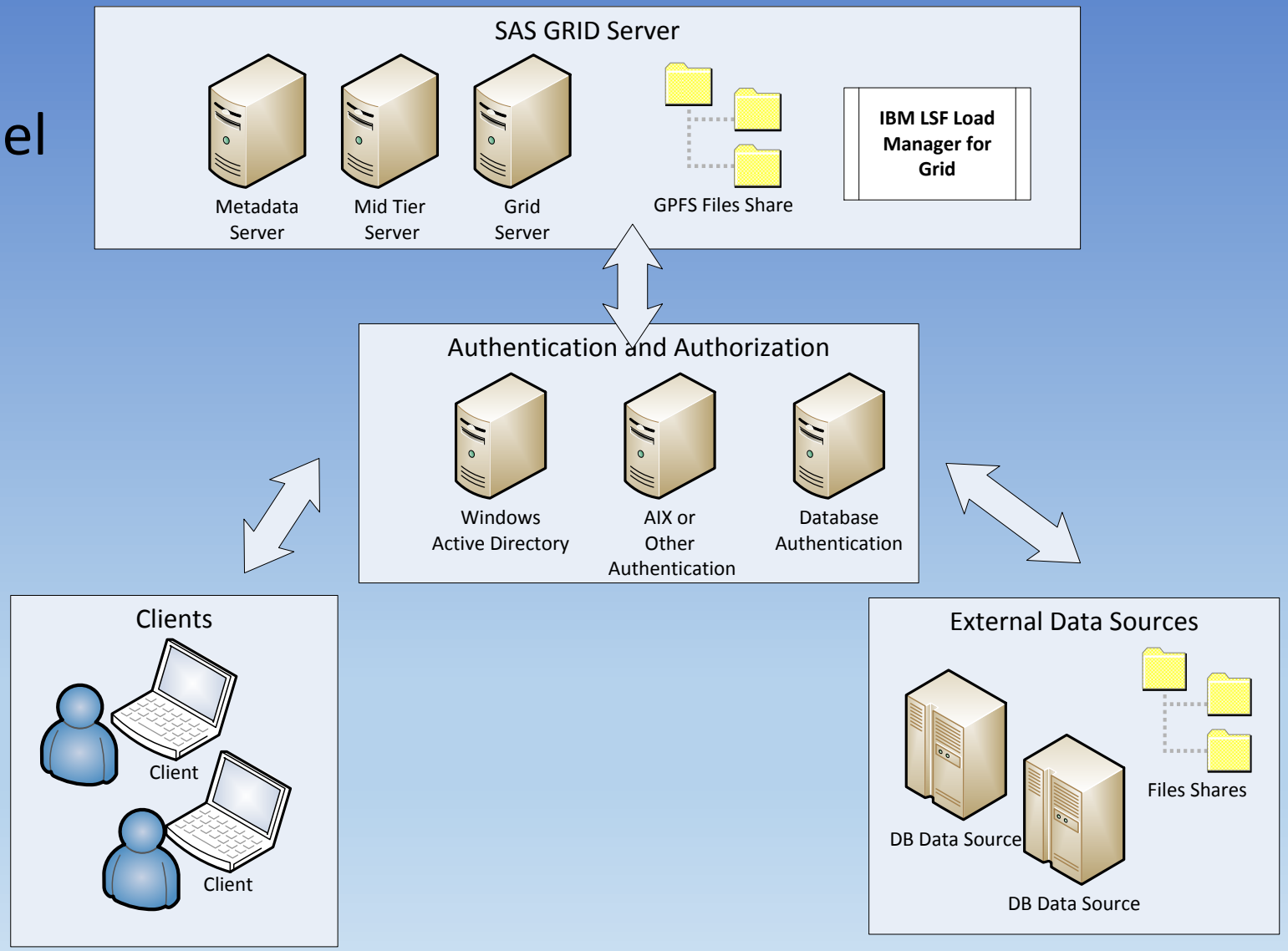
SAS Security

Windows Grid Environment SAS 9.4

Gary Hochstenbach, SAS Sys Admin ATB

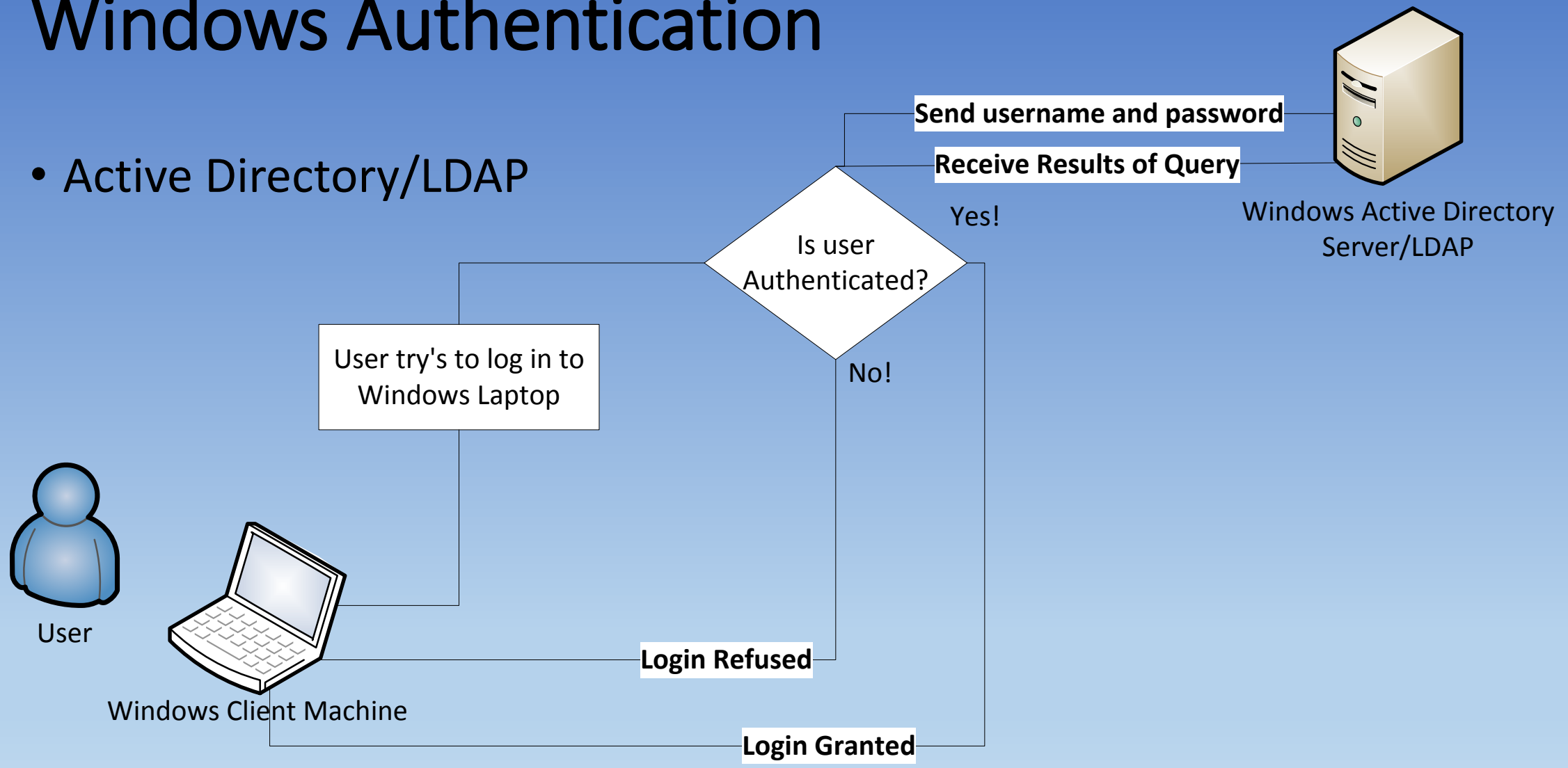
Security Architecture

- Complete Layered Model



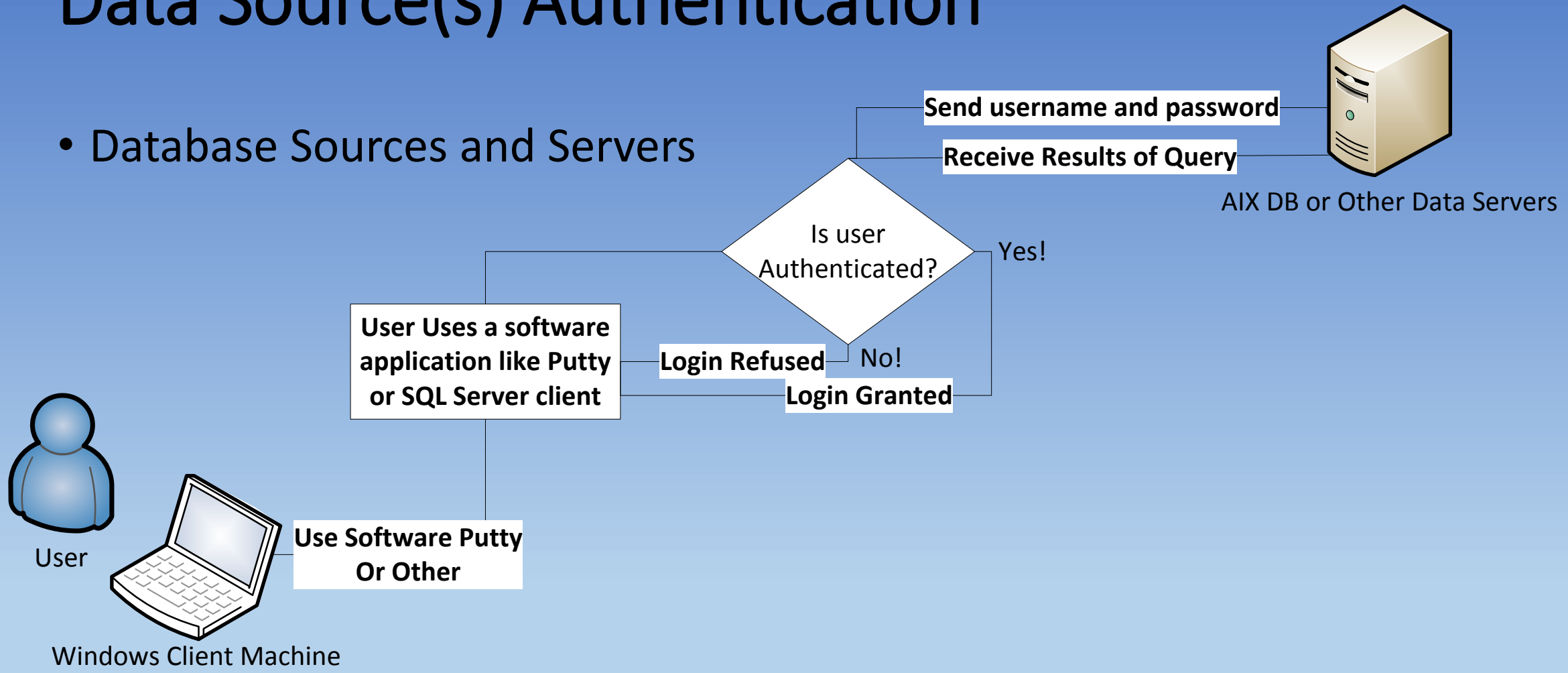
Windows Authentication

- Active Directory/LDAP

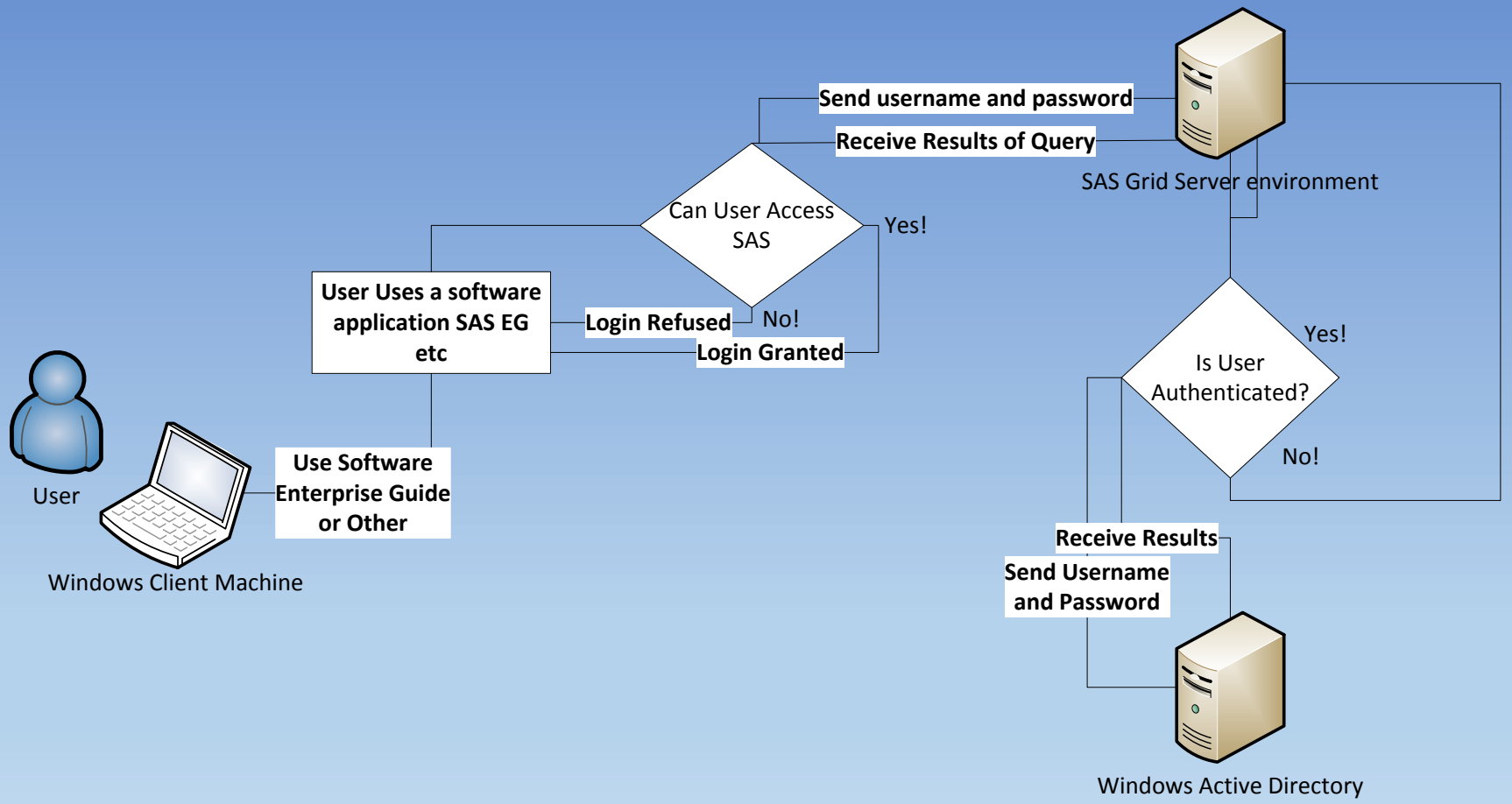


Data Source(s) Authentication

- Database Sources and Servers

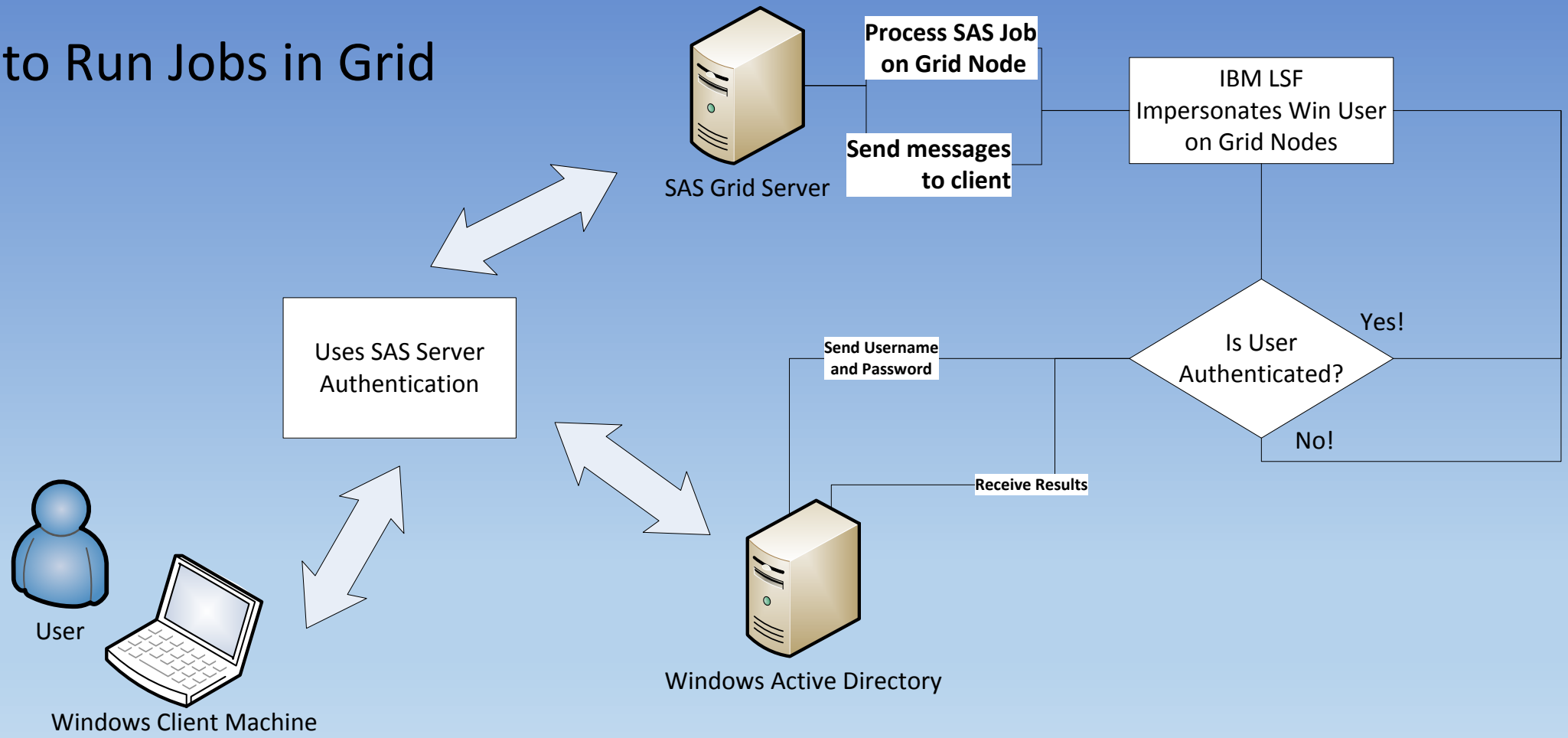


SAS Grid Server Authentication



SAS/IBM LSF Authentication

- Needed to Run Jobs in Grid

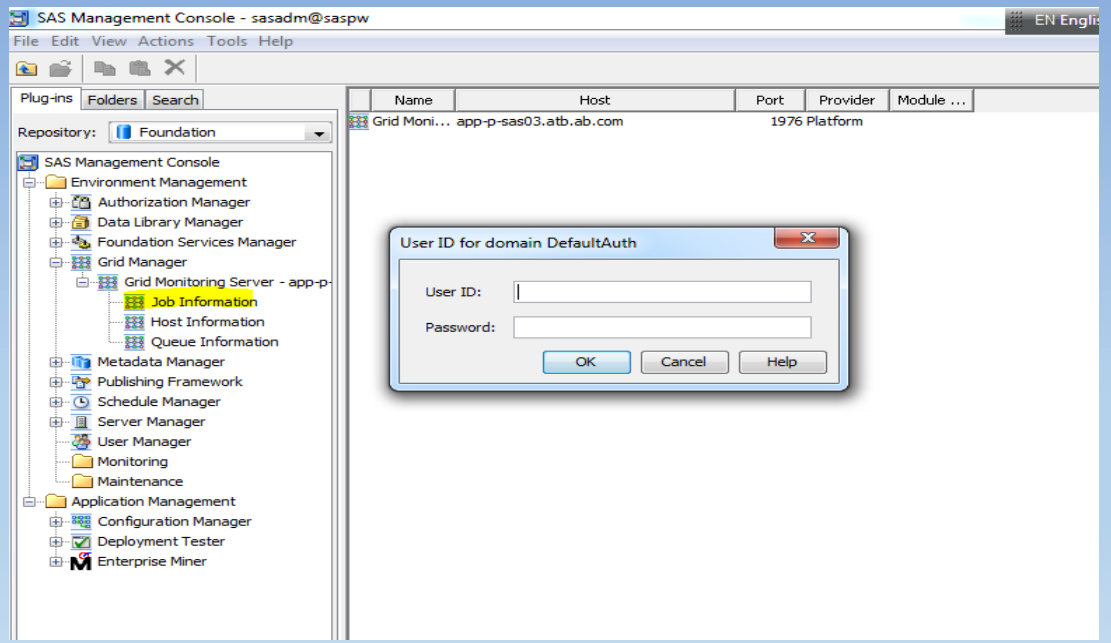


Maintain Windows Authentication

- Standard Password Management on Client Work Station
- Passwords do Expire after a predetermined amount of time.
- Need to keep IBM LSF Passwords in sync with Active Directory (Windows) password changes.

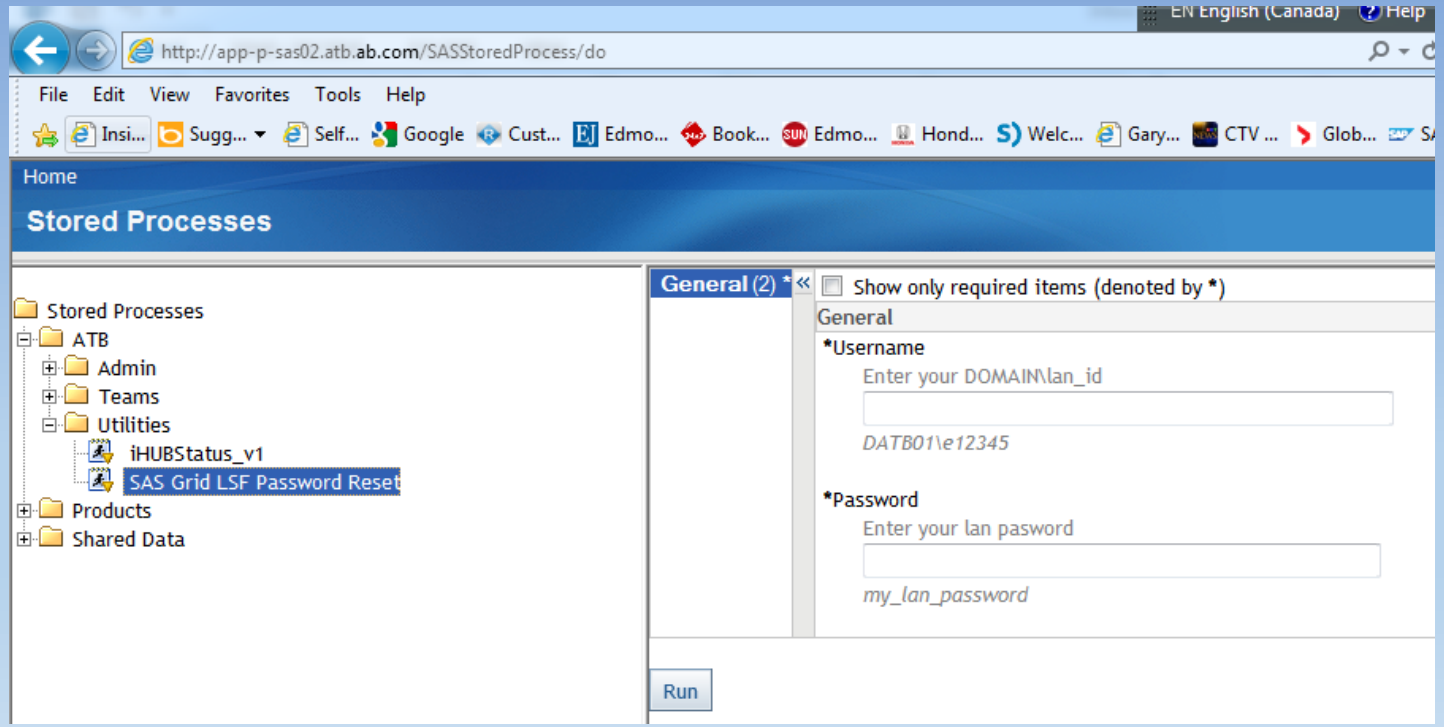
Maintain IBM/LSF Windows Authentication

- User must after each password change in Windows go to the SAS Management Console and select Grid Manager and Log in. This sets LSF Password which is the same as their windows password.



Maintain IBM/LSF Customization for ATB

- At ATB we have a custom Stored Process that is web based to allow users to set their password via web interface which negates the use of SAS Management Console for LSF Password sets.

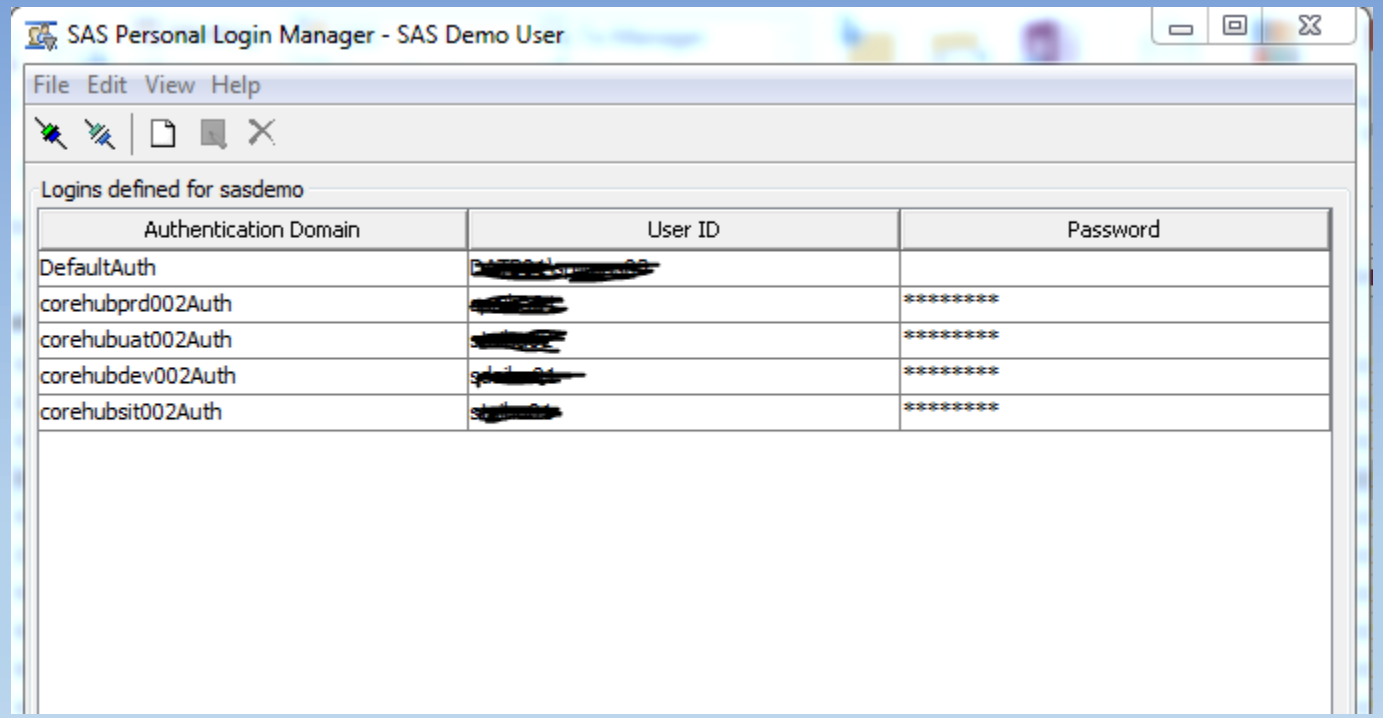


Maintain Data Source Authentication(s)

- Each Data Source will have their own process for maintaining its authentication.
- In Some cases Data Sources might use Active Directory for authentication which would limit the maintenance to Windows and LSF.
- In Other cases a user might have to maintain several usernames and passwords to different systems depending on technologies, OS Type and network architecture.
- Up Next we will show you how SAS maintains pass-through authentication for your data sources with SAS Personal Login Manager

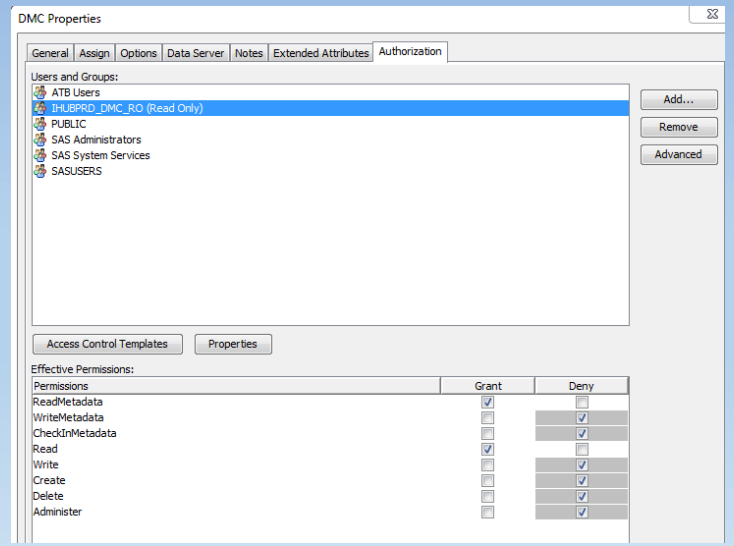
SAS Personal Login Manager

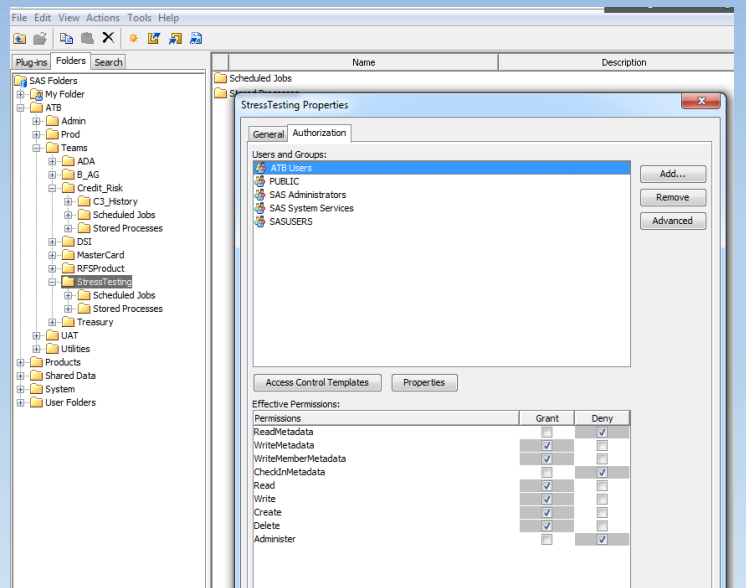
- In SAS all Data Source accounts are linked to your Windows Account as shown below:



SAS Metadata Security

- SAS Metadata security is used within SAS on all objects
- Metadata Security is applied at databases, schemas, fields and libraries as it is applied to data.
- Metadata Security is also applied to the shared folders that users are encouraged to use for storing their data sets and files.



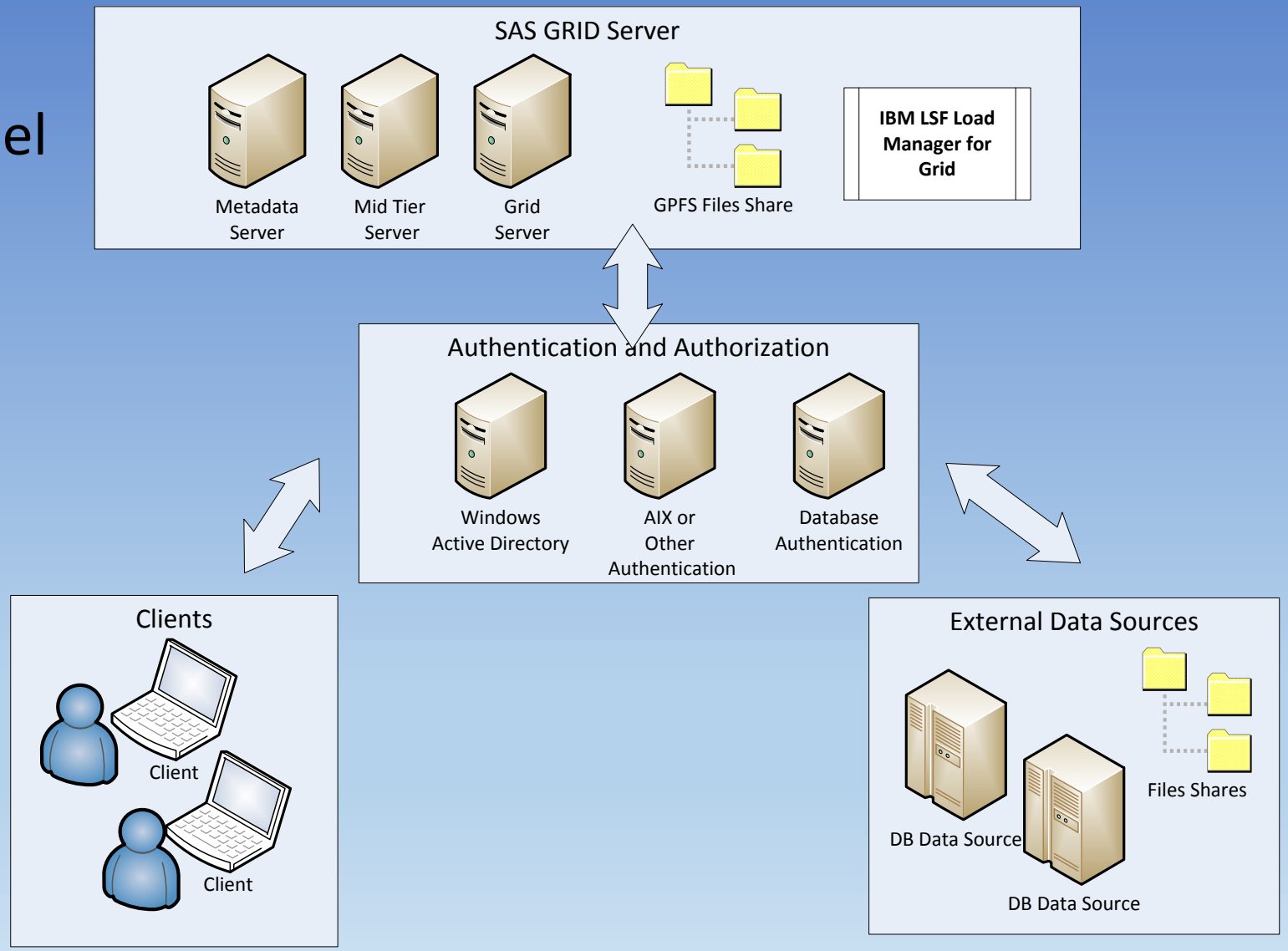


SAS Shared File Access Security

- SAS needs GPFS or other shared file facility as SAS is very IO intensive.
- At ATB we have a GPFS Share on each of our Grid Nodes.
- Shared folders are governed by Metadata Security and Operating Systems Security. Together they contribute to the users security access and actions.

Security Architecture

- Complete Layered Model



Questions?

- Contact: Gary Hochstenbach
- Email: ghochstenbach@atb.com