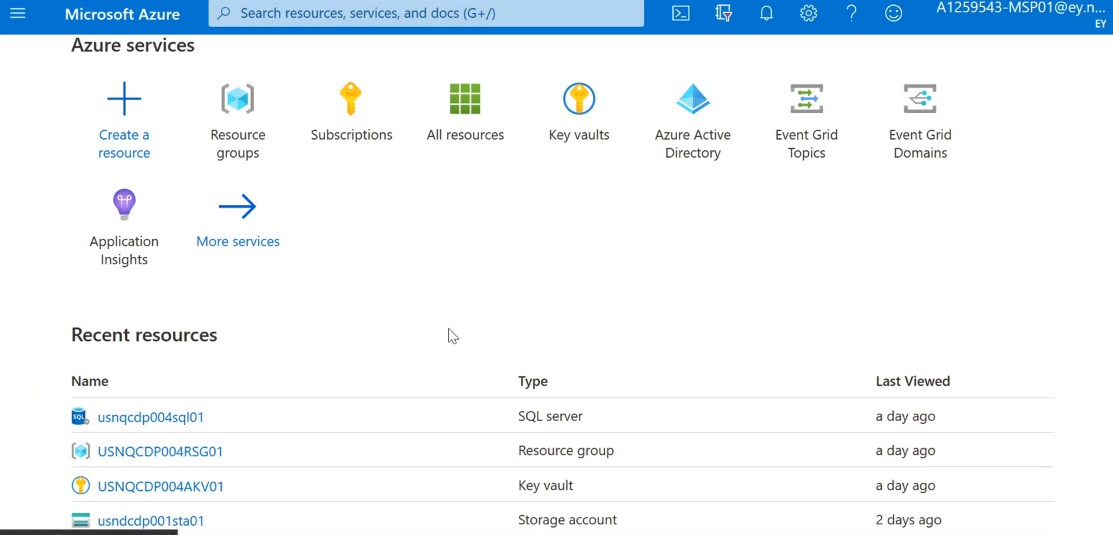
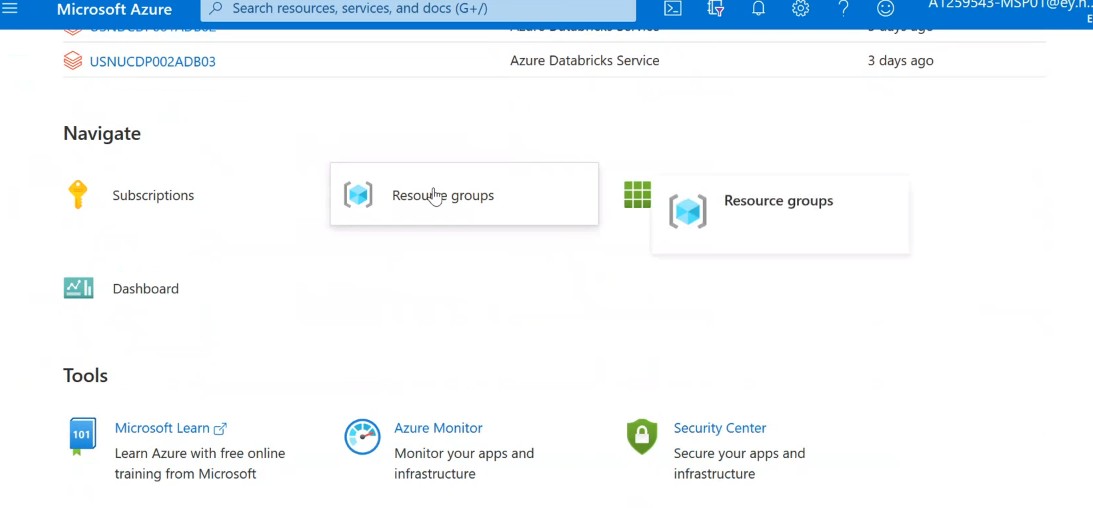
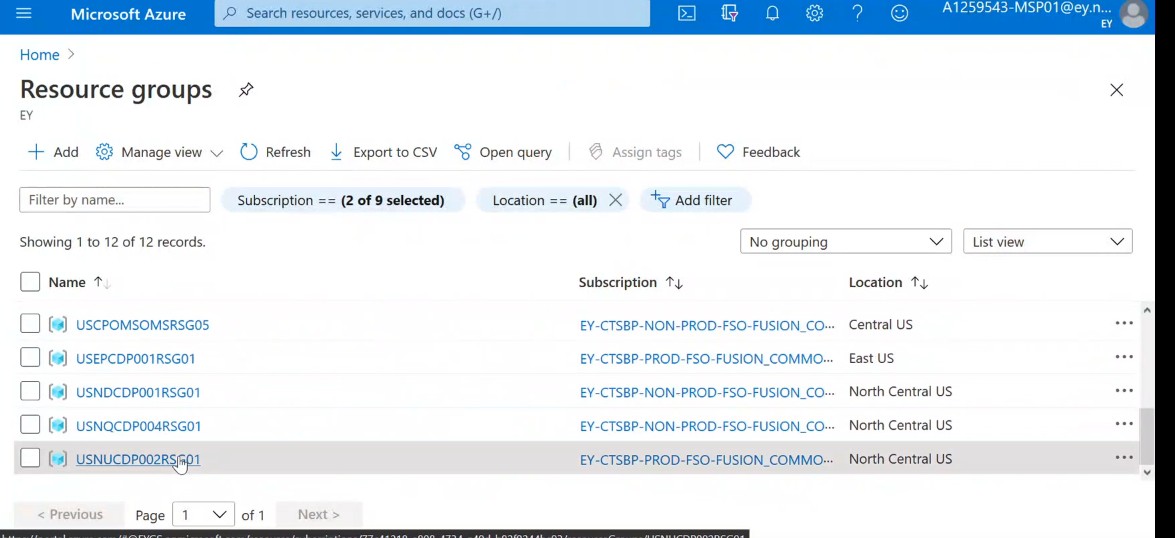
Please find the Azure Homepage



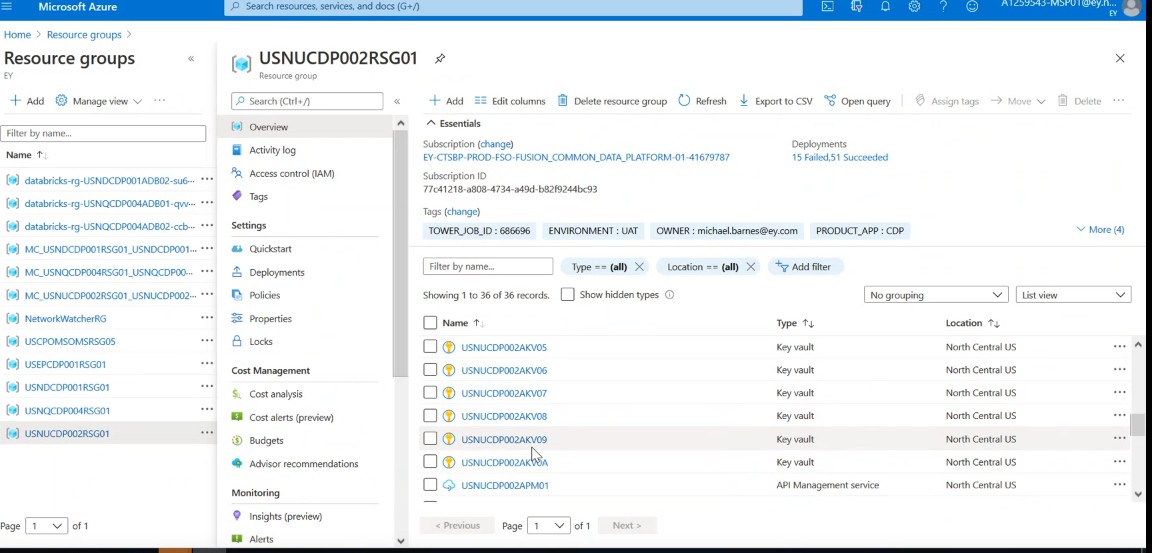
And the next step is to got the resource group



Under the Resource group click on the below



After clicking on the respected resource groups USNUCDP002RSG01. We can find the list of keyvaults



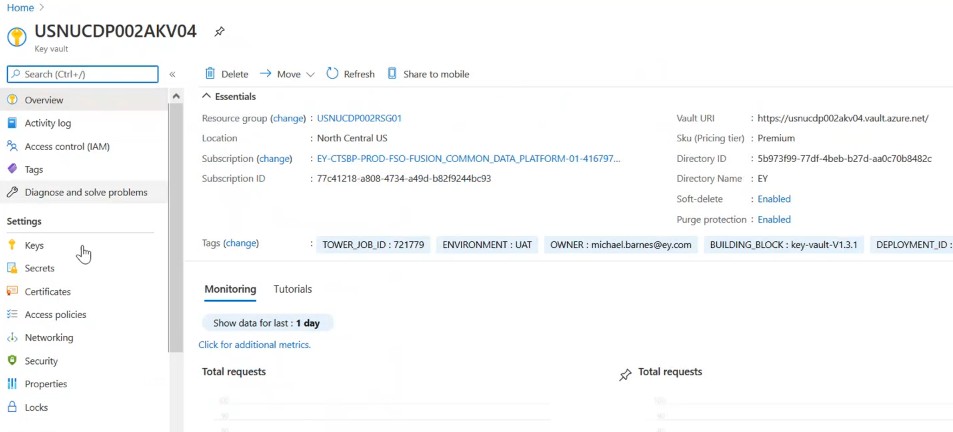
Among the Keyvaults . the below keyvault **USNUCDP002AKV01** is the area where our passwords and everything are stored for daily execution



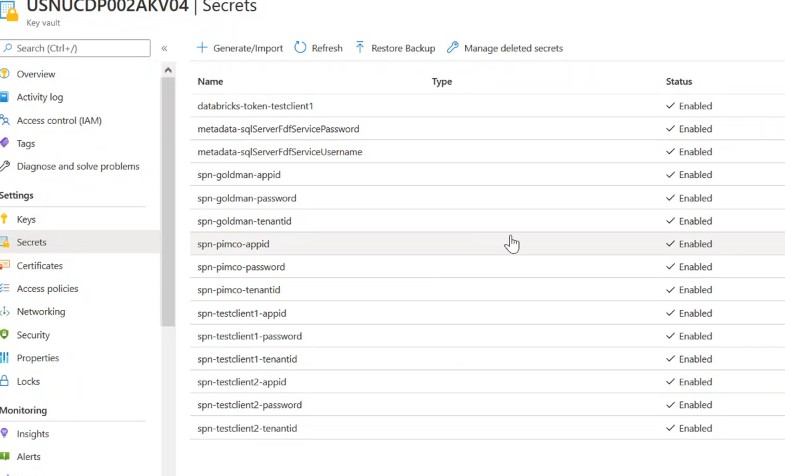
Then we have **USNUCDP002AKV04** where all our admin passwords are stored



When u click on the above keyvault the below window appear



When u click on Secrets on the left tab



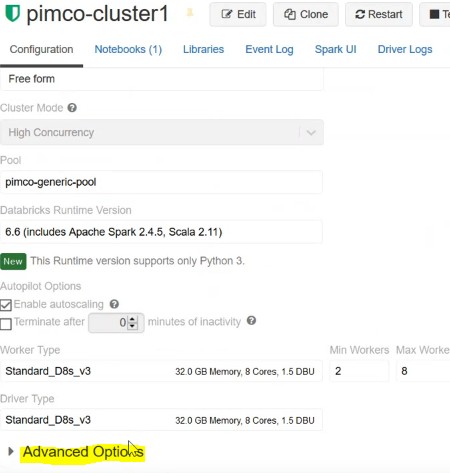
When u click on the below vault **USNUCDP002AKV05 ,** We can the details of our Event hub

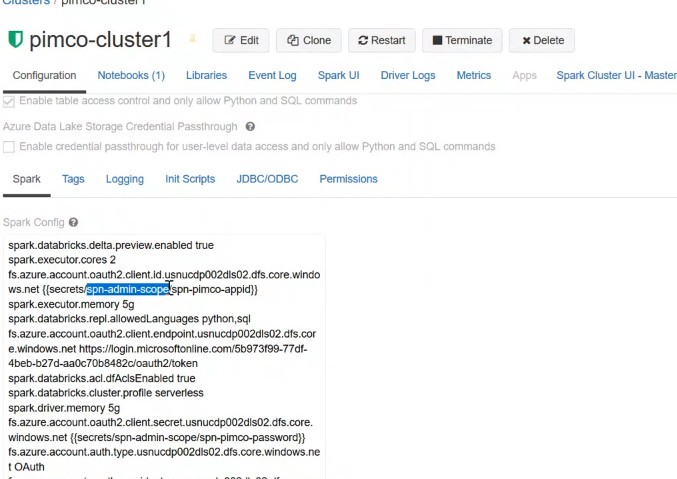


We need to be concern on the above three vaults only as we are using them on the Dev,QA and UAT Environment.

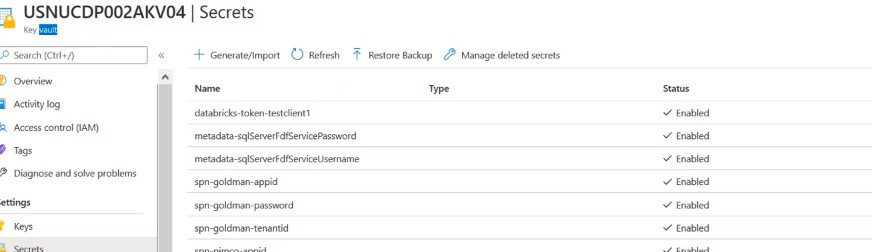
In Databricks there is a way to link your azure databricks environment with the key vault that can be achieved only by an ADMIN .As an admin when a scope is created(genericscope) we can access all the keys in the keyboard. We are using this generic code in scala for retrieving the passwords

There is another scope which you commonly find in all the cluster settings if you go to the advanced options you can find the below

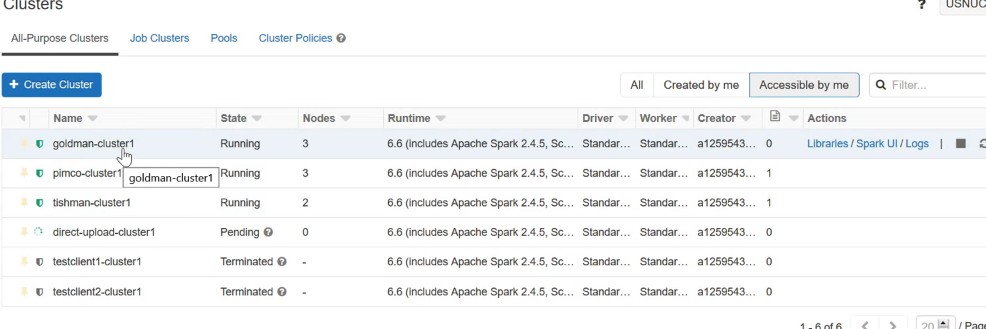




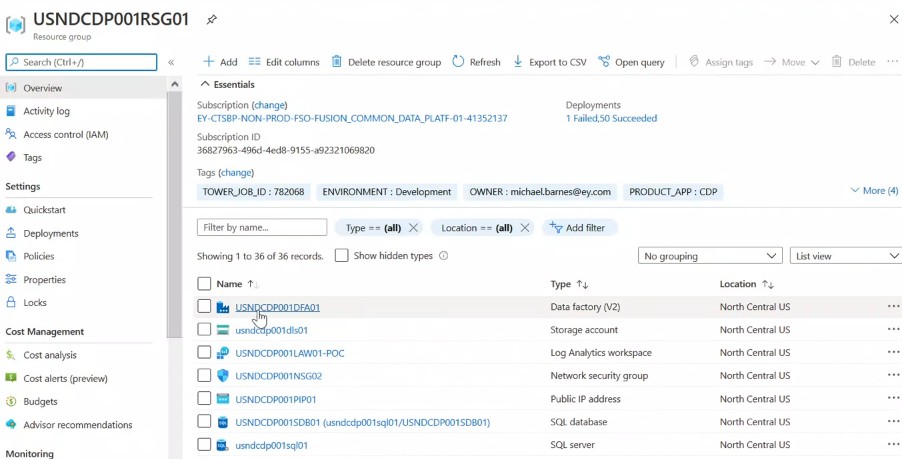
It is pointing to the **USNUCDP002AKV04**



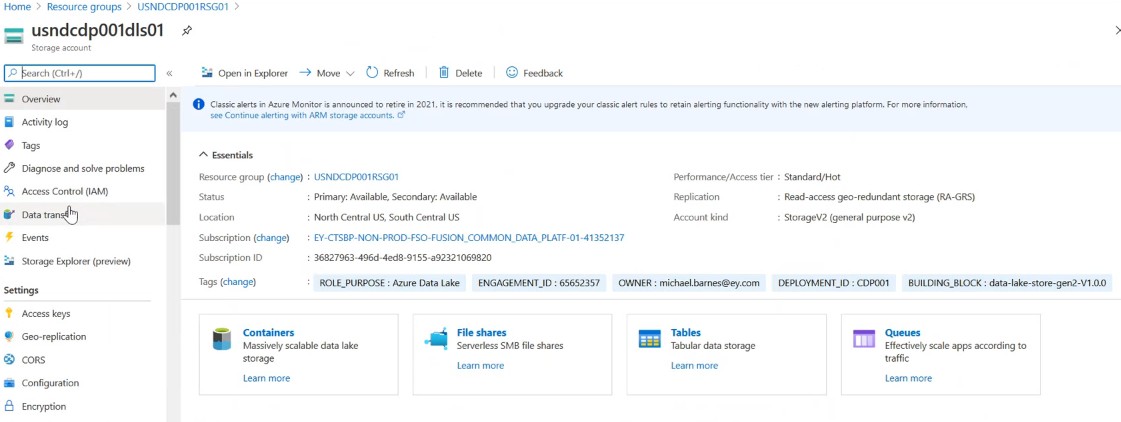
All are client level settings .Our goal is to have data segregation whenever we do any any setup for a particular client . We have golden Cluster,PIMCO Cluster,Tishman Clusterin . My goal is when some person has the ability to come to attachment cluster, they should only see Dishman.



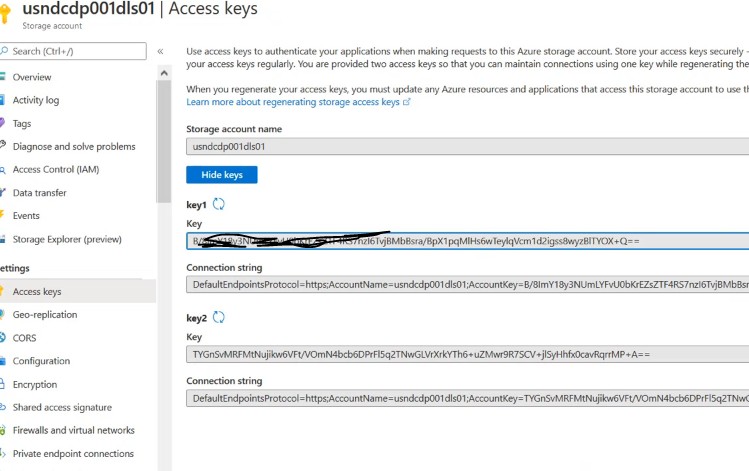
We store our data in ADL Storage account



When I click on usndcdp001dls01

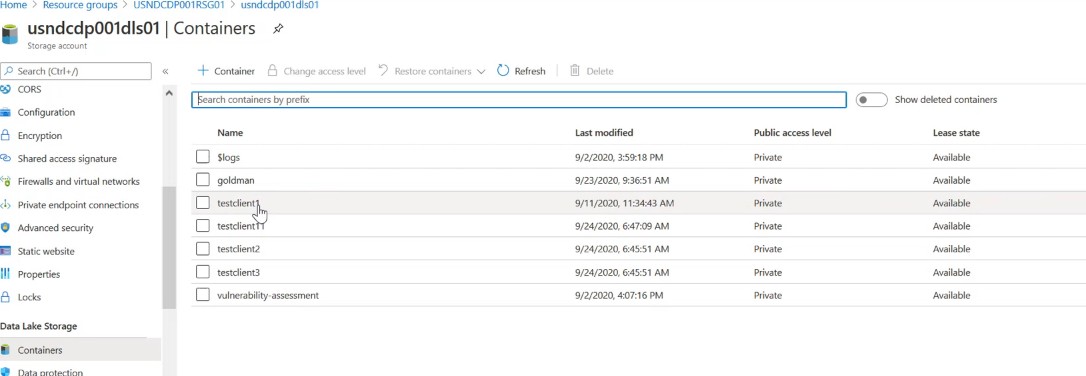


When I click on the acesskeys on the left

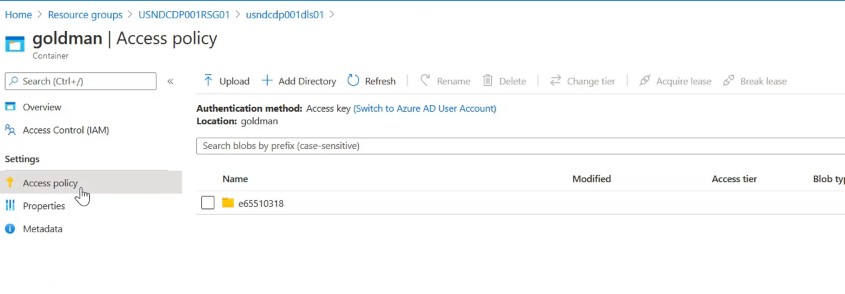


In the Dev environment it has been added .Any one who comes to this cluster by default the access will be provided to all the containers in this particular ADLS resource . So we need to avoid this

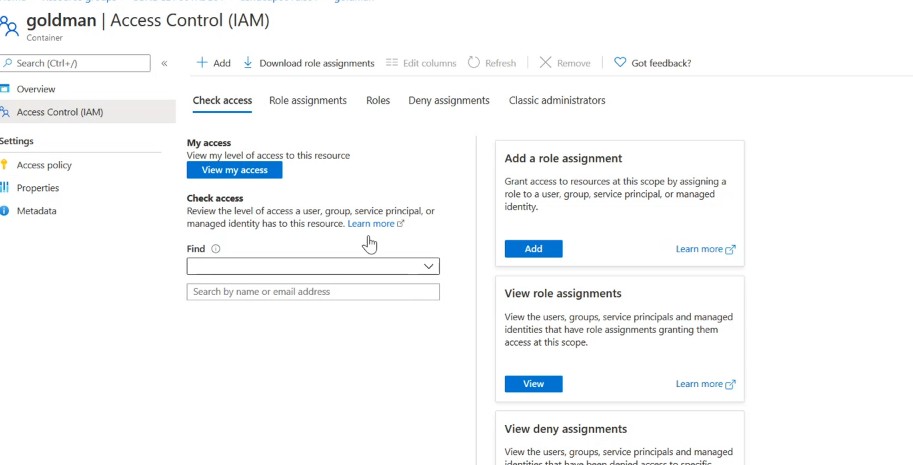
Lets come to the container



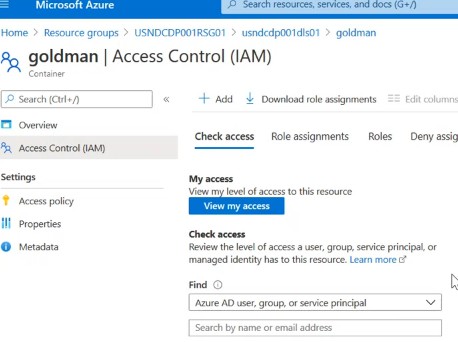
Click on Goldmaan



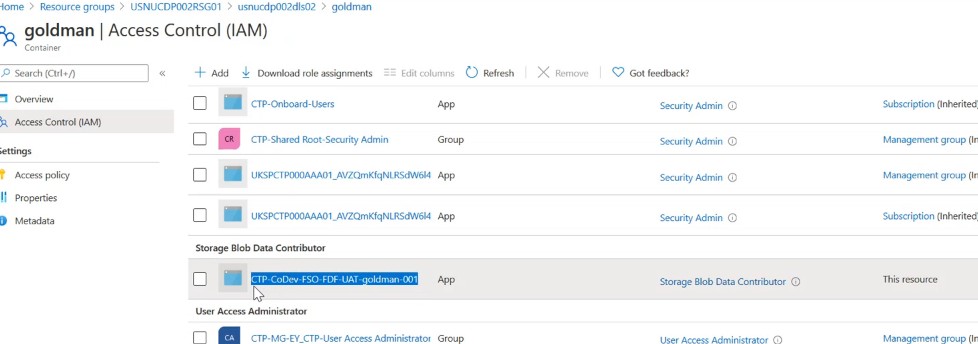
We have access control on the left



Here Service principal is being created which is used to communicate between azure resources, here Goldman specific service account has been created and I am going to provide access to the corresponding container alone .In role assignment

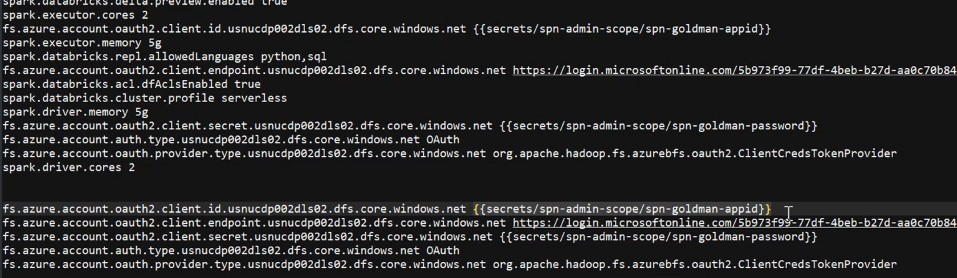


In the role assigments

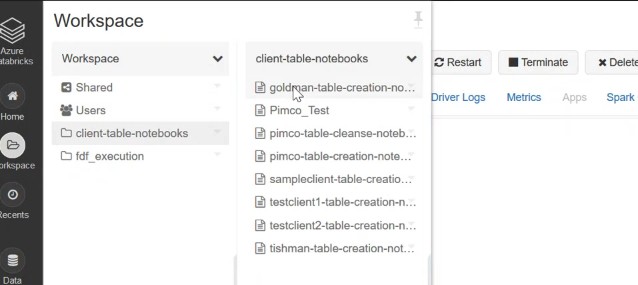


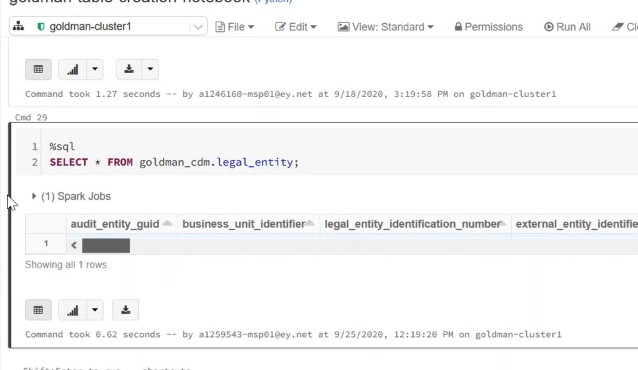
Now this service principal have access to this container and the process is same for all the container

In the logs they refer the service level principal for goldman alone for processing

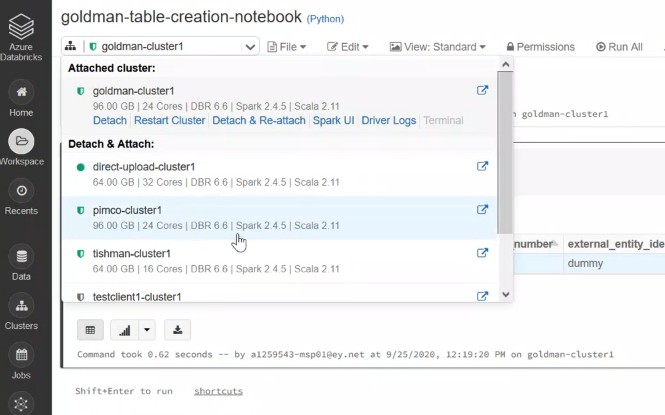


If the user tries to access any tables in the Goldman container

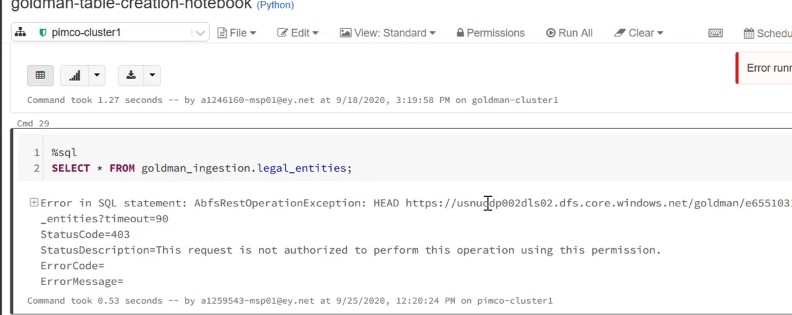


When u click on the Goldman table creation u can find the status of the job with out any error as mentioned below

When the cluster gets changed



It will give an error like



Which shows that PIMCO service principal didnt have access to view Goldman container . We have container level data segregation along with API Security and even going to have role based and attribute based security and immune which is the combine level operation which enable the access for different groups who are going to access the data. It seems whenever a setup of this kind needs to be done for a new client a request needs to be raised and submitted to the Client technology team and they can create a new service principal for that particular client .The whole process takes nearly 30 minutes .So once it is done follow the same process as mentioned above like store it in the key vault and create a cluster and for the service principal assign the corresponding container and then u are succeded in creating the cluster with the requested privileges

So when a user come here without admin access and then try to create scope it is not possible as it can be done only via admin access