Rolyon. (n.d.). *What is azure role-based access control (Azure rbac)?* Microsoft Learn. Retrieved December 20, 2022, from https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

Notes :

- in the scenario the insurance company has a claims application to capture data
- Hurricane will cause a lot of claims due to property damage which creates a spike
- They are using a public cloud provider
- Needs control access between the enterprise system and the virtual machines
- Wants to limit access to only authorized agents of the company

With the hurricane on its way it's projected to create a huge spike for insurance claims. This will create a lot of stress for the corporate IT infrastructure. In return we need to make an access control solution to help the IT infrastructure. The solution would include controlling access between the enterprise system and the virtual machines hosted by the cloud provider, limiting access to only authorized agents of the company. It needs to 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 cloud provider must ensure that no traces of the application or its data remain whenever a virtual machine is shut down. These are the main constraints the solution needs to cover and resolve. For the solution its best to use Microsoft Azure

Before implementing the solution you need to know how it all works. Azure is a RBAC which translates to role based access control, which allows you to manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. How it works is that you have to assign roles which is how permissions are enforced, a role assignment consists of 3 properties: security protocol, role definition and scope. A better way to understand the elements is to break them down. Security Principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources. According to “Rolyon. (n.d.). *What is azure role-based access control (Azure rbac)?* Microsoft Learn. Retrieved December 20, 2022, from https://learn.microsoft.com/en-us/azure/role-based-access-control/overview “
Another way to put security principal is that it's a symbol to identify who you are based on a user, group, service principal, ormanaged identity. The next property is Role definition is a collection of permissions. Another word for it is role. Which allows lets say the user to execute certain actions/ commands. The Last property is Scope. The article “ Rolyon. (n.d.). *What is azure role-based access control (Azure rbac)?* Microsoft Learn. Retrieved December 20, 2022, from https://learn.microsoft.com/en-us/azure/role-based-access-control/overview “ Describes Scope as being the set of resources that the access applies to. The article also states “ When you assign a role, you can further limit the actions allowed by defining a scope. This is helpful if you want to make someone a website contributor, but only for one resource group.” Also with Scope there are 4 structure levels from top to bottom: Management group, Subscription, Resource group and Resource. You as a consumer are able to set roles at any level of scope.

In the beginning it was discussed that there was a problem that needed to be solved, and then implement the solution. It's not just 1 problem, but it's many that needed to be solved but many. The first problem is how to create a system that will control access from the enterprise system through the virtual machines. According to " Rolyon. (n.d.). *What is azure role-based access control (Azure rbac)?* Microsoft Learn. Retrieved December 20, 2022, from https://learn.microsoft.com/en-us/azure/role-based-access-control/overview "
Microsoft describes to consumers how they can define roles by using Role definitions.they state that Azure has built in roles that consumers can use, such as the virtual machines contributor role allows a user to create and manage virtual machines. This is very useful so that attackers aren't able to immediately gain access and if the virtual machine seems suspicious Azure allows users to deny access by using their feature Deny assignment. Deny assignment is the opposite of role assignment but similar to it. "A deny assignment attaches a set of deny actions to a user, group, service principal, or managed identity at any particular scope." This is how Azure allows you to manage your virtual machines and control them using role definition.

Another problem the insurance agency had was being able to securely transmit data back inside the corporate firewall. With Azure data is stored globally so that customers can timely access data anywhere and anytime. If the company wasn't domesticated in the US they would be able to have someone from across the world working while other workers are sleeping on the other side of the world. According to " Rolyon. (n.d.). *What is azure role-based access control (Azure rbac)?* Microsoft Learn. Retrieved December 20, 2022, from https://learn.microsoft.com/en-us/azure/role-based-access-control/overview "
They state "When a role assignment or any other Azure RBAC data is deleted, the data is globally deleted. Principals that had access to a resource via Azure RBAC data will lose their access.`` This is great for the company which allows them to have their data be permanently deleted when they want to delete something which creates better security since it won't be lingering.