**Cloud Security Part 1**

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.

• To determine which resources and actions need to be controlled based on user roles, first determine which resources and actions are needed to be managed. These could involve operations like adding, removing, or changing resources. They could also include access to particular cloud services, virtual machines, or storage accounts.  
  
• After that establish the necessary roles and permissions to regulate access to the mentioned resources and actions. A user with the "administrator" position, for instance, might have complete power over all resources, but a user with the "read-only" role might only be able to examine resources—not alter them.  
  
Role-based access control (RBAC) should be used depending on the chosen cloud environment, role-based access control (RBAC) tools offered in either Azure or AWS can be used to implement the appropriate roles and permissions. While using AWS Identity and Access Management (IAM) to create and manage roles and permissions, specific roles in AWS can be created by Azure RBAC.  
  
• Assign roles to users: Following the definition of roles and permissions, assign the proper roles to users in accordance with their requirements and duties. This could be carried out manually or automatically using software like AWS Organizations or Azure AD.  
  
• Review and monitor access: It's important to do this frequently to make sure that people are only given the permissions they require, and that access is being utilized properly. This can be achieved through recording, auditing, and routinely checking the responsibilities and permissions given to users.

• Synchronization of user identities and permissions between cloud and on-premises systems. If the access control solution needs to be integrated with on-premises systems, it may be necessary to use additional tools or technologies like Azure AD Connect or AWS Directory Service.  
  
• Security and compliance requirements. It's necessary to take into account any security and compliance standards or regulations that can be relevant to the access control solution. Utilizing particular tools or capabilities from Azure or AWS, as well as adding extra security measures like multi-factor authentication or encryption, may be required.  
  
• User experience and ease of use. To guarantee that the access control solution is accepted and utilized properly, it is crucial to make sure that it is simple for users to understand and use. In addition to developing the solution in a simple and user-friendly manner, this may entail offering comprehensive documentation and training.  
  
• Scalability and flexibility. It's necessary to make sure the access control system is flexible and scalable enough to adapt to changes in the number of users, roles, and resources as the business and its demands change over time. AWS Resource Groups or Azure Dynamic Groups may be used to manage permissions at scale, as well as designing the solution to be easily expandable and flexible.