Troubleshoot HCMF

Network Errors During Installation

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If the server cannot connect, a message appears; you are prompted to select one of the following options:

- **RETRY**—The installation program tries to validate networking again. If validation fails again, the error dialog box appears again.

- **REVIEW (Check Install)**—This option allows you to review and modify the network configuration. When this option is detected, the installation program returns to the network configuration windows.

  The network configuration is validated after you complete each networking window, so the message may appear multiple times.

- **HALT**—The installation stops. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.

- **IGNORE**—The installation continues and the networking error is logged. In some cases, the installation program validates the network configuration multiple times, so this error dialog box may appear multiple times. If you choose to ignore network errors, the installation may fail.

Log File Examination

If you encounter problems with the installation, you may be able to examine the installation log files by running the following commands in the command line interface.

To obtain a list of install log files from the command line, enter

CLI > file list install *

To view the log file from the command line, enter

CLI > **file view install** *log_file*

where:

`log_file` specifies a log file name having the format: `install_log_YYYY-MM-DD.HH.MM.SS.log` in which the date and time of the log file is the time at which the install or the upgrade was initiated on the system.

You can get more information about installation events by viewing or downloading the System History log. For more information, see .

WS Node Installation Failure

- A common cause of WS node installation failure is forgetting to add the WS Node to the cluster on the Application Node.

  To confirm that this is the source of the failure, check the install log for the message `IPM|Capture: Node not in cluster: Install will halt | LVL::Debug`.

  To correct the problem, log in to the CLI on the Application Node, and add the WS node to the cluster using the **set hcs cluster node** command. After adding the WS node to the cluster, repeat the WS node installation.

- A WS node installation can fail if the admin password for the Application node contains a '$' character.

  The install log will contain the error: `"Critical Error" "The installation has encountered a unrecoverable internal error."`

  To correct the error, change the password on the Application node to a password that contains only alphanumeric, hyphens, and underscores, then reinstall the WS node.

Cluster Node Version Mismatch

Sometimes, a Web Services (WS) Node installation or upgrade may complete, but the WS Node version is not correctly updated in the cluster information on the Application Node.

For an installation, the output of the **show hcs cluster node** command shows the WS Node version as `Not_Installed`.

For an upgrade, the output of the **show hcs cluster node** command shows the WS Node version as a back-level version.

A cluster node mismatch is a valid condition when you are installing or upgrading multiple WS Nodes and some have completed and others have not completed. The nodes that have not been installed or upgraded have the results shown above.

You can correct the error situation in which a WS Node has been installed or upgraded, but continues to show Not_Installed or a back-level version.

1. Verify that the installation or upgrade of the WS Node is complete. Check the WS Node VM console to see that it is waiting for a login, and the version is correct.
2. Log in to the WS Node as OS admin.

3. Run the **set hcs version** command.
4. Log in to the Application Node as OS admin.
5. Run the **show hcs cluster node** command to verify that the WS Node version is correct.

Synchronization Failure Between HCMF and UCS Manager

There can be following reasons for encountering issues during HCMF and UCS manager sync failure:

• UCS Manager Certificate expiration.

• UCS Manager Certificate is not added in the trust store of HCMF.

In either case, execute the following steps:

1. Check whether the UCSM sync is successful by disabling the certificate authentication.

2. Get the output for the following commands:

   • **show cert list own**

   • **show cert list trust**

3. In the output at step 2, check whether the UCSM server's cert is added to the trust store list.

4. Check if there are any expired certificates.

   See View Certificate Status at Service Provider Level to check the certificate status of all customers.