft Active Directory (AD) for authentication, with workstations running Windows 10. The claims systems are running Oracle Database 19c on Linux.

Assignment Paper (2-4 Pages)

You have been tasked with implementing an access control solution based upon users' roles. Write a 2–4 page paper on how you would go about doing this assuming that the cloud environment is either Microsoft Azure or Amazon Web Services (AWS) (pick only one).

In AWS, Role-based access control (RBAC) is also referred to as the authorization model in Identity and Access Management (IAM). You apply RBAC by creating different policies for different job functions. You then attach the policies to identities (IAM users, groups of users, or IAM roles). In IAM, Identity refers to the authentication of the users to the AWS account. Passwords are used to verify the identity. Access management refers to authorization which controls what a user can access once they become authenticated. In access control a user is assigned permissions to access specific AWS resources. Within IAM, there are also Access Control Mechanisms such as MFA and Key Management Service. In summary, IAM is used to manage authentication, authorization, and access control to a user to allow access to resources within an AWS account.



NOTE: Ensure that no traces of the application or its data remain whenever a virtual machine is shut down

In the diagram shown above, an Insurance company has decided to handle an extra load of claims using AWS cloud. The company is expecting numerous claims when a hurricane hits the area and destroys property. The AWS infrastructure can be set up for application load balancing where the traffic is sent outside the Virtual Private Cloud (VPC) using the IP address as the target. Security for authorized agents needs to be established in the AWS infrastructure shown in the diagram. IAM is important in securing the AWS infrastructure. If a user's identity and password is compromised by a hacker, setting IAM permissions will prevent the hacker from getting access to the whole AWS infrastructure. Without restrictive permissions, the hacker can also download Personal Identifiable Information (PII) from the claims system.

The insurance company consists of authorized agents such as Linux Administrators and Oracle DBAs that need permissions to perform certain job functions on the claims system which are hosted on EC2 and connected to the Oracle database. If you are dealing with a large number of users that are in groups in the on-premise Active Directory (AD) then integrating AD with AWS using SAML 2.0 is a viable option. This integration can be done to give the Linux Administrators and the Oracle DBAs the least privilege access to the claims systems in AWS which is good security policy. The Linux Administrators will have full access to the EC2 instance hosting the claims system and read only access to Oracle. The Oracle DBAs will have full access (i.e. insert, delete and update records) and read only access to the EC2 instance. The following steps are required to merge Active Directory with AWS:

- Both Active Directory Federation Services (ADFS) and Active Directory (AD) will be installed and configured on Windows Server. The user has a URL linked to the ADFS sign-on inside their domain. The sign-on page will authenticate the user against the Active Directory. ADFS provides a way for managing online identities and providing single sign-on functionality which is important from running applications on-premises to running applications in the cloud.
- The user will receive a Security Assertion Markup Language (SAML) assertion in the form of an authentication response from ADFS. SAML is an open standard that allows the client to use a set of credentials to log into many different websites.
- In the domain controller, add individual names to a group name starting with "AWS-". For example, for the linux administrators the name will be AWS-admin. The insurance company will already have groups with all the users on-premise. The groups for administrators and Oracle DBAs will be renamed to "AWS-admin" and "AWS-oracle". Starting the names with "AWS-" is required.
- To use ADFS, set up the Web server (IIS) which will be used to obtain a valid certificate of the ADFS server. You need the server certificate to configure ADFS.
- In AWS IAM, setup Identity Provider. Go to IAM services, Identity Providers, create a provider, choose provider type SAML , enter the provider name "adfsfederation", and upload the afds metadata that was downloaded from the Windows Server.
- Create two roles inside IAM. One role will be named ADFS-admin and the other ADFS-oracledba. After you select the create role button, select "SAML 2.0 federation" . Next, enter the SAML provider as "adfs" and allow programmatic and console access. The role name has to start with "ADFS- ".

The procedure to enable federation to AWS using Windows AD, ADFS, and SAML 2.0 as outlined above will be used to create the ADFS-admin and ADFS-oracledba roles. The ADFS-admin role will have the “AmazonEC2FullAccess" policy. A snapshot of the production claims EC2 instance can be created for a development claims EC2 instance used for the Linux Administrators. When the EC2 instance is created for development it can be configured to use the snapshot of the production EBS volume. The same procedure can be used to for the Oracle DBAs. In IAM, the ADFS-oracledba role can be created and assigned the “AmazonRDSFullAccess” policy. A test environment can be created for the Oracle DBAs by attaching a volume created from a snapshot of the production claims EC2 instance. In the article “How do I allow users to authenticate to an Amazon RDS MySql DB instance using their IAM credentials”, https://aws.amazon.com/premiumsupport/knowledge-center/users-connect-rds-iam/ , the author explains the EC2 and DB configurations required to authenticate. This type of authentication is more secure for a few reasons, one of them being that IAM database authentications use tokens and not database user credentials which can be easier to compromise. To set up IAM database authentication using IAM roles, the **following steps** can be taken:

- Create the user “oracledba” and configure it to use an AWS authentication token
- Add an IAM policy that maps the oracledba user to the ADFS-oracledba role
- Attach the ADFS-oracledba role to the EC2 instance that is used for Oracle development
- Download the SSL root certificate file of certificate bundle file
- Connect to the RDS DB instance using IAM role credentials and the authentication token.

Another option in AWS cloud to use on-premise Microsoft Active Directory is AWS Directory Service. AWS Directory Service makes it easy to set up and run directories in the AWS cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory. The **following steps** can be taken to accomplish this:

- Set up networking by creating a Virtual Private Cloud using the wizard. Next, configure the subnets and routing table.
- Create and IAM role which will be used for the EC2 instance hosting the claims system and using AWS Active Directory. After you select ‘create role’ , select ‘EC2 Role for Simple System Manager’. Then accept the default permissions for this role.
- Create the Microsoft Active Directory in the AWS Directory Service screen. In the Directory details screen you will configure the directory DNS, the NetBios name and the Admin password. This can be information from your on-premise Active Directory or your Microsoft Active Directory on the cloud. Next, select the VPC you configured. Lastly, configure DHCP.
- Create the EC2 instance that will host the claims instance. In the ‘configure Instance Details’ screen, fill in the ‘Domain join directory’ and the ‘IAM role’ with what was already configured in the previous steps.

The AWS Directory Services can be used for the other users of the claims systems that are not administrators of the testing (development) servers but are the insurance agents that need access to the production claims EC2 instances. Using a site-to-site VPN will allow the claims systems to access the intranet in the on-premise Active Directory. The insurance agents

(agents) can therefore get authenticated on the active directory and then connect to the claims system on AWS. To balance the traffic between AWS and on-premise claims systems, an application load balancer (ALB) can be used. The ALB which the AWS virtual private cloud hosts will redirect traffic to the on-premise claims systems using their IP addresses as targets. This can be done through a VPN connection.

As an extra note on security, when an instance is shutdown the root EBS volume will be detached but not deleted. The company policy wants to ensure that no traces of the application or its data remain whenever a virtual machine is shut down. To accomplish this the root EBS can be encrypted when the instance is created. It is important to note that the input/output operations per second (IOPS) performance is the same on the encrypted volumes as it is on the unencrypted volumes. When the instance is brought up a different virtual machine (VM) is used by AWS and the root EBS is attached. Since a different VM is brought up the public IP address will be different.