1. Making target node alternate communication paths retriable when connected via Secure Proxy

1.1 Overview

When PNODE(CDz) attempts to connect with the SNODE through SS, first the connection from Pnode to SSP is built then SSP tries to communicate with Snode, upon a successful connection the transfers are initiated. In current scenario, if SSP fails to connect to Snode as is not reachable due to connectivity issues then SSP reports this failure back to Pnode (CDz) as SSL handshake error (CSPA202E) with RC=001. Pnode (CDz) does not attempt to retry the connection with alternate node as this is a secure plus error and retries are done for connection errors.

To customer it appears that with intermediary in between if the Snode is unreachable the alternate path is not being tried. While the intermediary could be configured with alternate path, Customer's configuration requires the alternate comm to be configured at Pnode (CDz).
This leads to the requirement of handling the SSL handshake error with RC=001 differently when CDz has SSP in between and an alternate path is configured.

As part of the proposed enhancement, we will introduce a new behavior for handling the **CSPA202E with RC=001** error when the **SSP** is in the middle of a connection. Below are the detailed research points and considerations related to this enhancement:

Research points/Assumptions:

1. CSPA202E Error with RC other than 001

- For all instances of **CSPA202E errors with return codes (RC) other than 001**, the behaviour will remain unchanged. These errors will continue to be processed and handled as they currently are, without any modification. The new retry mechanism only applies to **RC=001** errors when SSP is involved in the connection.

2. SSP Not Between Connection

- If the **SSP** is not involved in the connection (i.e., it's not between the source and target nodes during communication), the **CSPA202E with RC=001** error will **not** be retried using an alternate communication path. In this scenario, the system will behave as it does today, and no additional retry logic will be triggered.

3. Alternate Communication Path Availability

- The ability to retry the **CSPA202E with RC=001** error using an alternate communication path is contingent on the presence of such a path in the node

definition. If an **alternate communication path** is not defined within the node configuration, the retry mechanism will not be triggered. In this case, the system will revert to the current error handling process, which does not involve retrying the connection.

4. Configuration of New Initparm Parameter (ALTCOMM.SSP)

- A new **initparm parameter (ALTCOMM.SSP)** must be set to **'yes' or 'Y'** for the retry mechanism to be activated. If this parameter is not explicitly set to **'yes' or 'Y'**, the system will behave according to the existing error handling procedures, and the **CSPA202E with RC=001** error will not be retried. This provides flexibility in enabling or disabling the retry feature based on the specific needs of the environment.

5. Support for Both PUSH and PULL Processes

- The new retry logic will be applicable to both **PUSH** and **PULL** processes. Whether data is being pushed from the source node or pulled from the target node, if the conditions for the **CSPA202E with RC=001** error are met, the system will attempt to use the alternate communication path for retry, if the required conditions (such as SSP in the middle of the connection and availability of the alternate path) are satisfied.

6. Applicable Only When CD z/OS is the PNODE

- The retry functionality for **CSPA202E with RC=001** error will be applicable only in scenarios where the **CD z/OS** system is the **PNODE (Primary Node)**. In other words, this enhancement will not work if the **PNODE** is a different system type, as it specifically relies on CD z/OS as the primary node for the alternate communication path to function properly.

1.2 High Level Architecture

1.2.1 Approach

The current system experiences a scenario where the error code **CSPA202E**, accompanied by **return code RC=001**, causes the connection to halt, preventing any further execution. This issue is particularly challenging as the error is not retriable under the existing configuration, and the file transfers start to fail.

As part of the proposed enhancement, we are introducing a mechanism to allow the **CSPA202E with RC=001** error to be retriable under certain conditions. Specifically, when the error occurs due to issues in the communication path (such as a failure in the communication with the **SSP** in the middle of a connection), the system will be able to attempt recovery through an **alternate communication path**. This recovery process would be initiated by setting a new **initparm parameter** named **ALTCOMM.SSP** to **'YES'** or **'Y'**.

1.3 Workflow:

1.3.1 New Initparm Parameter:

We are introducing a new initialization parameter, **ALTCOMM.SSP**, which enables the system to treat the **CSPA202E** error with a return code of **RC=001** as a retriable error, using an alternate communication path.

ALTCOMM.SSP = YES|NO , Y|N

Parameter Details:

- **Default Value**: The default setting for the **ALTCOMM.SSP** parameter is **'NO'**.
- **Enabled Value**: If you wish to enable this functionality, set the **ALTCOMM.SSP** parameter to **'YES'** or **'Y'**.
- **Conditions for feature to be in force:**
    1. **ALTCOMM.SSP** is set to **'YES'** or **'Y'.**
    2. **SSP is in the Middle of the Connection**: The communication process must involve an **SSP (Secure System Proxy)** located in the middle of the connection.
    3. **Alternate Communication Path defined in the Node Configuration**: There must be an **alternate communication path** defined in the node's configuration. This alternate path will be used if the primary communication fails.

When the above three conditions are met, a CDz Pnode will automatically retry communication via an alternate path upon encountering the CSPA202E error with RC=001. The file transfers will be routed to this alternate path till the system continues to receive CSPA202E error with RC=001.