



Failover and Scalability

The MOVEit DMZ secure file transfer server software has a well-earned reputation for reliability. It is also known for making efficient use of available system hardware and software resources. Nevertheless, some organizations require that their mission-critical enterprise-level solutions be deployed on multiple systems — with automatic failover and scalability — in order to help guarantee continuous 24/7 availability. This document provides an overview of MOVEit DMZ, how its built-in high availability capabilities work, and the resources required to implement them. (A separate similar document is available for the MOVEit Central file transfer management client.)

Product Overview

MOVEit DMZ server is an enterprise-level solution that 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 wide variety of MOVEit and third-party clients that use any of these popular protocols: secure HTTP (HTTPS) used by Web browsers and MOVEit clients, secure FTP over SSH2 (SFTP/SCP2) and various flavors of secure FTP over SSL (FTPS).

Designed as a security solution, 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 Notification, Secure Messaging, User Aging, Extensive Audit Trail and Reporting capabilities, an API XML Machine Interface, and English, French and Spanish language end-user interfaces.

Implementing Resiliency

Configuring resiliency is substantially different than deploying MOVEit DMZ on a standalone basis. MOVEit DMZ resiliency requires prior planning and up to four days of installation and training. Standard Networks strongly recommends one of our technicians be brought onsite to do this work.

Each MOVEit DMZ license permits the software to be run on one production system and one non-production system (with the latter typically used for training, development/QA or at a DR site). Resiliency requires a minimum of two identical MOVEit DMZ 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 use of 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 by EMC Corporation are both supported for this purpose).

Each MOVEit DMZ node must be running under the same operating system, either Windows 2003 or Windows 2000 Server. Each node must also be using the same version of MOVEit DMZ (3.1 or higher) as well as identical versions of the separate "MOVEit DMZ Resiliency" application. A special license key is needed to implement the MOVEit DMZ failover and scalability capabilities.

"MOVEit" is a registered Trademark and "MOVEit DMZ" is a Trademarks of Standard Networks, Inc.

All other Trademarks are the property of their respective owners. This document Copyright 2004-2006 by Standard Networks, Inc.

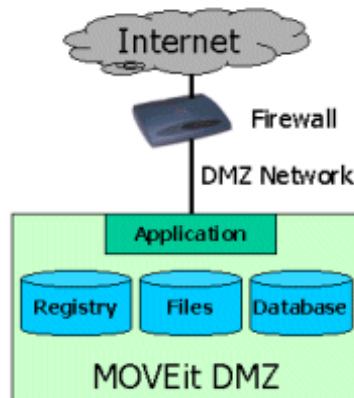
info@standardnetworks.com — 1-608-227-6100 (Central US/GMT-6) — www.standardnetworks.com



Failover and Scalability, Cont.

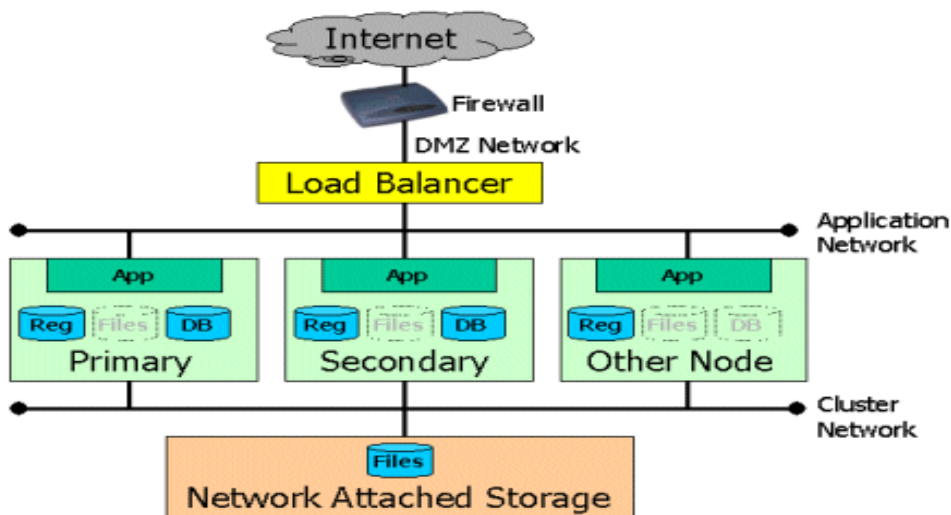
Data Storage

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 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.



"MOVEit" is a registered Trademark and "MOVEit DMZ" is a Trademarks of Standard Networks, Inc.

All other Trademarks are the property of their respective owners. This document Copyright 2004-2006 by Standard Networks, Inc.

info@standardnetworks.com — 1-608-227-6100 (Central US/GMT-6) — www.standardnetworks.com



Failover and Scalability, Cont.

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, which MOVEit DMZ 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 port used by FTP over SSL clients to a single MOVEit DMZ 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 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.

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.

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.



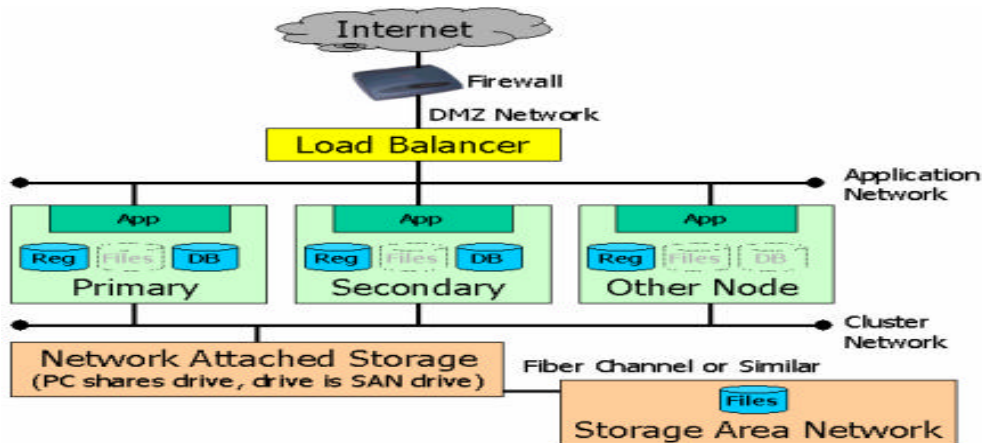
Failover and Scalability, Cont.

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 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 with 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."

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.



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.

Resiliency technical questions can be directed to the MOVEit support staff at Standard Networks. Please contact Standard Networks sales staff for MOVEit DMZ licensing and evaluation information.