

MOVEIT DMZ: HIGH AVAILABILITY AND SCALABILITY

A growing number of organizations are requiring that all mission-critical enterprise-level solutions be deployed on multiple, tiered systems — with automatic failover between them — in order to help guarantee continuous 24/7 availability. This document provides an overview of MOVEit DMZ, how its built-in failover capabilities work, and what resources are required to implement them. (A separate similar document is available for the MOVEit Central managed file transfer workflow engine.)

PRODUCT OVERVIEW

MOVEit DMZ is a highly secure enterprise data transfer server which boasts end-to-end encrypted transfer and storage of data and files and delivers powerful administration and reporting capabilities.

MOVEit DMZ runs as a Windows service and enables the encrypted transfer and storage of files, messages, and Web form postings. It provides a secure portal for exchanging sensitive data using a variety of MOVEit and third-party clients that use the secure AS2 or AS3 protocols, the secure HTTP (HTTPS) that Web browsers and MOVEit clients use, or the secure FTP over SSH2 (SFTP / SCP2) or secure FTP over SSL (FTPS / TLS) methods.

Designed as a security solution, MOVEit DMZ has its own built-in authentication and access controls, and an integrated FIPS 140-2 validated cryptographic module with 256-bit AES encryption that it uses to safely store each file received. This means the security of MOVEit DMZ, and the files it handles, does not depend on the security (or lack thereof) of the underlying operating system.

In addition to file non-repudiation and guaranteed delivery, MOVEit DMZ offers an extensive feature set that provides advanced integration and operational flexibility, including the following: multi-factor authentication, external authentication via LDAP, Secure LDAP and RADIUS protocols, email file arrival notification, easy-to-use secure administrative and end-user interfaces, secure messaging, user groups, user aging, extensive audit trail and reporting capabilities, an API interface, and English, French and Spanish end-user interfaces. MOVEit DMZ has a flexible architecture that allows for several deployment configurations including a single server or across many servers in a segmented network or a web farm.

IMPLEMENTING HIGH AVAILABILITY

MOVEit DMZ has a flexible architecture designed for high availability systems. It can be deployed on a two or more boxes and in various configurations depending on your business, technology, and security requirements. Below is a table identifying various configurations supported by MOVEit DMZ and the business requirement behind why each would be used.

Configuration	Business Requirement	MOVEit DMZ Nodes (#)	Details
Resiliency	Failover and Scalability	2 Active	Automatic failover that's built into MOVEit DMZ
Tiered Architecture Deployment	Security and IT Policy	1 or more Active	Can deploy MOVEit DMZ, file system, and database on three different servers as part of a segmented network
Web Farm	Performance and Scalability	2 or more Active	Use load balancer or clustering to distribute load across multiple MOVEit DMZ's

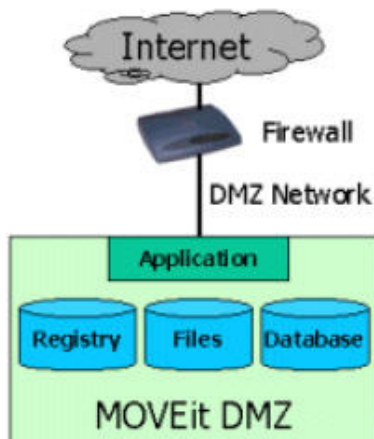
RESILIENCY

Configuring resiliency is different than deploying MOVEit DMZ on a standalone basis. MOVEit DMZ resiliency 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.

Each MOVEit DMZ license permits the software to be run on one production system and on one non-production system (the latter is typically used for training, development/QA, or at a DR site). Resiliency requires a minimum of two identical MOVEit DMZ production licenses, each with the same number of organizations and options (including API Interface, External Authentication, Secure Messaging, and Multi-lingual Interface options). Acquisition of two or more MOVEit DMZ licenses permits the licensee to use the required "MOVEit DMZ Resiliency" application without charge.

MOVEit DMZ resiliency can be implemented using any combination of physical or virtual systems (Microsoft Virtual Server and VMware ESX are both supported for this purpose).

Each MOVEit DMZ node must be running under Windows 2003 or Windows 2008 (32-bit), be using the same MOVEit DMZ version (v.5.2 or higher recommended) and the identical "MOVEit DMZ Resiliency" program version. A special license key is needed to implement the MOVEit DMZ failover and scalability capabilities.

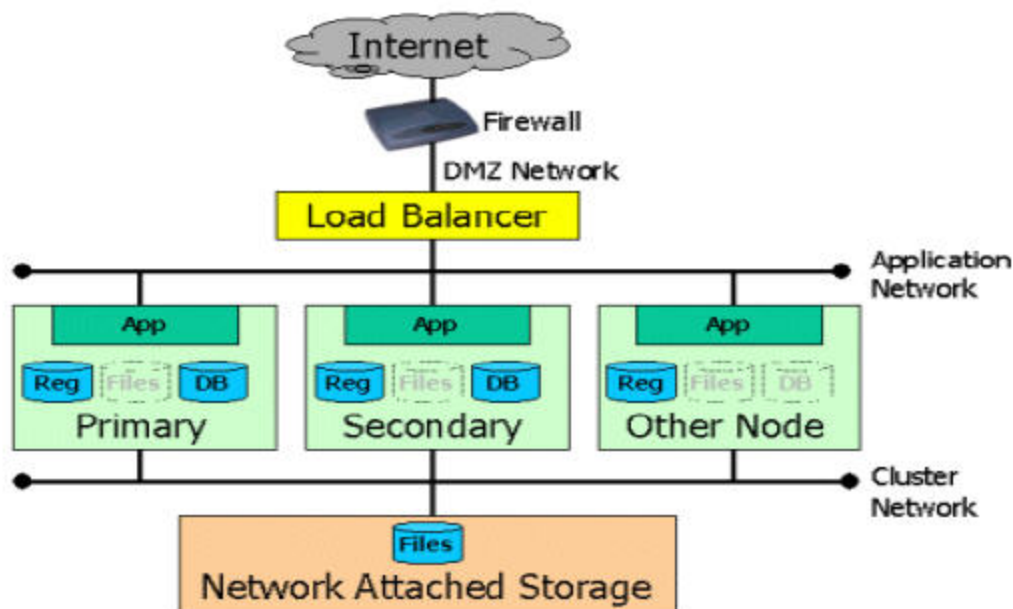


DATA STORAGE

MOVEit DMZ stores data in three main locations. Heavily-accessed global settings are stored in the registry. Encrypted files, debug files, and web content are stored in the FileSystem. User, file and folder data, and the audit log are stored in MOVEit DMZ's ODBC-compliant database. When MOVEit DMZ is deployed on a standalone basis, each of these is located on the same host.

RESILIENCY DATA STORAGE

The MOVEit DMZ resiliency software replicates data amongst the systems involved and detects failures in order to insure that the MOVEit DMZ services can survive the loss of any individual component. This resiliency is built-into MOVEit DMZ and is independent of third party applications.



FAILOVER RESPONSIBILITIES

The MOVEit DMZ Primary node handles all database updates, fields all database queries, and passes all database changes to the Secondary node. (Note: While additional "Other" MOVEit DMZ nodes can be added for increased scalability, they will play no role in database replication.)

HERE IS WHAT WILL HAPPEN AUTOMATICALLY IF THE FOLLOWING MOVEIT DMZ NODES FAIL.

If the Primary node goes down, then the Secondary node will take the Primary's place within approximately 30 seconds. All transfer services (HTTPS, FTPS and SFTP/SCP2) will automatically be switched over, though the dead Primary node's existing connections/sessions will not survive the handover.

If the Secondary node goes down, but the Primary node is up, then the Primary will automatically queue updates for the Secondary and deliver them once the Secondary is either replaced or returned to service.

If an additional ("Other") node goes down, but the Primary node is up, then the Primary will automatically refresh the additional node with configuration information once it is either replaced or returned to service.

To enable this, a “MOVEit DMZ Database Resiliency” service runs on the Primary and Secondary, and a “MOVEit DMZ Web Resiliency” service runs on all the MOVEit DMZ nodes.

(Note: MOVEit DMZ Resiliency will automatically replicate any applicable registry changes from the box on which they are made to all other nodes.)

LOAD BALANCER (LB) REQUIREMENTS

MOVEit DMZ Resiliency requires use of either a separate third-party LB hardware device or the native Network Load Balancing Services (NLBS) in Windows 2003 and Windows 2008 (32-bit), which MOVEit DMZ runs on.

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.

If electing to use a separate LB hardware device, the following criteria should be considered.

- **If FTSP is Required**, then the LB must be able to direct traffic from the multiple ports used by FTP over SSL clients to a single MOVEit DMZ node.
- **If FTSP is Not Needed**, then the LB must only be able to direct traffic from the single port used by SFTP, SCP2 and HTTPS client to the same MOVEit DMZ node.

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

Note: If using remote management tools (such as Microsoft Windows Terminal Services, etc.), then it will be helpful if the LB can expose each MOVEit DMZ node as a separate IP address to your internal network, and the entire resilient array to the outside as a single virtual MOVEit DMZ.

NETWORK ADDRESS STORAGE (NAS) REQUIREMENTS

MOVEit DMZ resiliency requires use of a third-party NAS device to store the files uploaded to it.

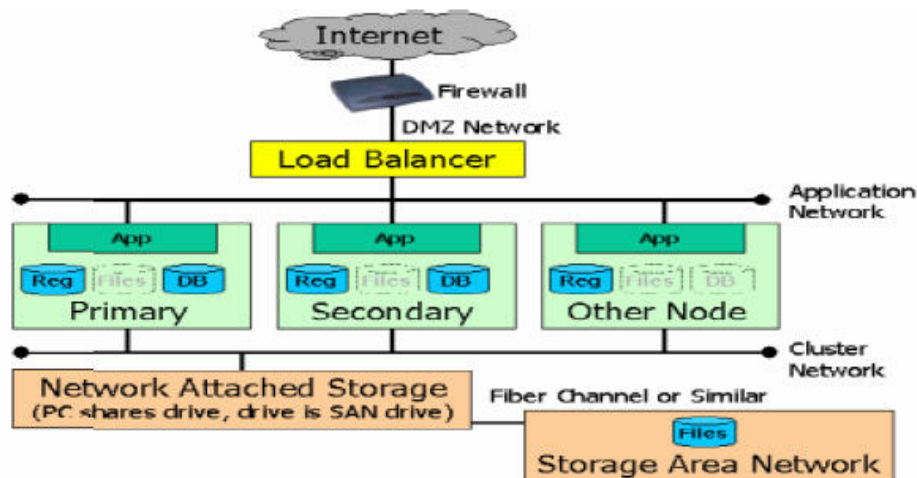
The NAS is used to store the files that are uploaded to each of the MOVEit DMZ resilient nodes. (Before being stored, each file is protected by MOVEit DMZ using its built-in FIPS 140-2 validated 256-bit AES encryption, with each file having its own key, which is itself encrypted.

WARNING: Almost any NAS available today can support MOVEit DMZ resiliency, but 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.

If an existing internal NAS will be used as part of the MOVEit DMZ resilient setup, then it will be necessary to determine the minimum number of firewall rules required to let the MOVEit DMZ nodes communicate with the internal NAS from inside the firewall's DMZ segment. In a worst-case scenario, this may be “whatever is needed to support IPSec.”

STORAGE AREA NETWORK (SAN) OPTION

MOVEit DMZ Resiliency can support using a SAN to store the MOVEit 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 DMZ resilient nodes, and a fiber SAN attachment is available, then a third box should be set up to connect to the SAN (via fiber) and to share the SAN drive with MOVEit 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 resilient features like redundant power supplies and NICs, but may not need large local or RAID hard drives because it will only be a pass-through device.

TIERED ARCHITECTURE & WEB FARM SUPPORT

Tiered architecture enables the deployment of MOVEit DMZ 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..

TIERED ARCHITECTURE

A deployment with a single application node (one MOVEit DMZ application) provides increased security by segmenting the database and filesystem 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 DMZ with existing database servers and SAN/NAS storage servers.

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

WEB FARMS

As with Resiliency, 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 DMZ production licenses, each with the same number of organizations and options (including API Interface, External Authentication, Secure Messaging, and Multi-lingual Interface

options). Acquisition of two or more MOVEit DMZ licenses permits the licensee to use the required “MOVEit DMZ Web Farm” application without charge.

A MOVEit DMZ web farm can be implemented using any combination of physical or virtual systems (Microsoft Virtual Server and VMware ESX are both supported for this purpose).

Each MOVEit DMZ node must be running under Windows 2003 or Windows 2008 (32-bit), be using the same MOVEit DMZ version (v.6.0 or higher required) and the identical MOVEit DMZ “Add to Web Farm” utility version.

WEB FARM DATA STORAGE

The MOVEit DMZ web farm software allows multiple application nodes (MOVEit DMZ applications) to use one data storage location. User, file and folder data, and the audit log are stored in MOVEit DMZ’s ODBC-compliant database, which can be on one host. Encrypted files, and debug files are stored in the FileSystem, which can be on another host. Heavily-accessed global settings are stored in the registry on the DMZ node and replicated across nodes through the database. Web content is stored on the DMZ node and replicated across nodes through the database.

HIGH AVAILABILITY AND PERFORMANCE

The distributed deployment of MOVEit DMZ components with access controlled by a third-party load balancer provides a means to scale availability and increase performance by adding application nodes to the web farm. High availability can be gained by clustering multiple database nodes and multiple filesystem nodes. The MOVEit DMZ web farm operates as a single MOVEit DMZ that handles all client requests, and coordinates data across the nodes.

Load Balancer, Network Address Storage (NAS), and Storage Area Network (SAN) requirements are the same as those identified for the Resiliency software.

MOVEit DMZ technical questions can be directed to the MOVEit support staff at Ipswitch. Please contact the Ipswitch MOVEit sales staff for MOVEit DMZ licensing and pricing information.



Ipswitch

10 Maguire Road • Lexington, MA 02421

MOVEit: (608) 824 3600 • moveitinfo@ipswitch.com