

## MOVEIT DMZ ENTERPRISE ENTERPRISE: 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 Enterprise, how its built-in failover capabilities work, and what resources are required to implement them.

### IMPLEMENTING HIGH AVAILABILITY

MOVEit DMZ Enterprise 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 Enterprise and the business requirement behind why each would be used.

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

### RESILIENCY

Configuring resiliency is different than deploying MOVEit DMZ Enterprise on a standalone basis. MOVEit DMZ Enterprise 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 Enterprise 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 Enterprise 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 Enterprise licenses permits the licensee to use the required “MOVEit DMZ Enterprise Resiliency” application without charge.

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

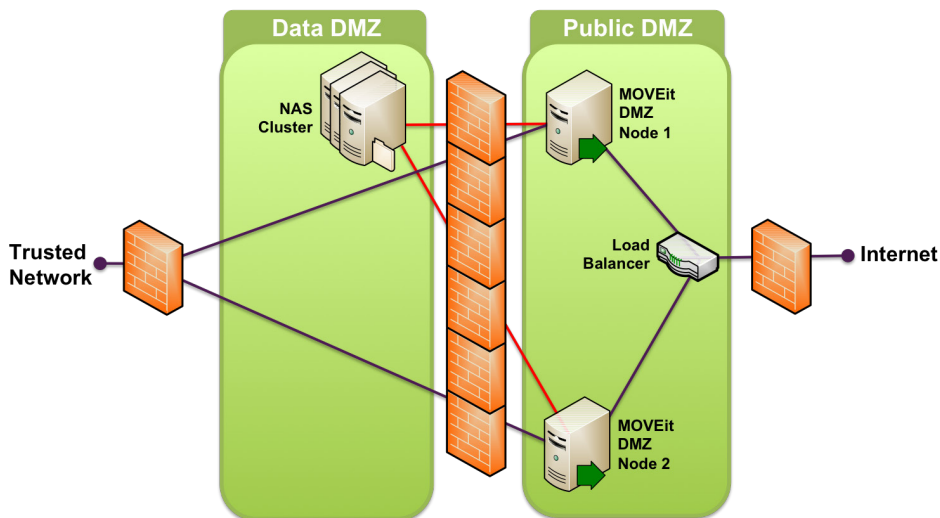
Each MOVEit DMZ Enterprise node must be running under Windows 2003 or Windows 2008 (32-bit), be using the same MOVEit DMZ Enterprise version (v.5.2 or higher recommended) and the identical “MOVEit DMZ Enterprise Resiliency” program version. A special license key is needed to implement the MOVEit DMZ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

### DATA STORAGE

MOVEit DMZ Enterprise 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 Enterprise’s ODBC-compliant database. When MOVEit DMZ Enterprise is deployed on a standalone basis, each of these is located on the same host.

### RESILIENCY DATA STORAGE

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



MOVEit DMZ Enterprise One Node Multi-Tier Deployment

## FAILOVER RESPONSIBILITIES

The MOVEit DMZ Enterprise 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 Enterprise nodes can be added for increased scalability, they will play no role in database replication.)

## AUTOMATIC RESPONSE IF MOVEIT DMZ ENTERPRISE 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 Enterprise Database Resiliency” service runs on the Primary and Secondary, and a “MOVEit DMZ Enterprise Web Resiliency” service runs on all the MOVEit DMZ Enterprise nodes.

(Note: MOVEit DMZ Enterprise 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 Enterprise 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 Enterprise runs on.

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

- **If FTPS 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 Enterprise node.
- **If FTPS 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 Enterprise node.

Additional criteria to consider when selecting an LB is its ability to handle certain types of traffic from the MOVEit DMZ Enterprise 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 Enterprise node as a separate IP address to your internal network, and the entire resilient array to the outside as a single virtual MOVEit DMZ Enterprise.

**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.**

## NETWORK ADDRESS STORAGE (NAS) REQUIREMENTS

MOVEit DMZ Enterprise 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 Enterprise resilient nodes. (Before being stored, each file is protected by MOVEit DMZ Enterprise 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 DMZ Enterprise resilient setup, then it will be necessary to determine the minimum number of firewall rules required to let the MOVEit DMZ Enterprise 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 Enterprise Resiliency can support using a SAN to store the MOVEit DMZ Enterprise 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 Enterprise 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 Enterprise Primary and Secondary nodes. This enables the SAN to be used as if it were a NAS device.

**WARNING:** Almost any NAS available today can support MOVEit DMZ Enterprise 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.

## TIERED ARCHITECTURE & WEB FARM SUPPORT

Tiered architecture enables the deployment of MOVEit DMZ Enterprise 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 Enterprise 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.

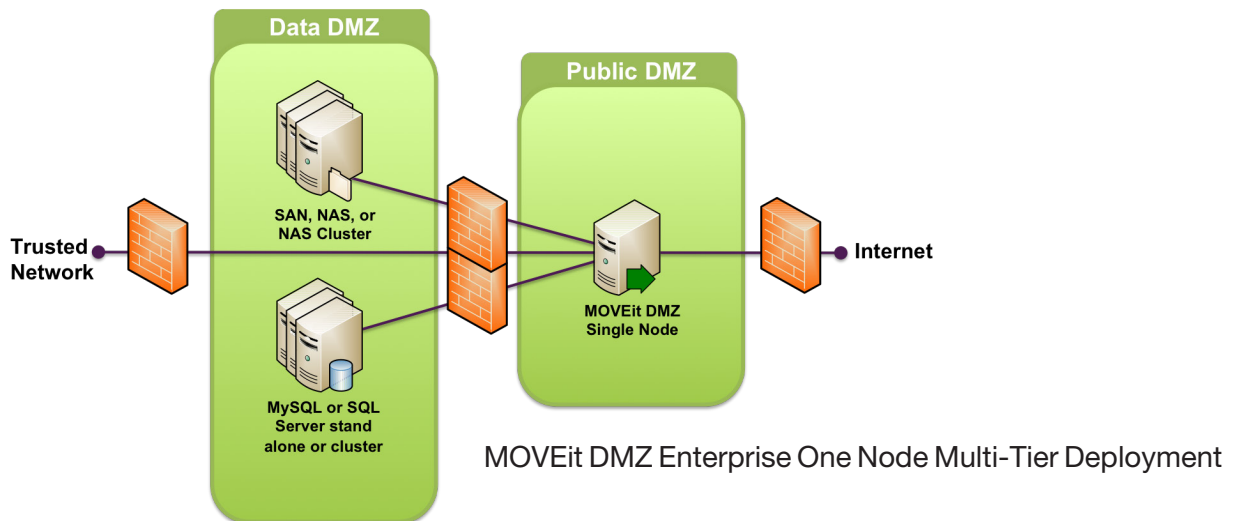
A multi-tier deployment can also leverage infrastructure by integrating MOVEit DMZ Enterprise with existing database servers and SAN/NAS storage servers.

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

**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.

### WEB FARMS

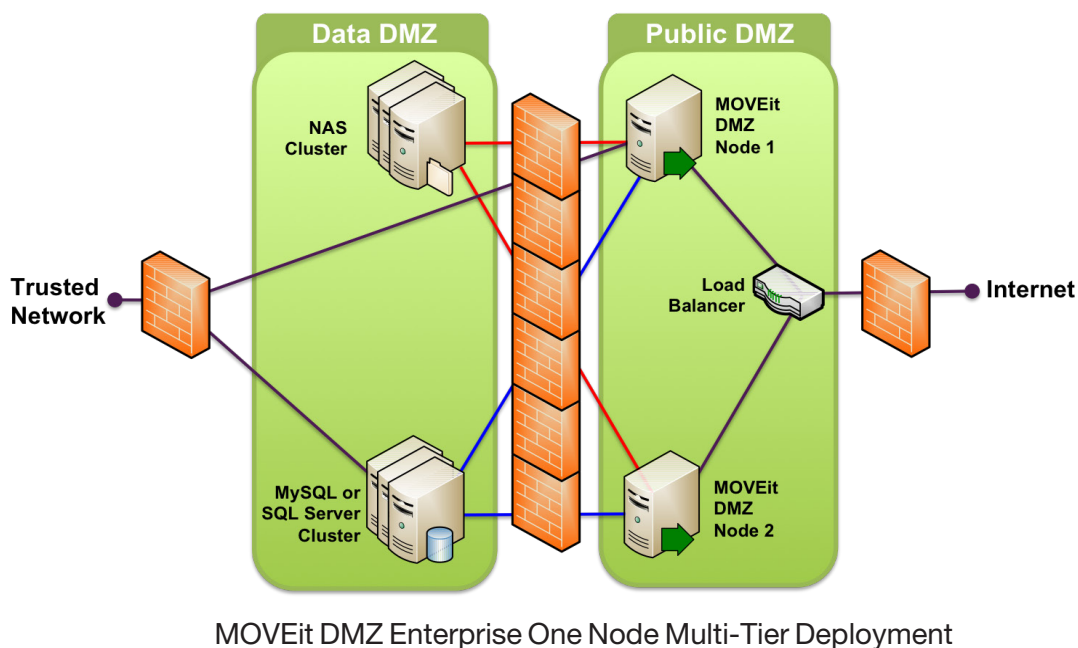
As with Resiliency, configuring a web farm requires planning and preparation for installation. Ipswitch File Transfer offers the necessary training and provides the option of sending a senior MOVEit technical support person onsite to do this work.



While you can have a single node multi-tier configuration, a web farm configuration requires a minimum of two identical MOVEit DMZ Enterprise 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 Enterprise licenses permits the licensee to use the required “MOVEit DMZ Enterprise Web Farm” application without charge.

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



## WEB FARM DATA STORAGE

The MOVEit DMZ Enterprise web farm software allows multiple application nodes (MOVEit DMZ Enterprise applications) to use one data storage location. User, file and folder data, and the audit log are stored in MOVEit DMZ Enterprise'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 Enterprise 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 Enterprise web farm operates as a single MOVEit DMZ Enterprise 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.

To learn more, please visit [www.lpswitchFT.com](http://www.lpswitchFT.com).

