I had created some groups that applied different kinds of policies in each group for our employees. Each group stand for each department in our company, which mean only the employee in that department can have access to data and resources needed for the work of that department. Those groups are very important because they can grant permission to employee to access the needed data for their use. Create different groups with different policies also a very fast way to assign employee to different department because all we need is add employee to a group which that employee need to work with, so they will have the access to specific data they need and when they done their work or they have to move to different department we can just remove them from the group and they will lost all the permissions to access the data. It is definitely faster and more secure than assign policies to each employee. I also created some Customer Managed policies for each group instead of using AWS default policies because in that way we can fully control what role we want each employee to have. Other than Customer Managed we also have some other options, for example, Block Public Access, Access Control, Bucket Policy and CORS Configuration. However, since I have created specific policies for specific department or role, it is very easy to manage employees; for example, if an employee leave the company, I can just remove him/her from every group so that he/she will not have any access to any resource and then remove his/her user account; or if an employee move to a different department, I can remove him/her from the old group and assign him/her to the new group which is his/her new department, or if an employee becomes a Wiki Contributor I can add he/she to the Wiki Contributor group and then he/she will have all permission need to done his/her job. Finally, I can make sure that my policies adhere to the principal of least privilege because I only assign specific role to different group so the user in that group will only have necessary permission to do their job. For example, I create two groups for each department one can only read resources and the other one can read and modify resources. In that way I can assign specific employee to who should have permission to read the data only and I can assign higher level employee to read write group so they can do more modification if needed.