Access Control Solution: Implementing Access Control Solution Based Upon Users’ Roles AWS

Vincent Kiweesi

Cloud Security Part 1

April 13, 2023

The company decided to use Amazon Web Services, a public cloud provider, to offer virtual machines in an effort to meet the anticipated demand, in order to restrict access to just authorized organizations representatives, the company must manage access between the enterprise system and the virtual machines. Any data generated by cloud-based instances of the program must first be safely transferred back inside the company's firewall. Second, when a virtual machine is shut down, the cloud provider must make sure that no traces of the application or its data are left behind. The task here is the responsibility to put in place an access control system for user roles. Role-based services are part of Amazon Web Services (AWS). Role-Based Access Control (RBAC), commonly known as the authorization model in Identity and Access Management (IAM), is a component of this system. RBAC is implemented to develop unique policies for various job functions. The next step is to associate these policies with specific people, user groups, or IAM roles. IAM is an important part of the solution to make sure the right people have access to the right resources, especially when using several cloud instances(cite). The security of the AWS infrastructure depends on IAM. Setting permissions will stop an attacker from accessing the full infrastructure if they manage to steal a user's identity. The hacker can download Personal Identifiable Information (PII) from the insurance claims system if there are no restrictions in place. (Access Control - AWS Prescriptive Guidance, n.d)  
  
 The insurance company uses Windows 10 workstations running Microsoft Active Directory (AD) for authentication. The claims systems use Linux and Oracle Database 19c. AWS integration with AD utilizing Security Assertion Markup Language 2.0 (SAML) is a workable alternative if you have a lot of users who are part of groups in the on-premises Active Directory. SAML is a standardized technique for verifying that a user is who they claim to be to external apps and services. Because of this connection, Linux system administrators and the least privileged access to the claims systems can be granted to Oracle DBAs. For instance, the Linux administrators will have read-only access to Oracle and full access to the EC2 instance running the claims system. By carrying out the procedures necessary to combine Active Directory with AWS. On the Windows server, install and configure Active Directory Federation Services (ADFS) and Active Directory. The sign-on for ADFS within the user's domain will be accessible via a URL. The user will then be verified by Active Directory on the sign-on page. For both operating applications on-premises and running apps remotely, ADFS offers a method for maintaining online identities and offering single sign-on capability within a cloud. The user will then get a SAML assertion from ADFS in the form of an authentication response. Add the names of the Linux administrators to a group called "AWS-admin" in the domain controller. Make a group with the name "AWS-oracle" for the Amazon RDS for Oracle DBAs. To construct the roles ADFS-admin and ADFS-oracle, the process to enable federation to AWS using Windows AD, ADFS, and SAML 2.0 will be used. (Oracle Relational Database - Amazon RDS for Oracle – AWS, n.d)  
  
 Also make use of AWS Directory Service to establish an EC2 instance that will house the claims system as part of my access control solution. A development claims EC2 instance for the Linux administrators will be made using a snapshot of the production claims EC2 instance. Set up the development instance to use a snapshot of the production EBS volume when it is produced. A block storage solution built in the AWS cloud is called Elastic Block Store (EBS). EBS uses blocks, which function like hard drives, to store massive quantities of data. Also set up a testing environment for the Oracle DBAs. The additional users of the claims systems will make use of the AWS Directory Service. The other users of the claims systems who are not development server administrators will make use of the AWS Directory Service. Grant access to the production EC2 instance to the insurance agents. The other users of the claims systems who are not development server administrators will make use of the AWS Directory Service. Granted access to the production EC2 instance to the insurance agents. A site-to-site virtual private network (VPN) will be used by me. The claims systems will be able to access the intranet in the on-premises Active Directory thanks to this VPN. The insurance agents can connect to the AWS claims system after successfully authenticating themselves. Finally, when a virtual machine is shut down, the cloud provider must make sure that no traces of the application or its data are left behind. The root EBS will be encrypted when the instance is built in order to do this. The root EBS volume will be detached but not erased when an instance is shut down. (Amazon EC2, n.d.)

References

*Amazon EC2*. (n.d.). Amazon Web Services, Inc. <https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225->

4784bced9843&sc\_channel=ps&ef\_id=CjwKCAjw0N6hBhAUEiwAXab-

TSeQR1UnTY0reA72E19isGkJHwefFhq8hFKh5n1Pekg0phBH6Q9ffxoCpPAQAvD\_BwE:G:s&s\_kwcid=AL!4422!3!4677230

97970!e!!g!!amazon%20ec2!11198711716!118263955828

*Oracle Relational Database - Amazon RDS for Oracle - AWS*. (n.d.). Amazon Web Services, Inc.

https://aws.amazon.com/rds/oracle/

*Types of access control - AWS Prescriptive Guidance*. (n.d.). <https://docs.aws.amazon.com/prescriptive-guidance/latest/saas->

multitenant-api-access-authorization/access-control-types.html