Here is the explanation of the authorisations users require to determine CATT and eCATT permissions in addition to the system level enablement.

We observed that despite the system level permission being in place, the function call introduced by the latest SAP patch 'CAT_PING' was still failing for the users in question who were still unable to run non-batch scripts.

On examination of the code for the CAT_PING function module in transaction SE37 in SAP we discovered the below authority checks:

```
IF sysinfo-cattok CO 'XEF'.
  AUTHORITY-CHECK OBJECT 'S_DEVELOP'
       ID 'DEVCLASS' DUMMY
       ID 'OBJTYPE'  FIELD 'SCAT'
       ID 'OBJNAME'  FIELD '*'
       ID 'P_GROUP'  DUMMY
       ID 'ACTVT'    FIELD '16'.
  IF sy-subrc <> 0.
    AUTHORITY-CHECK OBJECT 'S_DEVELOP'
         ID 'DEVCLASS' DUMMY
         ID 'OBJTYPE'  FIELD 'ECSC'
         ID 'OBJNAME'  FIELD '*'
         ID 'P_GROUP'  DUMMY
         ID 'ACTVT'    FIELD '16'.
    IF sy-subrc <> 0.
      sysinfo-cattok = 'Y'.
    ENDIF.
  ENDIF.
```

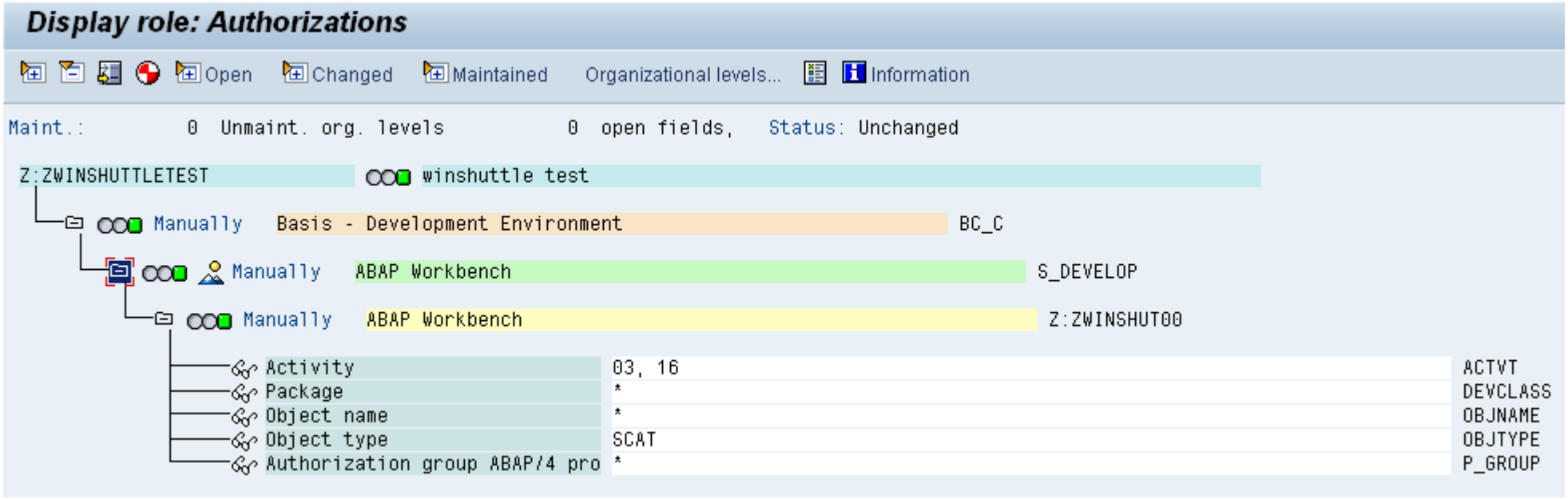
These lines of code pinpointed the authorisation objects that needed to be set up, namely the users need to have an auth object with the attributes:

OBJECT: 'S_DEVELOP'
OBJTYPE: 'SCAT'
OBJNAME: '*'
ACTVT: '16' (=execute)

Failing that, it needs to have the object

OBJECT: 'S_DEVELOP'
OBJTYPE: 'ECSC'
OBJNAME: '*'
ACTVT: '16' (=execute)

We were able to put together an authorisation based on these values as follows and assign it to our test user:




After assigning the above authorisation object to the test auth role 'Z:ZWINSHUTTLETEST', the test user was able to again run non-batch scripts.

So for all clients who have experienced the inability to run non-batch scripts after applying SAP BASIS 7.00 Support Package 24, as well as enabling the system level (client specific) parameter 'CATT/Ecatt – allowed', they need to ensure at the user level that users are assigned the above authorisation object somewhere in their authorisation roles and profiles – perhaps built into a special 'Winshuttle user profile/role'.