IPSWITCH FILE TRANSFER
DATASHEET

MOVEit®
FILE TRANSFER (DMZ)

IPSWITCH
FILE TRANSFER

MOVEit™ File Transfer (DMZ)
High Availability and Scalability

A growing number of organisations require mission-critical solutions be available 24/7. MOVEit™ has a flexible architecture that delivers flexible scalability, high availability and turnkey disaster recovery to geographically disperse locations. This document provides an overview of MOVEit File Transfer (DMZ), how its high-availability and disaster recovery capabilities work, and what resources are required to implement them.

Tiered Architecture, Web Farm Support and Disaster Recovery

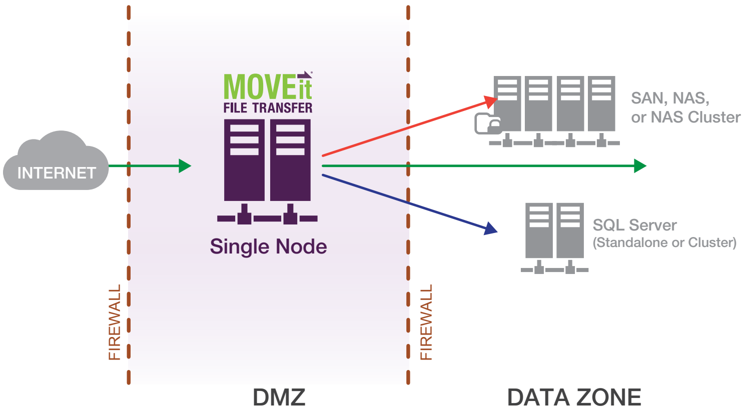
MOVEit File Transfer has a flexible architecture designed for high availability systems and via integration with Neverfail IT Continuity Engine supports disaster recovery and failover configurations. It can be deployed on two or more systems and in various configurations depending on your business, technology, and security requirements. Below is a table identifying various configurations supported by MOVEit File Transfer and the business requirement that might determine each configuration.

CONFIGURATION	BUSINESS REQUIREMENT	MOVEit FILE TRANSFER (DMZ)	DETAILS
Tiered Architecture Deployment	Security and IT Policy	1 Production Server	Can deploy MOVEit File Transfer, file system, and database on three different servers as part of a segmented network
Web Farm	Performance and Scalability	2 or more Production Servers	Use load balancer or application nodes to distribute load across multiple MOVEit instances
Disaster Recovery and Failover	DR/Failover only (not scalability)	1 Production Server 1 Disaster Recovery Server	Requires NeverFail IT Continuity Engine.

Tiered Architecture

Tiered architecture enables the deployment of MOVEit File Transfer in a distributed configuration, with the application, database, and file system running on different machines. This configuration is flexible and can expand to provide increased file transfer performance and availability.

A deployment with a single application node (one MOVEit File Transfer application) provides increased security by segmenting the database and file system components on different servers. Files and permissions/configuration data are moved off the public DMZ. A multi-tier deployment can also leverage infrastructure by integrating MOVEit File Transfer with existing database servers and SAN/NAS storage servers.



MOVEit File Transfer Enterprise Tiered Architecture Deployment

WARNING: Many single-box NAS devices may not be resilient due to a lack of redundant power supplies, NICs, RAID drives, etc. — making such devices a potential single point of failure.

Web Farms

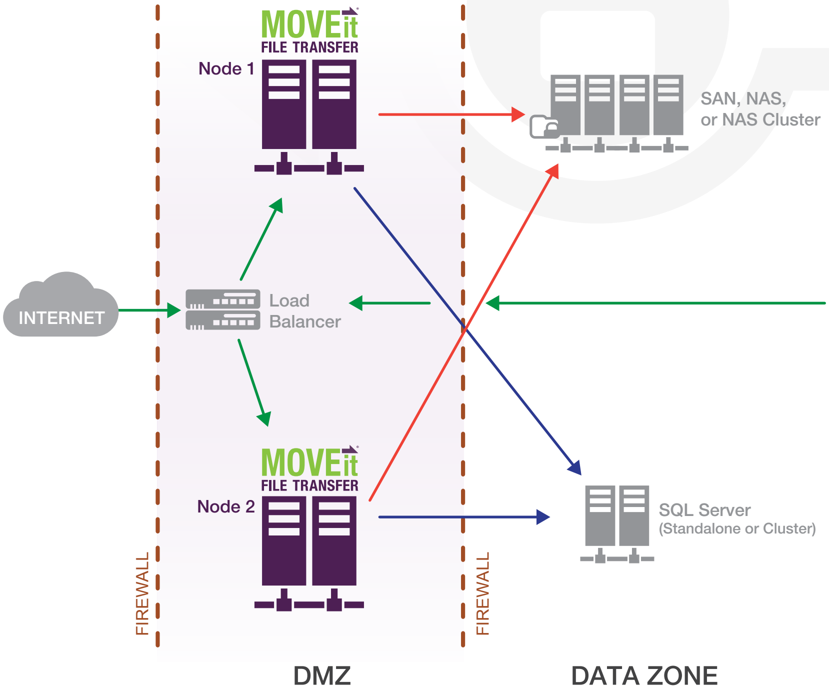
A deployment with multiple MOVEit File Transfer (DMZ) nodes (a Web Farm) increases performance and availability by distributing the file transfer load. The Web Farm deployment is described in the following sections.

Configuring a Web Farm requires planning and preparation for installation. Ipswitch File Transfer offers the necessary training and provides the option of sending a senior MOVEit technical support person onsite to do this work.

While you can have a single node multi-tier configuration, a Web Farm configuration requires a minimum of two identical MOVEit File Transfer production licenses, each with the same number of organisations and options (including API Interface and Ad Hoc packages).

Acquisition of two or more MOVEit File Transfer licenses permits the licensee to use the required "MOVEit File Transfer Web Farm" application without charge.

A MOVEit File Transfer Web Farm can be implemented using any combination of physical or virtual systems (Microsoft Hyper-V and VMware ESX are both supported for this purpose).



MOVEit Two Node Web Farm Deployment

Web Farm Data Storage

The MOVEit File Transfer (DMZ) Web Farm software allows multiple application nodes (MOVEit File Transfer DMZ applications) to use shared data storage locations, possibly located on a LAN segment separate from your File Transfer zone. User, file and folder meta-data, and the audit log are stored in MOVEit File Transfer (DMZ)'s SQL server database, which can be on one host. Encrypted files and debug files are stored in the FileSystem, which can be on another system. Heavily accessed global settings are stored in the registry on the DMZ nodes and replicated across nodes through the database.

High Availability and Performance

The distributed deployment of MOVEit File Transfer components provides a means to scale availability and increase performance by adding application nodes to the Web Farm. High availability can be gained by eliminating single points of failure through clustering multiple database nodes and multiple filesystem nodes. The MOVEit File Transfer Web Farm operates as a single MOVEit File Transfer (DMZ) system that handles all client requests, and coordinates data across the nodes.

Load Balancer (LB) Requirements

High Availability utilises a separate third-party LB hardware device. When deploying a separate LB hardware device, the following criteria should be considered: If FTP and SFTP are required, then the LB must be able to direct each connection's traffic to the same MOVEit File Transfer (DMZ) node for the entire communication. This is sometimes called "sticky" connections.

Additional criteria to consider when selecting an LB is its ability to handle certain types of traffic from the MOVEit nodes, including SMTP notifications, LDAP and RADIUS queries, as well as packets from any third-party monitoring tools that are being used.

Network Address Storage (NAS) Requirements

High Availability requires use of a third-party NAS device to store the files uploaded to it. The NAS is used to store the files that are uploaded to each of the MOVEit File Transfer (DMZ) nodes. (Before being stored, each file is protected by MOVEit File Transfer (DMZ) using its built-in FIPS 140-2 validated 256-bit AES encryption, with each file having its own key, which is itself encrypted.

If an existing internal NAS will be used as part of the MOVEit File Transfer (DMZ) setup, then it will be necessary to determine the minimum number of firewall rules required to let the MOVEit File Transfer (DMZ) nodes communicate with the internal NAS from inside the firewall's DMZ segment.

Storage Area Network (SAN) Option

High Availability can support using a SAN to store the MOVEit File Transfer (DMZ) AES-encrypted files. Doing so does not involve paying a separate MOVEit license or maintenance fee.

Using a SAN requires using an intermediate machine configured to act as a NAS interface. For example, if a configuration calls for two MOVEit File Transfer (DMZ) nodes, and a fiber SAN attachment is available, then a third box should be set up to connect to the SAN (via fibre) and to share the SAN drive with MOVEit File Transfer (DMZ) Primary and Secondary nodes. This enables the SAN to be used as if it were a NAS device.

WARNING: The system sharing the SAN drive should be equipped with features like redundant power supplies and NICs.

WARNING: Many single-box Load Balancing devices may lack redundant power supplies, NICs, RAID drives, etc. — which means such devices are a potential single point of failure.

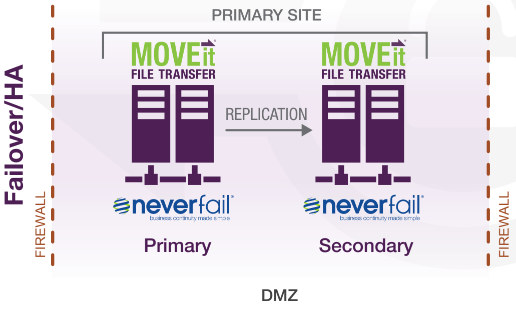
Disaster Recovery and Failover

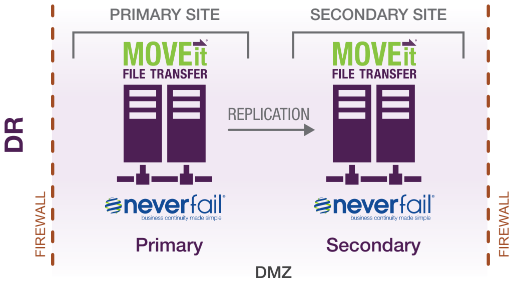
Deployment with MOVEit File Transfer and Neverfail IT Continuity Engine delivers complete continuous availability for high availability to either disaster recovery (multi-site) or local failover (single site) server. It offers these benefits:

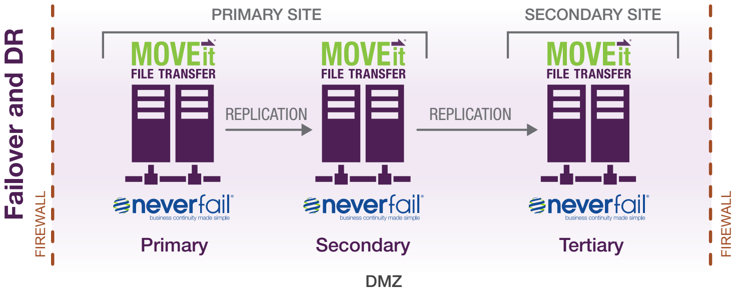
- Real-time replication of data to a 'hot-standby' DR/failover server ensuring file transfer services are always available
- Failover rules monitor performance metrics on production server and can perform switchover to a hot-standby before downtime
- Fully automated failover with Recovery Time Objectives (RTO) of less than a minute and Recovery Point Objectives (RPO) of seconds.
- Protects against the impact of hardware or application failure

IT Continuity Engine maintains multiple synchronised instances of MOVEit File Transfer Server (DMZ) and automatically monitors application health in real-time to identify and fix problems before they cause downtime. If a site-level disaster strikes, Neverfail delivers rapid site-to-site (or on-site) failover to keep businesses running. It incorporates a full range of technologies required to deliver continuous availability: real-time application monitoring, run-time system remediation with failover/failback automation, data replication, cross-platform support and WAN acceleration. The WAN acceleration technology with real-time data de-duplication reduces replication volumes by up to 80 percent.

Both a disaster recovery (multi-site) or failover (single site) configuration requires a MOVEit File Transfer production license and MOVEit File Transfer Disaster Recovery License, each with the same number of modules (including Ad Hoc, Mobile and API Interface modules) and multi-tenant organisations. It also requires complete replication of the local database and file store for both single and multi site configurations.







Deployment can be configured in any of the following topologies (as shown in the diagrams):

- Failover/HA (single site)
- Disaster recovery (multi-site)
- Failover and DR (local failover with remote DR)

Database Options

Microsoft SQL Server. See MOVEit File Transfer (DMZ) supported databases for supported versions and editions of Microsoft SQL Server. Microsoft SQL Server Cluster is recommended for High Availability configurations.

System Requirements

Each MOVEit File Transfer DMZ node must be using the same MOVEit File Transfer version (v.6.0 or higher required) and the identical MOVEit "Add to Web Farm" utility version. See MOVEit File Transfer (DMZ) system requirements for the list of supported platforms.

Please refer to the Ipswitch support website for further information on hardware and software system requirements.

IPSWITCH
FILE TRANSFER

www.IpswitchFT.com

Copyright © 2014 Ipswitch, Inc. All rights reserved. MOVEit is a registered trademark of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective holders.