Best Practice - How to analyze user lock issue

If you have maintained logon data in many settings and it's not documented, you may have trouble when you find that the user is locked automatically.

In this page, we will discuss what to do when you found a user is automatically locked in AS ABAP.

Security Audit Log should be the first place you need to look at.

If you have not activated it yet, you should activate it via SM19. You can use dynamic configuration for trouble shooting.(FAQ note:539404)

After Security Audit Log is activated, unlock the problematic user and then wait until it is locked.

After the user is locked, you can open SM20 to check the records for the user.

Here is an example:

The columns "Terminal name" and "Security Audit Log message text" are important.

"Terminal name" tells you the host name which has triggered the request with wrong logon data.

"Security Audit Log message text" describes the type of request. You can look up the explanation for "reason, type, method" in note 320991.

The next steps are based on these information.

Case 1: You found the requests were triggered by RFC requests.

In this case, if you know the programs running on the host(Terminal name in SM20) which can trigger such kind of request, you can check the logon data for the programs.

If you don't have an idea, you can try to generate trace as per note 171805 to find the program name.

Case 2: You found the user are locked by user SAPJSF.

SAPJSF is used during the user authentication that takes place between the JEEE Security service and the AS ABAP by RFC communication.

So if SAPJSF locks a user, it means the request is from AS JAVA.

You need to check the HTTP access log "responses.<Nr>.trc" from the HTTP provider service in the directory "/cluster/server<Nr>/log/system/httpaccess" in the AS JAVA.

If you are lucky, you should be able to find an entry with return code 401 like:
Next, you should check on host [xxx.xxx.xxx.xxx] to see what program can trigger HTTP request to the J2EE engine.

The URL will give you hint about what application the program is related to.

For example, if the URL is SLD related, you should check the following notes:

1828470 SLDDSUSER and SLDAPILUser accounts Locked
1650035 SLDDSUSER locked due to incorrect logon to SLD
1426723 Solman_Setup locked slddsuser, sldpiuser
1665838 How to check why a technical PI user gets locked

In worst case, if you are not able to find the source of the wrong logon data, you can copy the user to another user and start to use the new user in the known settings so that you don't need to unlock the user manually time by time.

Recommendations:

1. Keep records whenever you maintain logon data so that you won't suffer such kind of issue.
2. Use username with application/system related words. eg: SLDDSUSER_<SID>. Never use SAP*, J2EE_ADMIN or DDIC.
3. If the issue occurs due to trigger from a J2EE server, then go through SAP Note 1493272 thoroughly and the attachment LocationGuide.zip. A location "com.sap.security.userlocking" needs to be created. This won't be existing on the system by default and needs to be created. After this check all the possibilities mentioned in the note.

Password settings in AS ABAP:

1. SM59 RFC destinations.
2. SICF
3. SLDAPICUS
4. SWU3
5. SOAMANAGER

Password settings in AS JAVA:

1. SAP NetWeaver Administrator -> Configuration -> Infrastructure -> Destinations
2. SAP NetWeaver Administrator -> Configuration -> Infrastructure -> Jco RFC provider.