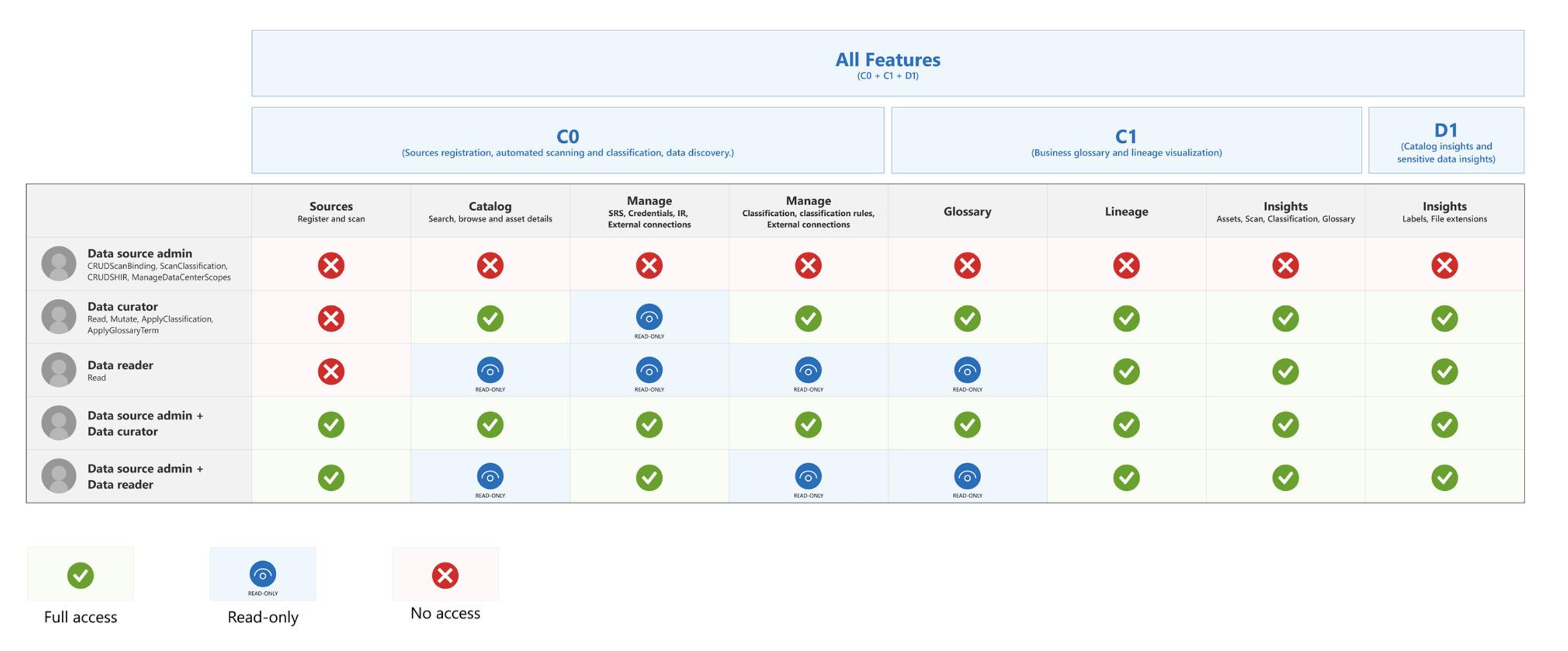
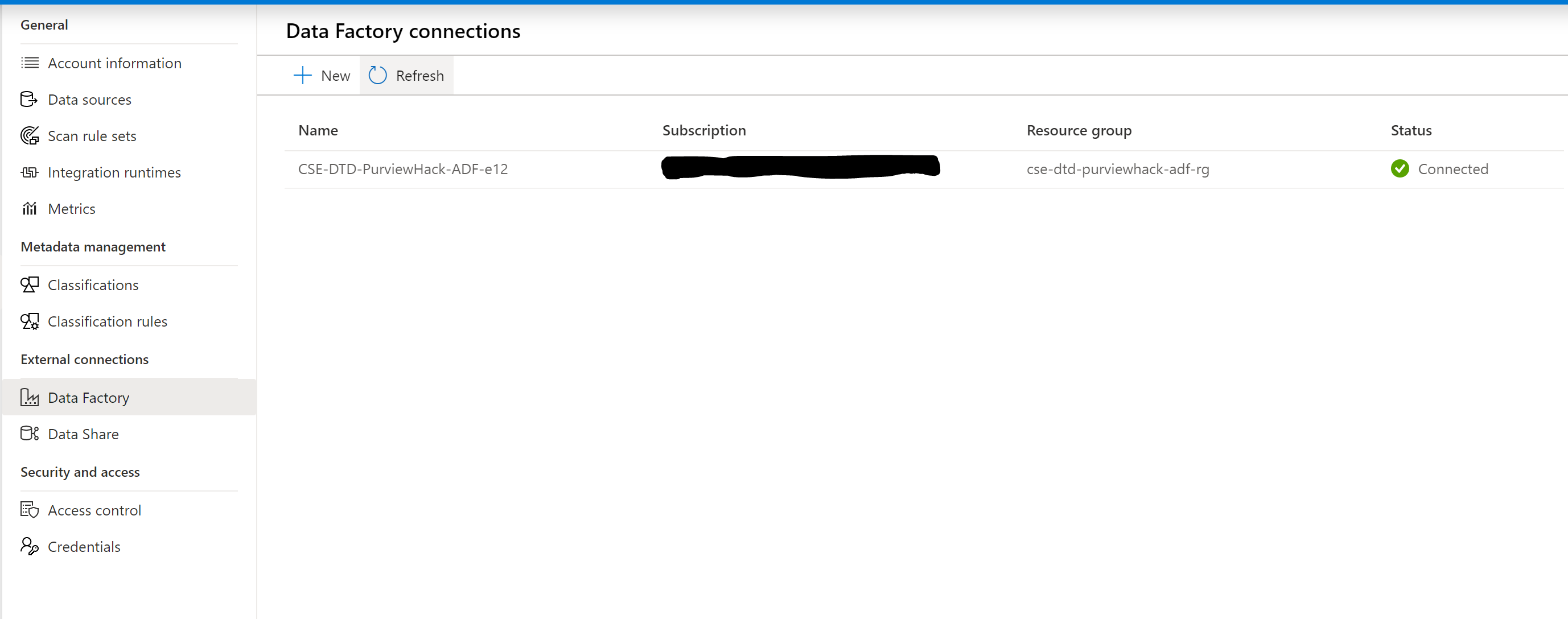
**How does the ADF scanning work on Purview?**

Purview can not only scan different data source but also extract lineage by scanning the Azure Data Factory. What has been raised as a question many a times is whether the login that added ADF used by purview for authenticating and populating the lineage? The answer is an emphatic No! Before we go any further it is worth reviewing the Purview roles:



**How is this done?**

Once ADF has been registered successfully, the following will appear on the ADF registration screen.



When a Purview user registers an ADF to which he/she has access to, the following happens in the backend:

1. The ADF MSI gets added to Purview as purview data curator.



1. The ADF needs to be executed again.
2. Scan/re-scan the data source-destination-which is the target in the ADF.

**Conclusion**

Purview does not use the user credentials that registered the ADF to extract lineage. Instead, the ADF’s MSI is provided Purview Data Curator permission. Finally, a push operation from ADF to Purview takes place to populate lineage.