It was mentioned that the CATS item does not require that all the jobs be migrated, just that the access be more granular than the current “all users with ROOT access, have access to Autosys”

The audit matrix references removing the “root” id as the super user / super edit, from the R11 system and replace it with an alternative id like “autosys”.

Can you ensure that task item(s) be added to an early location in the plan to accomplish this.

1. Identify all users that require update access into the scheduler
2. Create an “autosys” or similar id to be the super user / super exec id in the R11 system
3. Credential all identified in #1 to have pbrun or sudo access to id created in #2
4. Test users access based on above credential
5. Remove “Root” id form R11.3 Autosys instance as super user / super exec.
6. All servers referenced
7. All job definitions
8. All machine Definitions
9. A Cross reference of job to machine definition

Based on meeting today:

1. LDAP/Active directory will not need to create any specific autosys related groups
2. EEM needs a read only bind to LDAP Denise will be providing specifics
3. a read only ID will be required for the bind, most likely AUTOSYS@CORP
4. Standard EEM groups created at EEM install time, and additional Application specific groups (that will need to be created in EEM) will be used.
5. users will be mapped from "IDENTIES-USERS" in EEM to the groups listed above
6. EEM policies will be applied to specific groups to control level of access for that group (policy to group relationship can be one to multiple)
7. Policies will restrict both WCC access and CLI access.
8. Within WCC standard views will be used that will be populated by data controlled by the EEM policies.
9. A user may belong to one or more EEM groups based on job role.
10. users leaving SSC will automatically be purged from EEM and WCC when their corp account is deleted (it will roll through)
11. Additional ‘Corp’ ldap may be required, reviewing if operators also have CORP, if sop ‘Corp’ domain may not be needed
12. Question on NIS controlled access is still an open issue as these will not be loaded by the bind.