ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

Review Article

Open Access

Sterling Integrator File Transfer Protocol Configurations

Prashanth Kodurupati

Information Technology, Managed File Transfer Engineer, Minisoft Technologies LLC, Alpharetta, USA

ABSTRACT

IBM Sterling Integrator supports a wide range of file transfer and communication protocols, including SFTP, Connect: Direct, and Mailbox (HTTP). While connecting with client servers, it's imperative that these protocols and all other prerequisites for a successful file transfer, including authentication protocols, encryption, and file naming conventions, match between the IBM Sterling adapter for a connection and the client server.

***Corresponding author**
Prashanth Kodurupati, Information Technology, Managed File Transfer Engineer, Minisoft Technologies LLC, Alpharetta, USA.

Received: January 11, 2024; **Accepted:** January 16, 2024; **Published:** January 25, 2024

Keywords: Sterling Integrator, IBM Sterling Integrator

Introduction

With a significant market share across multiple verticals, IBM's Sterling Integrator is one of the most widely used B2B integration platforms with robust bulk communication and data exchange capabilities. It facilitates secure connectivity between businesses and their B2B clients and data transfer and streamlines the process through various features. However, for a seamless transfer to occur between a business and its client's servers, the configuration has to align for each connection, especially when it comes to data transfer and communication protocols. Three of the protocols Sterling Integrator natively supports are SFTP, Connect: Direct, and Mailbox (HTTP).

Literature Review

There is ample literature on two of these three protocols and relatively limited (and mostly from a single source - IBM) literature on Connect: Direct, which is a proprietary file transfer solution. In both cases, the literature covers a comprehensive range of scenarios, including the challenges that may arise if there is a protocol discrepancy. Secure File Transfer Protocol (SFTP) allows the transfer of files/data over a network and is among the most widely used secure file transfer protocols, capable of catering to a wide range of use cases, including remote systems, but they need to be configured as per the requirements of the connection and transfer [1]. Most mailboxes, whether they are operating in conjunction with IBM Sterling integrator (or under it), rely on HTTP for their access layer, but there are other options as well, and even HTTP-based mailboxes may vary greatly based on their inherent security and other features [2]. Literature on IBM's proprietary Connect:Direct file transfer mechanism (or protocol) focuses on its strengths, typically in the context of other IBM systems, and the official IBM documentation on the topic covers everything from its features to configuration [3]. There is also ample literature, mostly from IBM and other resources, on how IBM Sterling should be configured to ensure secure and seamless data transfer [4].

Problem Statement: Misconfiguration of the Protocols

Before evaluating the problem itself, we have to consider three of the commonly used communication and data transfer protocols supported by IBM Sterling integrator that are at the root of this problem.

Overview of Three Protocols

It's important to understand that IBM Sterling supports a wide range of protocols, but based on use cases, industries, and preferences, businesses may only work with a limited set of these protocols during their operations.

SFTP

Secure File Transfer Protocol (SFTP) is a variation of widely used File Transfer Protocol (FTP) and is built on top of Security Shell (SSH), an encryption protocol. This allows SFTP to secure both data and instructions being exchanged between the client and host servers via encryption. It's also quite versatile.

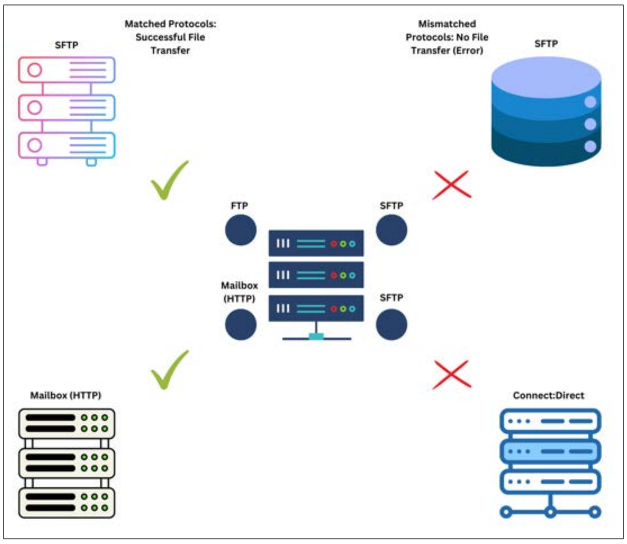
Connect: Direct

Connect: Direct is a proprietary peer-to-peer integration middleware that facilitates secure data transfer, both high volume and massive file size. It also allows for automation, making it an ideal tool for a wide range of Managed File Transfer (MFT) scenarios.

Mailbox (HTTP)

HTTP-based mailboxes, whether used in an IBM Sterling environment or with another integrator, lean more toward communication than data transfer.

Failed Communication and File Transfer Because of Protocol Misconfiguration


SFTP
Matched Protocols: Successful File Transfer
Mismatched Protocols: No File Transfer (Error)
SFTP
FTP
SFTP
Mailbox (HTTP)
SFTP
Mailbox (HTTP)
Connect:Direct

The host server leveraging IBM Sterling integrator has to treat each connection for file transfer and communication individually/separately, and if it's misconfigured, messages and data won't transfer between host and client servers (either way) and will result in an error side requesting the transfer. This can prevent client servers from requesting important and, in some cases, mission-critical data from host servers.

Suggested and Implemented Solutions

The overarching solution to this problem is to configure each connection as per the client's requirements, for which the first prerequisite is setting up the connection using the same protocol that the client-server will use to transfer the files. For example, if they use SFTP, the connection should be configured for SFTP (an SFTP adapter) [5].

However, there are other considerations beyond matching the file transfer/communication protocol. This includes authentication protocols that the client is using as well as their encryption protocols. An encryption mismatch and the presence of incompatible encryption protocols on either side of the connection can prevent files from being transferred successfully between client and host servers.

When setting up a more advanced solution/protocol like Connect:Direct, there may be additional requirements, like setting up the right node configurations. Similarly, a different set of configuration requirements may apply when setting up a mailbox within the IBM Sterling integrator environment, including choosing between NIST or FIPS compliance based on the client's requirements.

In conclusion, the file transfer protocol configurations have to take into account the client's requirements and protocols, and while configurations may be swapped between clients with similar requirements, a universal set of configurations governing all file transfers and connections will not be advisable.

Summary of Configuration Mismatch Scenarios and Solutions for the Three Protocols

The following scenarios and solutions go beyond the protocol level mismatch.

Protocol	Mismatch Scenario	Potential Solution
IBM Sterling Mailbox (HTTP)	Incorrect URL path or mailbox name	Verify the mailbox name and path exactly match the client's configuration. Ensure the configured path points to a valid directory on the Sterling Integrator server.
	Authentication method mismatch	Configure the Sterling Mailbox adapter using the same authentication method the client uses (e.g., Basic Authentication, OAuth). Ensure valid credentials are provided for the chosen authentication method.
	File naming convention mismatch	Align the Sterling Mailbox's file naming conventions with the client's expectations. This might involve filename extensions, timestamps, or specific formats.
Connect:Direct	Incompatible node configurations	Review the client's node configuration details (source and target node names, passwords) and ensure they match exactly in Sterling Integrator's Connect:Direct configuration.
	Incorrect file transfer directive (SEND or RECEIVE)	Verify if the intended action is to send or receive files from the client. Configure the Connect:Direct adapter with the correct directive (SEND or RECEIVE) based on the requirement.
	Missing or incorrect security settings (like SNA security products)	Ensure the required security products (e.g., ACF2, TSAF) are configured on both Sterling Integrator and the client's Connect:Direct server. Verify that security product settings (like key rings and profiles) are identical on both sides.

SFTP	Mismatched encryption algorithms (e.g., AES-256 vs. DES)	Configure the SFTP adapter in Sterling Integrator to use the same encryption algorithm supported by the client-server. Refer to the client's documentation for supported algorithms.
	Incompatible TLS versions	Update the Sterling Integrator's SFTP adapter settings to use a TLS version compatible with the client-server (ideally TLS 1.2 or higher).
	Incorrect username/ password or key authentication issues	Verify the username/ password combination or private key used for SFTP access matches the client server's authentication setup.

Best Practices to Avoid Misconfiguration Issues

The most important practice when establishing connections with new client servers is to obtain all the necessary information required to properly configure a client-host server connection, including the file transfer/communication and authentication protocols they use. Access to this information at the time of configuration can prevent failures and reconfiguration.

FTP engineers and other professionals responsible for ensuring IBM Sterling on the host side and creating adapters for client connections should look into a broader set of mismatches than just configurations. This includes file naming conventions. If you have a different naming convention than your clients, it may cause transfer errors, or even if the transfer is successful, there may be traceability and usability issues.

Creating configuration templates for some of the most commonly used adapter settings and connections can prevent repetitions when setting up connections for new clients.

Potential Use Cases

The solutions can be implemented in every host-client connection scenario where the host uses IBM Sterling to connect with their clients/client servers and govern data transfers. However, the solutions are limited to three primary file transfer/communication protocols, i.e., SFTP, Connect: Direct, and Mailbox (HTTP), and if the clients are using protocols other than that, they may require a different set of solutions. However, the underlying aim in almost every scenario would be to match host-side adapter configurations with the client requirements.

Conclusion

File transfer and communication protocols are a core element of every secure connection and file transfer instance, and any clash among these protocols between two server entities initiating a file transfer or connection can lead to a failed file transfer. However, if it's identified when the file transfer is critical to business interactions/operations, it can result in financial and reputational losses. Therefore, the goal should be to have every client connection in IBM Sterling tested and configured correctly.

References

1. Jasveer Singh TJ, Pavneet S, Kunal B (2018) What is Remote Triggered Software Defined Radio Using GNU Radio. Online Engineering & Internet of Things, Lecture Notes in Networks and Systems 822-830.
2. Mohammed M Alani (2014) Guide to OSI and TCP/IP Models. Springer Briefs in Computer Science https://link.springer.com/book/10.1007/978-3-319-05152-9.
3. (2018) IBM Connect:Direct Overview 6.0 Documentation. IBM https://www.ibm.com/docs/en/SS4PJT_6.0.0/cd_overview_PDF/cd_60_overview_pdf.pdf.
4. James B, Claudemir B, Vasfi G, Rahul G, James BH, et al. (2012) End-to-end Integration with IBM Sterling B2B Integration and Managed File Transfer Solutions. International Technical Support Organization - IBM Redbooks https://www.redbooks.ibm.com/redbooks/pdfs/sg247992.pdf.
5. Mark Beckner (2013) Ports, AS2 and Acknowledgements. BizTalk 2010 EDI for Health Care 55-74.