FTP Replacement: Where MFT Makes Sense and Why You Should Care

Gartner RAS Core Research Note G00208765, Thomas Skybakmoen, 8 November 2010, RAV5A5 11232011

This research provides advice on when to replace FTP with managed file transfer (MFT) solutions, and which features to consider. MFT solutions can be MFT software and MFT as a service; see "Gartner 2010 Research Outlook on Managed File Transfer." We also highlight where MFT fits into the technology landscape, along with some of its key benefits.

Key Findings

- The technical differences between FTP and MFT are increasing, such as security, administration and scalability.
- Organizations migrating from FTP to MFT must recognize that additional implementation concerns accompany the added functionality provided by MFT.
- A number of vendors are expanding their MFT portfolios to include support for more deployment options and usage scenarios.

Recommendations

Organizations replacing FTP:

- Decide whether you are looking for a plain FTP replacement, or whether you need upgraded functionality to better work in conjunction with the infrastructure deployed and include support for more-challenging business processes and integration.

Organizations implementing MFT:

- Consider service-oriented architecture (SOA), cloud and e-mail integration needs as part of your planning process.

MFT vendors:

- Clarify your messaging to distinguish between simple FTP replacement scenarios and full B2B MFT implementations, as organizations often do not see the differences.

Gartner

ANALYSIS

What You Need to Know

Organizations often use MFT solutions to replace FTP. This is due to increased focus on compliance, privacy regulations and corporate transparency – which demand increased auditing, management, security and process. FTP is slowly showing its age. Nevertheless, as organizations undertake FTP replacement, they should be approached with caution; there is a need to understand existing file transfers, and how to manage for the security, monitoring, scheduling and auditing that the file transfer warrants.

Introduction

FTP has been around since the late 1970s, and has been seen as the de facto method for exchanging large packets of data over the Internet. It has been widely used by businesses to transfer bulk data, both internally and in B2B environments, and is still offered as part of many B2B products. As with the growth of the Internet, businesses have also experienced a larger volume of file transfers; this can be from application to application (A2A), internally, as well as to business partners.

For this purpose, FTP meets business requirements. However, as file sizes and the volume of files transferred increased, in combination with the increase in business partners and applications, many found the need to look to alternatives that provide support for larger file sizes (typically over 2GB), improved throughput, the managing of simultaneous transfers of multiple files to multiple endpoints, better scalability and integration (A2A), and that better integrate into current SOA and cloud environments. Organizations have also found that the security (such as integration with Active Directory or Lightweight Directory Access Protocol [LDAP]), auditing, process control, monitoring and end-user interface fail to provide the adequate administration of growing FTP solutions.

FTP replacements demand better understanding to manage existing file transfers, and provide for the security (authentication at both ends of the transfer, and authorization for access to the push or pull target); auditing (nonrepudiation of both sender and receiver); process control (transfer initiation is script-based, schedule-based, file-system-based [move the file when it appears in a folder]); monitoring (restart failed transfers, send notifications of transfer starts/completions); scheduling; and governance and management that the MFT solution will bring.

FTP Meets Its Limitations

Although flexible and easy to deploy, FTP is based on the principle of “one to one” and, in some cases, “one to many,” but not “many to many.” In other words:

- FTP has often been used to send files from a single sender (e.g., one business partner to another).
- FTP has traditionally not been used to send one file to several business partners; while scripts and solutions can overcome this, writing and maintaining the scripts are cumbersome tasks.

An example of this can be found in the B2B environment, where the business is interacting with numerous trading partners, and the trading partner can download and upload files from and to the FTP server. However, there is no automated way for the business to communicate and share files with all trading partners in a collaborative way (e.g., via e-mail notifications on new file arrivals), which categorizes the many-to-many scenario often found in B2B environments.

Because there is an increase in the many-to-many file transfer scenario, FTP is showing its limitations. In these complex environments, businesses often have requirements that are not supported by traditional FTP solutions. These include, but are not limited to:

- Automated onboarding of users
- Automated rollout to servers for rapid deployment and provisioning
- APIs to integrate with applications, middleware, e-mail and cloud
- Management and security of file movement for collaborative purposes
- Internal connectivity between various operating systems and hardware
- Content validation before and after file transfer
- Route files based on policy or content
- Reporting and administration, including user activity, system utilization, scheduling, receipt monitoring, real-time notifications and routing
- Centralized reporting functionality for error reporting or status of all file transfers
- Centralized analytics

© 2010 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner’s research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner’s Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see “Guiding Principles on Independence and Objectivity” on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp

- File/data transformation, and file management with versioning capabilities to prevent data duplication or data loss
- Built in encryption, certification and validation of data
- Checkpoint and restart capabilities
- Workflow rules that dictate file movement from one job to the next and events that would trigger an action
- Metadata to ensure file integrity

The business often finds that it ends up using FTP as a stand-alone solution with multiple and often separate deployments, which includes custom scripts and bolted-on security in the form of antivirus to check incoming files (e.g., Pretty Good Privacy [PGP]) to try to meet these challenges. Although it is possible to use FTP in these situations, scalability to meet the many-to-many file sharing is lacking, and monitoring all these file transfers, users, computers and scripts is very resource-intensive.

Furthermore, FTP solutions offer little or no automation, such as a scheduler and built-in scripting, which would help completely automate file transfers. FTP does not include the ability to create workflows – once a file is sent or received, the capability of an event (a file arriving or being sent) to trigger workflow is not provided by FTP. Another feature often lacking is automated recovery from failures and guaranteed delivery in the form of integrity protection and nonrepudiation.

MFT Can Help

Organizations with aging FTP solutions and increased file transfer proliferation often look to MFT solutions to support existing file transfers (FTP) and meet new requirements, such as administrating the growing number of files and systems. Often, existing file transfers cannot be replaced "overnight"; here, MFT can help support existing file transfers by governing and monitoring them, while also supporting more-advanced protocols, including Applicability Statement 2 (AS2). Over time, existing file transfer solutions can be migrated fully to MFT to take advantage of added security, monitoring and more-advanced protocols.

The added protocols and features that come with MFT offer the ability to track and verify file transfers with digital receipts, and ensure security with digital signatures. This would include pre- and postfile transfer processing, which enables automatic inspection of policies, virus scanning, file conversion/transformation, etc. MFT also provides plug-ins to existing infrastructures, such as Active Directory or LDAP, to take advantage of existing security mechanisms, which can help businesses offload resource-intensive tasks. Furthermore, MFT offers document tracking or verification of delivery (nonrepudiation).

MFT Helps Compliance

Regulatory compliance mandates, such as the Sarbanes-Oxley Act (SOX) or the Health Insurance Portability and Accountability Act (HIPAA), are forcing companies to document all their business processes. Often overlooked is data movement – especially when it's accomplished using FTP – and enterprises are now seeing the need to look to alternatives. The compliance laws force the IT organization to ensure that confidential business data is kept secure during transit, and to verify that it was delivered to the intended recipient.

Gartner has found that many different file transfer solutions exist in companies, including secure FTP for external transfer, AS2 for supplier connections, and unsecure FTP for most internal and some external transfer. However, this trend is slowly changing in response to the increased focus on compliance. MFT solutions can also now, for example, extend the AS2 file transfer all the way through to the internal endpoint (such as an SAP system), to be able to monitor and provide SLAs end to end on the file transfer in question, which many organizations see as one of many benefits.

Gartner has also found that because organizations have offices in multiple locations, there is a tendency to use different systems and products, which contributes to the complexity in managing and running FTP solutions. Many organizations have found some benefit in MFT consolidation, as this allows for greater visibility and control, and should also help to lower costs by eliminating the expense of managing and maintaining multiple solutions.

MFT and Governance

Midsize to large MFT deployments will require some governance; therefore, organizations need to look to MFT solutions that have the ability to integrate with a governance solution, and to be part of existing governance policies and processes. This will occur either through an API or services that offer the ability to integrate into current infrastructures and applications, which include, but are not limited to, SOA, B2B, cloud, e-mail and collaboration.

Organizations that have poor visibility into file transfers find that managing them is resource-intensive, and operations personnel often spend time on problem solving and testing on each system to locate the cause of the problem, rather than having full traceability into the file transfer process. This operational burden is particularly heavy when MFT is implemented on a larger scale across many applications, systems and partners; when it is used as part of a wider B2B process; or when it is embedded in the implementation of a service in an SOA.

Services are "black boxes," and, typically, the group that fosters proper reuse of services (frequently called an SOA center of excellence [COE]) needs to know under what rules or contracts services can be reused. Having poor visibility into file transfers makes the job of an SOA COE very difficult, because the SOA COE enforces governance policies on the design and operation of the services. MFT software and services can offer a solution. They provide users with the ability to manage and monitor file transfers within and between organizations. Often, no platform-specific knowledge is needed, and IT can easily integrate MFT capabilities into an SOA, MFT to be used in service implementations, allowing the SOA COE to provide centralized governance services for file transfer.

MFT in Relation to Other Back-End Integration Technology

MFT is one category of back-end integration technology. Others include enterprise service buses (ESBs), B2B gateway software and integration-as-a-service (IaaS) offerings. These integration products and services are used to securely and reliably exchange

transactions, files, messages and transactions between application systems, external business partners and cloud services with the same level of governance and compliance as MFT. What differentiates MFT from other forms of infrastructure are:

1. Its unique focus on particularly large files, typically over 150MB, and the scheduling and management of moving very large numbers of files and bulk data between applications and businesses, as well as streaming capabilities that not only move very large files, but also offer a high data transfer rate

2. The movement of files and data in usage scenarios not typically addressed by many integration solutions, such as enhancing the performance of file attachments in e-mail

Note, however, that all integration solutions are rapidly converging so that, for example, MFT solutions continue to incorporate more-general-purpose integration capabilities, such as ESBs or IaaS, and vice versa.

Complexities Involved With FTP Enhancement or Replacement

IT modernization initiatives continue to grow, and, as applications and infrastructures are upgraded or replaced, FTP is often overlooked or neglected, because organizations often find this effort too complex. Gartner has found that many enterprises have disparate FTP deployments and several other file transfer solutions, such as best-of-breed MFT solutions.

However, companies that are replacing mainframes or applications should consider the option to replace or enhance the file transfer mechanisms (usually plain FTP) for facilitating the bulk movement of data jobs. The challenge is often the tendency not to document instances of processes that are dependent on FTP and HTTP, and when undergoing this modernization, FTP replacement is "put on ice." MFT can help in these efforts, by deploying MFT side by side with FTP, where the MFT solution will scan and read logs from the FTP, thus automating part of the modernization process.

Some MFT vendors also offer services to help organizations document and transfer the file transfer from FTP to MFT. However, as companies start to uncover these undocumented instances of unsecured and unmanaged data transmissions, they also start to consider how enormous the task of process identification is, and determine its reliance on FTP and/or HTTP. There are two separate tasks needed here: One is to identify the business processes involved. That's the purview of the business analysts. The second task is to identify the technologies that are used to implement those business processes. That's the purview of system architects.

Process identification (and the larger discipline of process re-engineering), in reference to MFT, can be expensive, because it needs to dissect all the layers of technology and infrastructure, and to move across multiple boundaries and silos of the business to determine process dependency and the processes' reliance on "vanilla" FTP and/or HTTP. The IT organization should start with process identification, modeling and documentation, as these are critical to FTP replacement and enhancement. This allows for a staggered upgrade that can be stretched over several months, starting with the most-visible and critical processes. Here, the process COE becomes involved in prioritizing the order in which processes are modified to incorporate MFT.

SOA in Relation to MFT

SOA does not change or reduce the need for MFT. In fact, as companies embark on their SOA and business process improvement initiatives, they will examine many of the processes that affect their data, many of which will implicitly rely on plain, unmanaged and unsecured FTP. Exceptions include systems that use message-oriented middleware, which have more-inherent reliability and monitoring capabilities (e.g., IBM's WebSphere MQ and Tibco Software's Rendezvous).

Although most SOA platform vendors argue that management and monitoring is provided by their ESB and embedded technologies (such as business activity management), these approaches tend to have performance issues when it comes to larger files. This is mainly because many SOA-based platforms are based on integration middleware, which are usually transactional-based systems, but don't support the streaming input/output necessary for high-performance movement and manipulation of large files. Even organizations with an ESB deployed will generally require MFT technology, and vendors such as IBM, Software AG and Tibco Software offer ESBs and MFT solutions.

FTP and Secure Shell

Most infrastructure vendors offer the Secure Shell (SSH) protocol, and since becoming open source, support for SSH is now equal among those vendors. SSH is popular in both mainframes and Unix environments, and is often used as an inexpensive tool to secure file transfers. Some companies see SSH as a simple, tactical solution to some of their security issues.

However, to enable SSH support in the Windows environment, you must have a specialized client or server. What is not addressed in those implementations is how to adequately manage, monitor and audit the traffic, while leveraging SSH. What this means is that, even if you enable SSH support in your Windows and Unix environments, you must consider functionality for auditability, management, monitoring and automation.

MFT Evolves From FTP Replacement

The traditional deployment scenario for MFT was to replace FTP. However, the role of MFT has been expanded to include a range of integration efforts, from internal A2A, middleware and data integration initiatives to external B2B and cloud-computing projects. MFT has gone from a stand-alone solution to one that offers a holistic approach that includes the ability to integrate into existing solutions for those project types.

MFT also helps govern files in applications such as e-mail (e.g., Outlook), collaboration tools (e.g., Documentum) and application development tools. We still see many organizations that require basic MFT functionality, such as secure, reliable, high-performance, large-file transport; checkpoint/restart to work around unreliable networks/connections; and multithreading to increase performance versus traditional file transfers, which is one of the primary reasons for considering MFT solutions.

However, MFT will evolve into a holistic solution that includes the ability to provide a set of services that works to enable various governance processes and policies related to the management, coordination and trust of the file transfer. As the MFT market evolves and solutions mature, it is important that organizations clearly understand that implementing MFT integration projects without a holistic, coherent strategy generally leads to inefficiencies and vulnerabilities associated with individual IT groups implementing MFT projects using different approaches and technology.

The MFT integration project should be defined in cooperation with other relevant IT strategies for internal integration, A2A, B2B, middleware, cloud computing, software as a service (SaaS) and business process management (BPM). Failure to do so will lead to the proliferation of files moving outside the MFT, such as unsupported FTP, which will increase the chances of failure to achieve compliance efforts, and could lead to the complete failure of an MFT project.

Scenarios for MFT Suite Deployments

Gartner sees three major scenarios for which MFT suites are being deployed:

- Connectivity with external partners
- Internal connectivity between various operating systems and hardware
- Management and security of file movement for collaborative purposes

Connectivity With External Partners

Here, MFT generally replaces FTP and e-mail transfers. It offers templates for rapid onboarding and self-service for partners. MFT comes with reporting and group administration features to manage large groups of users. It also provides SLA reporting for the business and its partners.

Companies that want to use an MFT suite for this purpose generally ask:

- How can we be sure that our data was sent or received?
- How can we integrate this file transfer with the rest of our IT infrastructure?
- How can we achieve the auditability that's necessary for SOX or HIPAA compliance?
- How can we be sure that our data is secured at the termination points of the file transfer?

Internal Connectivity Between Various Operating Systems and Hardware

MFT can secure internal file transfer from A2A and from operating system to operating system. It can replace unsecured and unmanaged HTTP, FTP, or physical media transfer, such as backup tapes. MFT enables the management of all internal connections, makes workflows visible and helps business process improvement (BPI) efforts.

An example of this could be as files are received, rules would ensure that the file is routed to the correct server for processing, and then testing is undertaken to ensure that the file is ready for the next stage. This can be done without human intervention, because checkpoints exist between transfers to ensure that any errors are identified, at a file transfer level and within the file.

Companies that want to use an MFT suite for this purpose generally ask:

- How can we achieve the auditability that's necessary for SOX or HIPAA compliance?
- How can we secure the transfer between System A and System B?
- How can we more easily centralize the automation, integration and monitoring of all file transfers?
- How effectively can checkpoint/restart help us avoid having to retransmit if communication errors occur?

Management and Security of File Movement for Collaborative Purposes

Many organizations use e-mail as a means of exchanging large files with internal and external partners. However, companies often limit the size and type of attachment for security reasons, and to protect the performance of e-mail systems. MFT enables encryption and secure alternative delivery mechanisms for e-mail. Organizations can use plug-ins to integrate MFT with applications that require files to be moved on and off these systems, to provide full governance of file transfers.

Companies that want to use an MFT suite for this purpose generally ask:

- How can we monitor file attachments in e-mail with the least amount of disruption to our organization?
- What mechanism can we offer our organization for file exchanges when we start blocking various e-mail attachments due to size and security concerns?
- How can we be sure that our file transfers were received?
- How can we audit various file transfers and report the results?

As we have seen during the past few years, there has been a trend of MFT consolidating:

“IBM Makes a Big B2B Play With Strategic Potential as It Acquires Sterling Commerce”

“Ipswitch Buys MessageWay to Expand Beyond MFT Solutions”

“Tibco Buys Proginet to Add MFT Solutions to Product Portfolio”

Gartner expects some vendors to develop a full MFT solution, which will incorporate external file transfer and internal and collaboration features that will take advantage of cloud and SOA. This will enable companies to consolidate and centralize most internal and external communication. From the perspective of the B2B gateway, this means including compression, encryption, and stop and restart functionality in the gateway. From the perspective of the MFT suite, this means including trading partner management, at a minimum. Internal, e-mail and files (bulk data) moving from one application to the next thus can be governed.