Troubleshooting Validation errors of Autosys Server & Credential User

Autosys 11.3 & WCC 11.3

This document has been composed based on multiple experiences.

1. **Autosys environment:**

   a) On Unix/Linux: Config.$AUTOSERV file.

   ```
   AutoServer=<name>  \rightarrow specify the same name in WCC
   AutoServerPort=9000  \rightarrow specify 9000
   UseEncryption=0
      =1  \rightarrow specify the value NONE
      =2  \rightarrow specify the value DEFAULT
   ```

   On Windows, look at the Autosys Administrator GUI.

   ![Autosys Administrator GUI](image)

   ![Autosys Application Server](image)

   b) Run `chk_auto_up -r 111` and check if the application server is running. Make sure the name of application server matches with AutoServer.

   **Note:** You must use the `-r` option to check the status of the application server. If you invoke the `chk_auto_up` command without any arguments, it just checks the status of the event server(s) and scheduler(s).

   Example:

   ```
   $ chk_auto_up -r 111
   CAUAJM_I_50054 Attempting (1) to Connect with Database: orcl
   CAU AJM_I_50055 *** Have Connected successfully with Database: orcl. ***
   ```
c) Run “autorep –M ALL > machine.out” and look for the machine that corresponds with the system agent installed on this box. The status of this machine must be ‘Online’.

Example:

<table>
<thead>
<tr>
<th>Machine Name</th>
<th>Max Load</th>
<th>Current Load</th>
<th>Factor</th>
<th>O/S</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HostA.abc.com</td>
<td>---</td>
<td>---</td>
<td>1.00</td>
<td>Sys Agent</td>
<td>Online</td>
</tr>
</tbody>
</table>

Run “autoping –M <machine_name>” to see if this works fine. Autoping verifies that the server and agent are properly configured and are communicating successfully. It also verifies that the agent is able to communicate with the application server.

Example:

Autoping –M HostA.abc.com
CAUAJM_I_50023 AutoPinging Machine [HostA.abc.com]
CAUAJM_I_50025 AutoPing WAS SUCCESSFUL.

Note: The machine name is case sensitive. This is important when specifying <userid>@<hostname> as Credential User where hostname is in fact the machine name defined in Autosys.

Additionally you can also run an Autosys job onto this machine and look if it ran successfully.

- You can use JIL to define the job.
- Run “SENDEVENT –E FORCE_STARTJOB –J <job_name>”
- Run “autorep –J <jobname> -d”

This will tell us that the System Agent is working fine.
d) Run ‘autosys_secure’ and check if EEM is enabled. If EEM is enabled you can ignore the next point.
   - If you see the following option when running autosys_secure
     [1] Revert to NATIVE instance security.
     then EEM is enabled.
   - Choose following option under autosys_secure:
     [5] Manage user@host users.
     followed by
     [4] Show all user@host users.
     Check if the userid@host that will be used for Monitor ID is defined
     Example: CAUAJM_I_60140 Listing all user@host users:
               user1@HostA

   - You can add the userid which will be used for Monitor ID thru following option:
     [1] Create user@host or Domain password.

     Note: The password given for the userid in user@host must be identical as the password given in Monitor ID, obviously.

2. WCC environment

On the WCC side, the Autosys Server definition includes following important fields:
   - Application Server Host Address: ➔ put the same name as in AutoServer
     ➔ should match the name in chk_auto_up
     ➔ case sensitive
   - Application Server Host Port ➔ must match the AutoServerPort
   - EEM enabled or not ➔ check autosys_secure
   - Encryption Type : NONE/DEFAULT or AES + key
     ➔ See Use Encryption
   - Monitor ID :
     1. If EEM is enabled, then the userid must be defined within EEM and have correct access rights.
        No need to add @<hostname>
     2. This userid can be defined in 2 ways
        a. If you have defined 1 as_server name then there is no need to add @hostname
           
           Note: by default the @hostname suffix is taken from the Application Server Host Address
        b. If you have defined 2 as_servers (server1,server2) then you must define the user with
           @hostname suffix. The Monitor ID is only compared against what is defined in the
           autosys_secure under this option: [5] Manage user@host.
           This must match and it is case sensitive.
3. **CSAM**

Run the following 2 commands on both Autosys machine and WCC machine:
On Unix, it’s located under `$CSAM_SOCKADAPTER/bin`. On Windows, `%CSAM_SOCKADAPTER%in` should be in the PATH variable.

```bash
  csamconfigedit port=9000 display
  csamconfigedit portrange=49152-50176 display
```

Check the output of these commands and look for the 2 parameters “EnableSSL” and “EnablePmux”.

Example:

```bash
  $ ./csamconfigedit port=9000 display
  [ZoneName:  GLOBAL]
  Current settings for port:  9000

  General:
  OutboundHostList=<no value>
  EnableServiceLookup=<no value>
  SSL Authentication and Encryption:
    EnableSSL=False
    ServerStyle=<no value>
```

...
Port Multiplexing:

- PmuxServerPort=<no value>
  - **EnablePmux=True**
  - PmuxLegacyPortListen=<no value>
  
  ...  

The values themselves are less important but they do need to be identical on both Autosys and WCC side. If they aren’t identical, you can change the values using same command followed by the parameter and value you want to set.

Example:

```
csamconfigedit port=9000 EnablePmux=true
```

```
csamconfigedit portrange=49152-50176 EnablePmux=true
```

If the above settings are identical on both machines, check the "$CSAM_SOCKADAPTER\log\csam.log" file to see if connections between both machines are happening and/or if you don’t see other errors/problems.

4. **System Agent**

When validating a credential userid, WCC contacts the Application Server (AS) and the AS connects to the agent that is defined in @hostname to verify if the userid and password are valid. The agent submits a job that performs a command called "chkusr".

The userid must be a valid OS userid.

a) If you defined @hostname then this hostname must match the name of the system agent.
   - a. You can check the machine name: autorep -M ALL
   - b. You can check the parameter ‘agentname’ in ‘agentparm.txt’ located in directory
     `<install_path>/SystemAgent/<agentname>`
     This is case sensitive.

b) As mentioned the System Agent submits a job to check if the userid exists and if the password is correct. Under the SystemAgent directory you will find following structured directories:
   1. `<install_path>/SystemAgent/<agentname>`
   2. `<install_path>/SystemAgent/<agentname>/spool`
   3. `<install_path>/SystemAgent/<agentname>/spool/<$AUTOSERV>_SCH`
      → This directory contains job log files which are launched by Autosys itself
   4. `<install_path>/SystemAgent/<agentname>/spool/<$AUTOSERV>_APP_<machine_name>`
This directory contains the job log files from each credential user validation.
Go further into this directory structure .../MAIN/WAAE_WFO.1/...

For every validation you will find 2 files here. One of the files is named with a numeric value. The other file starts with same numbers and ends with extension .joblog. In Unix you’ll see a third file with extension .sh.

Look at the .joblog file. You should see that it executes a command that looks as follows:
```
Data(Command="/products/CA/WorkloadAutomationAE/SystemAgent/WA_AGENT/chkusr",Args="autosys 0C6C30073DF47232 su") User(root)
```

The other file should contain
User and Password okay

If job ends with a non-zero return code, then the validation failed.

Possible errors:
1. Check if userid and password being used are correct.
   Under <install_path>/SystemAgent/<agentname> directory you will find 2 binaries called password and chkusr:
   a) Run ./password <password_of_userid> → It returns encrypted password value
      Example:
      ```
      ./password p@ssw0rd1
      Encrypted password: 576A5FC56D6B8DA3C8
      ```
   b) Run ./chkusr <userid> <encrypted password value obtained from previous command> → This should give you ‘User and Password Okay’
      Example:
      ```
      ./chkusr userA 576A5FC56D6B8DA3C8
      User and Password okay
      ```

   If this isn’t the case, then possible problem could be that userid doesn’t exist and/or password is invalid.

2. Check the .joblog file if the args for chkusr command are identical to what you just tried with password and chkusr command.

3. When PAM is used for User Authentication on Unix systems, you need to check the parameter ‘oscomponent.auth.pam.svc’ in <install_path>/SystemAgent/<agentname>agentparm.txt.
It specifies which PAM service the agent will use. The list of available PAM services for your system is located in /etc/pam.conf or etc/pam.d/ file.

The default is login. Others are sshd and su.
   Example:
   oscomponent.auth.pam.svc=sshd

Again, you can use ‘./chkusr’ command to test this. You need to add the value after the password. If this fails, then try same command with ‘login’ or ‘su’.
   Example:
   ./chkusr userA 576A5FC56D6B8DA3C8 sshd
   ./chkusr userA 576A5FC56D6B8DA3C8 su
   ./chkusr userA 576A5FC56D6B8DA3C8 login

If it works with one of these values, then modify this parameter accordingly in agentparm.txt and recycle the agent.

5. **Ports**

If firewalls are located between WCC and Autosys machines, you’ll need to check if ports are opened in both directions.

- WCC will not be able to connect to the Application Server without the ports opened BIDIRECTIONALLY (Inbound/Outbound).
- The Autosys Server will not validate or connect without these ports “Opened”.

Following Default Ports need to be opened on both the WCC AND Autosys Server:
   9000 7163 7520 7507 7500

You can find a complete list of ports being used by WCC in the “CA Workload Control Center Implementation Guide – Chapter C: WA WCC Default ports”.

a) You can use “telnet” as a testing tool to figure out if a specific port is open or not.
   On most systems, you can test to see if you can reach the Autosys Server Application port 7163. You should be able to get a PID back from the Application server if you are able to reach it.
   
   Example 1:
   From the Autosys Server you can telnet to itself on port 7163.
   telnet localhost 7163
   Connecting to localhost...

   If you see messages about connection closed by foreign hosts, your port *maybe* blocked. This does not happen in all instances.
Example 2:

From the WCC server you can telnet to the Autosys Server on port 7163. We want to see if WCC is able to reach out to the application server.

telnet HostA.abc.com 7163
Connecting to HostA.abc.com...

This method is not fool proof, but it can help in determining if the ports are open for use.

b) You can use “netstat -a” as a tool on the WCC machine to see if the WCC processes are using the assigned ports. You should see a listener on these ports.

Example:

```
netstat -a
```

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:1527</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1627</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:5250</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:7001</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:7163</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:7520</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:8080</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10129</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10132</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10135</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10138</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10143</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10146</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10149</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10152</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10155</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10158</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10161</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:10222</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:11501</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:11502</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49152</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49153</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49154</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:49155</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:64366</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:64368</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:64414</td>
<td>wcc-testbox1:0</td>
<td>LISTENING</td>
</tr>
</tbody>
</table>
6. **Hostname resolving**

Check the `/etc/hosts` (unix) or `C:\Windows\system32\drivers\etc\hosts` file to make sure that the hostname resolves to the correct IP address. This can be different to DNS configuration/setup.

Check out if you’re using short hostname and/or fully qualified hostname.

You can use ping and `ipconfig` commands to verify.