IPSWITCH File Transfer

MOVEIT DMZ: HOCHVERFÜGBARKEIT UND SKALIERBARKEIT

Immer mehr Unternehmen möchten sämtliche geschäftskritische Lösungen auf Unternehmensebene in mehreren abgestuften Systemen mit gegenseitiger automatischer Ausfallsicherung implementieren, um eine ständige Verfügbarkeit zu jedem Zeitpunkt sicherzustellen. Dieses Dokument bietet einen Überblick über MOVEit DMZ, seine integrierten Ausfallsicherungsfunktionen und die für die Implementierung erforderlichen Ressourcen. (Für die verwaltete Dateiübertragungslösung und Workflow-Engine MOVEit Central ist ein ähnliches Dokument verfügbar.)

PRODUKTÜBERBLICK

MOVEit DMZ ist ein hoch sicherer Server zur Übertragung von Unternehmensdaten, der die verschlüsselte End-to-End-Übertragung und Speicherung von Daten und Dateien ermöglicht und mit leistungsstarken Verwaltungs- und Berichterstattungsfunktionen aufwartet.

MOVEit DMZ wird als Windows-Dienst ausgeführt und erlaubt die verschlüsselte Übertragung und Speicherung von Dateien, Nachrichten und Beiträgen aus Internetforen. Er bietet ein sicheres Portal für den Austausch vertraulicher Daten über verschiedene Clients von MOVEit und Drittanbietern mit den sicheren Protokollen AS2 oder AS3, dem von Webbrowsern und MOVEit-Clients verwendeten Secure HTTP (HTTPS) oder dem sicheren FTP über SSH2 (SFTP/SCP2) oder FTP über SSL (FTPS/TLS).

Als Sicherheitslösung verfügt MOVEit DMZ über eine eigene Authentifizierungs- und Zugriffssteuerung und ein integriertes, FIPS 140-2-validiertes Kryptographie-Modul mit 256 -Bit-AES-Verschlüsselung, mit dem alle empfangenen Dateien sicher gespeichert werden. Der Vorteil: Die Sicherheit von MOVEit DMZ und den damit bearbeiteten Dateien hängt nicht von der – nicht immer optimalen – Sicherheit des zugrunde liegenden Betriebssystems ab.

Neben der Nicht-Ablehnung und garantierten Lieferung von Dateien bietet MOVEit DMZ umfassende Funktionen zur erweiterten Integration und betrieblichen Flexibilität, einschließlich: Multi-Faktor-Authentifizierung, externe Authentifizierung über LDAP, Secure LDAP- und RADIUS-Protokolle, Benachrichtigung über den Eingang von E-Mail-Dateien, bedienerfreundliche, sichere Verwaltungs- und Benutzerschnittstellen, Secure Messaging, Benutzergruppen, Ablauf nicht genutzter Benutzerkonten, umfassende Prüfungspfad- und Berichterstattungsfunktionen, eine API-Schnittstelle und Benutzeroberflächen in englischer, französischer und spanischer Sprache. Dank der flexiblen Architektur von MOVEit DMZ ergeben sich verschiedene Implementierungsmöglichkeiten – unter anderem mit einem einzigen Server oder über mehrere Server in einem segmentierten Netzwerk oder einer Webfarm.

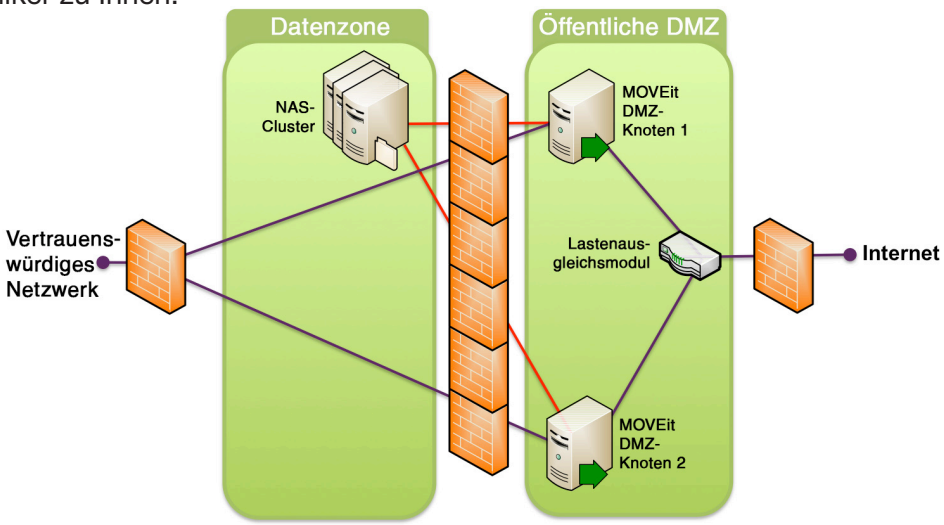
IMPLEMENTIERUNG VON HOCHVERFÜGBARKEIT

Die flexible Architektur von MOVEit DMZ wurde speziell für Hochverfügbarkeitssysteme entwickelt. Abhängig von Ihren Unternehmens-, Technologie- und Sicherheitsanforderungen kann sie auf zwei oder mehr Knoten und in verschiedenen Konfigurationen implementiert werden. In der folgenden Tabelle finden Sie die verschiedenen von MOVEit DMZ unterstützten Konfigurationen und die zugrunde liegenden Unternehmensanforderungen.

Konfiguration	Unternehmensanforderung	MOVEit DMZ-Knoten (Anzahl)	Details
Resiliency	Ausfallsicherheit und Skalierbarkeit	2 aktiv	Automatische, in MOVEit DMZ integrierte Ausfallsicherung
Abgestufte Architektur Implementierung	Sicherheit und IT-Richtlinien	1 oder mehr aktiv	Kann MOVEit DMZ, Dateisystem und Datenbank als Teil eines segmentierten Netzwerks auf drei verschiedenen Servern implementieren
Webfarm	Leistung und Skalierbarkeit	2 oder mehr aktiv	Verwendet Lastenausgleichsmodul oder Clustering zur Lastverteilung auf mehrere MOVEit DMZs

RESILIENCY

Die Konfiguration von Resiliency unterscheidet sich von der Implementierung von MOVEit DMZ auf Standalone-Basis. Die Installation von MOVEit DMZ Resiliency muss geplant und vorbereitet werden. Ipswitch File Transfer bietet entsprechende Schulungen an und sendet auf Wunsch einen erfahrenen MOVEit-Techniker zu Ihnen.



MOVEit DMZ Multi-Tier-Bereitstellung mit einem Knoten

Mit jeder MOVEit DMZ-Lizenz darf die Software auf einem Produktivsystem und einem Testsystem ausgeführt werden. Letztere werden in der Regel für Schulungen, Entwicklung und Qualitätssicherung oder an DR-Standorten eingesetzt. Für Resiliency werden mindestens zwei identische MOVEit DMZ-Produktionslizenzen mit der gleichen Anzahl von Organisationseinheiten und Optionen (einschließlich API-Schnittstelle, externer Authentifizierung, Secure Messaging und mehrsprachigen Benutzeroberflächen) benötigt. Bei Erwerb von zwei oder mehr MOVEit DMZ-Lizenzen kann die erforderliche Anwendung „MOVEit DMZ Resiliency“ kostenlos verwendet werden.

MOVEit DMZ Resiliency kann mit einer beliebigen Kombination aus physischen und virtuellen Systemen verwendet werden. Für diesen Zweck wird sowohl Microsoft Virtual Server als auch Vmware ESX unterstützt.

Alle MOVEit DMZ-Knoten müssen unter Windows 2003 oder Windows 2008 (32 Bit) ausgeführt werden und die gleiche MOVEit DMZ-Version (empfohlen wird v.5.2 oder höher) sowie die gleiche „MOVEit DMZ Resiliency"-Programmversion nutzen. Zur Implementierung der Ausfallsicherheits- und Skalierungsfunktionen von MOVEit DMZ wird ein gesonderter Lizenzschlüssel benötigt.

SPEICHERN VON DATEN

MOVEit DMZ legt Daten an drei Hauptspeicherorten ab: Allgemeine Einstellungen, auf die häufig zugegriffen wird, werden in der Registry gespeichert. Verschlüsselte Dateien, Debug-Dateien und Webinhalte werden im Dateisystem gespeichert. Benutzer-, Datei- und Ordnerdaten sowie das Prüfprotokoll werden in der ODBC-kompatiblen Datenbank von MOVEit DMZ verwahrt. Beim Einsatz von MOVEit DMZ auf Standalone-Basis befinden sich alle diese Speicherorte auf dem gleichen Host.

AUSFALLSICHERES SPEICHERN VON DATEN MIT RESILIENCY

Mit der Software MOVEit DMZ Resiliency werden Daten in den verschiedenen beteiligten Systemen repliziert und Störungen erkannt. So wird sichergestellt, dass die MOVEit DMZ-Dienste bei Ausfall einer einzelnen Komponente weiterhin funktionieren. Diese Funktion zur Ausfallsicherheit ist in MOVEit DMZ integriert und unabhängig von den Anwendungen von Drittanbietern.

AUFGABEN DER AUSFALLSICHERUNG

Über den Primärknoten von MOVEit DMZ werden alle Datenbank-Updates und -abfragen bearbeitet und sämtliche Änderungen der Datenbank an den Sekundärknoten weitergeleitet. (Hinweis: Zwar können zur Verbesserung der Skalierbarkeit zusätzliche „andere" MOVEit DMZ-Knoten hinzugefügt werden; diese spielen bei der Datenbankreplikation jedoch keine Rolle.)

BEIM AUSFALL EINES MOVEIT DMZ-KNOTEN WERDEN AUTOMATISCH FOLGENDE SCHRITTE AUSGEFÜHRT:

Wenn der Primärknoten ausfällt, werden seine Aufgaben innerhalb von 30 Sekunden vom Sekundärknoten übernommen. Alle Übertragungsdienste (HTTPS, FTPS und SFTP/SCP2) werden automatisch umgeleitet. Bestehende Verbindungen und Sitzungen des ausgefallenen Primärknotens bleiben dabei jedoch nicht erhalten.

Wenn der Sekundärknoten ausfällt, der Primärknoten jedoch aktiv ist, reiht letzterer alle Aktualisierungen für den Sekundärserver automatisch in die Warteschleife ein und liefert sie, sobald der ausgefallene Knoten ersetzt oder der Fehler behoben wurde.

Wenn ein zusätzlicher („anderer") Knoten ausfällt, der Primärknoten jedoch aktiv ist, aktualisiert letzterer den zusätzlichen Knoten automatisch mit Konfigurationsinformationen, sobald dieser ersetzt oder der Fehler behoben wurde.

Zu diesem Zweck wird auf dem Primär- und dem Sekundärknoten ein „MOVEit DMZ Database Resiliency"-Dienst und auf allen MOVEit DMZ-Knoten ein „MOVEit DMZ Web Resiliency"-Dienst ausgeführt.

(Hinweis: MOVEit DMZ Resiliency repliziert relevante Änderungen an der Registry eines Knotens automatisch auf allen anderen Knoten.)

VORAUSSETZUNGEN FÜR LASTENAUSGLEICHSMODULE

MOVEit DMZ Resiliency muss entweder auf einem separaten Lastenausgleichmodul eines Drittanbieters oder auf den nativen Netzwerklastenausgleich-Diensten (NLBS) in Windows 2003 und Windows 2008 (32 Bit) ausgeführt werden.

WARNUNG: Da Komplettgeräte zur Lastverteilung häufig nicht mit redundanten Netzteilen, Netzwerkkarten (NICs), RAID-Festplatten usw. ausgestattet sind, stellen sie einen potenziellen Single Point of Failure dar.

Bei Einsatz eines separaten Lastenausgleichmoduls müssen die folgenden Aspekte berücksichtigt werden:

- **Wenn FTPS erforderlich ist,** muss das Lastenausgleichsmodul in der Lage sein, Datenverkehr von den verschiedenen von den FTP-over-SSL-Clients verwendeten Ports an einen einzigen MOVEit DMZ-Knoten zu leiten.
- **Wenn kein FTPS erforderlich ist,** muss das Lastenausgleichsmodul nur in der Lage sein, Datenverkehr von dem einzelnen vom SFTP-, SCP2- und HTTPS-Client verwendeten Port an den gleichen MOVEit DMZ-Knoten zu leiten.

Weitere Punkte, die bei der Auswahl eines Lastenausgleichsmoduls berücksichtigt werden müssen, sind die Fähigkeit, bestimmte Arten von Datenverkehr von den MOVEit DMZ-Knoten, einschließlich SMTP-Benachrichtigungen, LDAP- und RADIUS-Anfragen sowie Paketen von verwendeten Überwachungstools von Drittanbietern, zu bewältigen.

Hinweis: Bei Verwendung von Remote-Management-Tools wie Microsoft Windows Terminal Services ist es sinnvoll, wenn das Lastenausgleichsmodul jeden MOVEit DMZ-Knoten im internen Netzwerk als separate IP-Adresse und das gesamte ausfallsichere System nach außen als einen virtuellen MOVEit DMZ ausweisen kann.

VORAUSSETZUNGEN FÜR NETWORK ADDRESS STORAGE (NAS)

Zum Speichern der auf MOVEit DMZ Resiliency hochgeladenen Daten wird ein NAS-Gerät eines Drittanbieters benötigt.

Auf diesem werden die Dateien gespeichert, die auf die einzelnen ausfallsicheren MOVEit DMZ-Knoten geladen werden. Vor dem Speichern werden die Dateien mit der integrierten FIPS 140-2-validierten 256-Bit-AES-Verschlüsselung von MOVEit DMZ gesichert, wobei jede Datei über einen eigenen Schlüssel verfügt, der wiederum ebenfalls verschlüsselt ist.

WARNUNG: Obwohl MOVEit DMZ Resiliency inzwischen von fast allen handelsüblichen NAS-Geräten unterstützt wird, sind viele NAS-Komplettlösungen nicht ausfallsicher, da sie nicht mit redundanten Netzteilen, Netzwerkkarten (NICs), RAID-Festplatten usw. ausgestattet sind und damit einen potenziellen Single Point of Failure darstellen.

Wenn ein bestehendes internes NAS Teil der ausfallsicheren MOVEit DMZ-Installation ist, muss die Mindestanzahl der erforderlichen Firewall-Regeln ermittelt werden, damit die MOVEit DMZ-Knoten innerhalb des DMZ-Segments der Firewall mit dem internen NAS kommunizieren können. Im schlimmsten Fall bedeutet dies: „alles, was nötig ist, um IPSec zu unterstützen“.

OPTIONALES STORAGE AREA NETWORK (SAN)

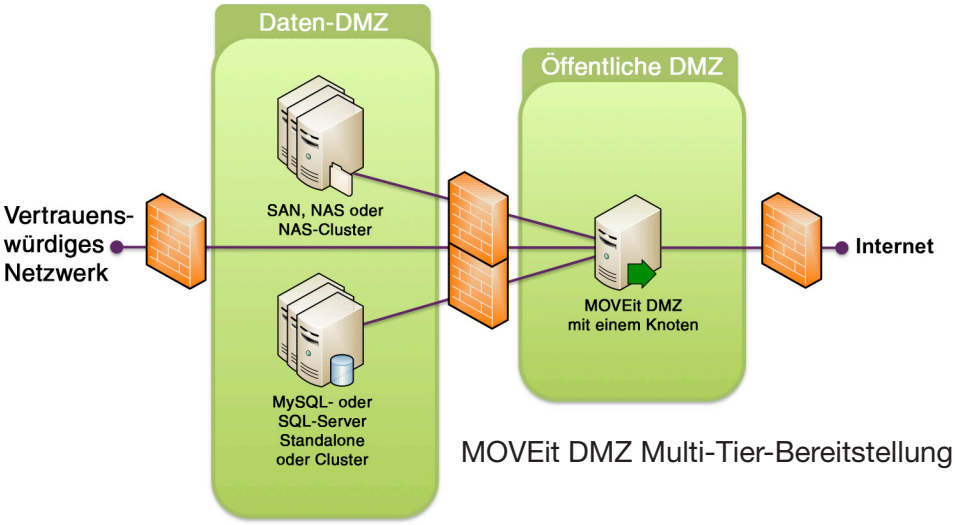
Mit MOVEit DMZ Resiliency können die AES-verschlüsselten Dateien von MOVEit DMZ in einem SAN gespeichert werden. Dabei fallen keine zusätzlichen MOVEit-Lizenz- oder Wartungsgebühren an.

Bei Verwendung eines SAN wird jedoch ein als NAS-Schnittstelle konfigurierter Zwischenrechner benötigt. Wenn eine Konfiguration beispielsweise zwei ausfallsichere MOVEit DMZ-Knoten erfordert und ein Fibre-Channel-SAN verfügbar ist, sollte ein dritter Knoten eingerichtet werden, der über Fibre Channel an das SAN angebunden ist und gemeinsam mit den Primär- und Sekundärknoten von MOVEit DMZ auf die SAN-Festplatte zugreift. Auf diese Weise kann das SAN wie ein NAS-Gerät genutzt werden.

WARNUNG: Das System, mit dem das SAN-Laufwerk geteilt wird, sollte mit ausfallsicheren Komponenten wie redundanten Netzteilen und NICs ausgestattet sein. Lokale oder RAID-Festplatten sind nicht unbedingt erforderlich, da es sich lediglich um ein Durchgangsgerät handelt.

ABGESTUFTE ARCHITEKTUR UND WEBFARM-UNTERSTÜTZUNG

Die abgestufte Architektur ermöglicht die Implementierung von MOVEit DMZ in einer verteilten Konfiguration, bei der Anwendung, Datenbank und Dateisystem auf unterschiedlichen Rechnern ausgeführt werden. Diese flexible Konfiguration lässt sich zur Optimierung der Datenübertragungsleistung und Verfügbarkeit erweitern.



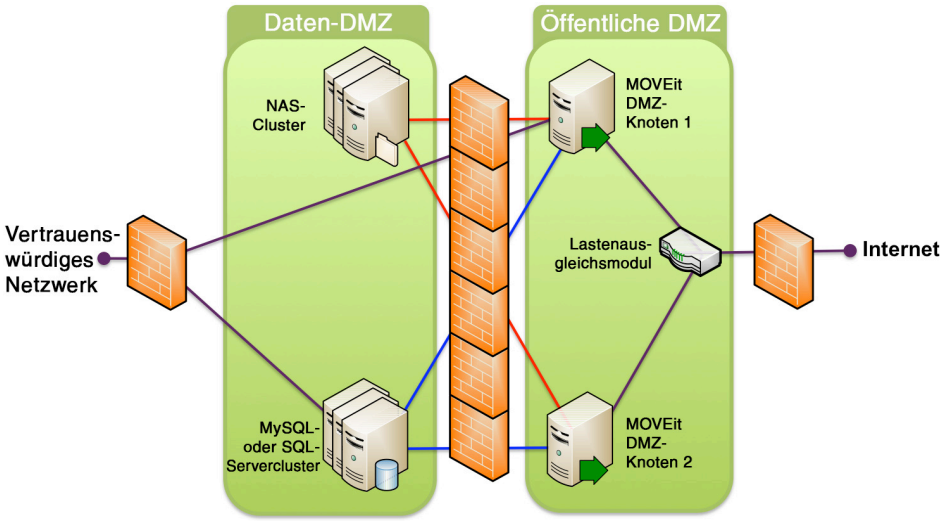
MOVEit DMZ Multi-Tier-Bereitstellung mit einem Knoten

ABGESTUFTE ARCHITEKTUR

Die Implementierung mit einem einzelnen Anwendungsknoten (eine MOVEit DMZ-Anwendung) sorgt für erhöhte Sicherheit, da die Komponenten der Datenbank und des Dateisystems auf unterschiedliche Server aufgeteilt werden. Dateien und Berechtigungen/Konfigurationsdaten werden aus dem öffentlichen DMZ entfernt.

Bei einer abgestuften Implementierung kann auch die Infrastruktur wirksam eingesetzt werden, indem MOVEit DMZ in bestehende Datenbankserver und SAN-/NAS-Speicherserver integriert wird.

Eine Implementierung mit mehreren MOVEit DMZ-Knoten (Webfarm) führt zu einer Verbesserung der Leistung und Verfügbarkeit durch Verteilung der Dateiverarbeitungslast. Der Aufbau der Webfarm wird in den folgenden Abschnitten beschrieben.



MOVEit DMZ Multi-Tier-Bereitstellung mit einem Knoten

WEBFARMEN

Wie bei Resiliency muss auch bei der Konfiguration einer Webfarm die Installation geplant und vorbereitet werden. Ipswitch File Transfer bietet entsprechende Schulungen an und sendet auf Wunsch einen erfahrenen MOVEit-Techniker zu Ihnen.

Während eine mehrstufige Konfiguration mit einem einzelnen Knoten möglich ist, werden bei einer Webfarm mindestens zwei identische MOVEit DMZ-Produktionslizenzen mit der gleichen Anzahl von Organisationseinheiten und Optionen (einschließlich API-Schnittstelle, externer Authentifizierung, Secure Messaging und mehrsprachigen Benutzeroberflächen) benötigt. Bei Erwerb von zwei oder mehr MOVEit DMZ-Lizenzen kann die erforderliche Anwendung „MOVEit DMZ Web Farm" kostenlos verwendet werden.

MOVEit DMZ-Webfarmen können mit einer beliebigen Kombination aus physischen und virtuellen Systemen verwendet werden. Für diesen Zweck werden sowohl Microsoft Virtual Server als auch Vmware ESX unterstützt.

Alle MOVEit DMZ-Knoten müssen unter Windows 2003 oder Windows 2008 (32 Bit) ausgeführt werden und die gleiche MOVEit DMZ-Version (v.6.0 oder höher) sowie die gleiche MOVEit DMZ „Add to Web Farm"-Dienstprogrammversion nutzen.

SPEICHERN VON DATEN IN EINER WEBFARM

Mit der MOVEit DMZ-Webfarm-Software können mehrere Anwendungsknoten (MOVEit DMZ-Anwendungen) einen gemeinsamen Datenspeicherort verwenden. Benutzer-, Datei- und Ordnerdaten sowie das Prüfprotokoll werden in der ODBC-kompatiblen Datenbank von MOVEit DMZ verwahrt. Diese kann sich auf einem Host befinden. Verschlüsselte und Debug-Dateien werden im Dateisystem gespeichert, das sich auf einem anderen Host befinden kann. Allgemeine Einstellungen, auf die häufig zugegriffen wird, werden in der Registry auf dem DMZ-Knoten gespeichert und über die Datenbank auf den anderen Knoten repliziert. Webinhalte werden auf dem DMZ-Knoten gespeichert und über die Datenbank auf den anderen Knoten repliziert.

HOCHVERFÜGBARKEIT UND LEISTUNG

Die verteilte Implementierung von MOVEit DMZ-Komponenten mit Zugriffssteuerung durch ein Lastenausgleichsmodul eines Drittanbieters ermöglicht die Skalierung der Verfügbarkeit und die Verbesserung der Leistung durch Hinzufügen von Anwendungsknoten zu der Webfarm. Hochverfügbarkeit kann durch Clustering mehrerer Datenbank- und Dateisystemknoten erreicht werden. Die MOVEit DMZ-Webfarm fungiert als ein einzelner MOVEit DMZ, der alle Client-Anfragen bearbeitet und Daten auf den Knoten koordiniert.

Die Voraussetzungen für Lastenausgleichsmodul, Network Address Storage (NAS) und Storage Area Network (SAN) entsprechen denen für die Resiliency-Software.

Bei technischen Fragen zu MOVEit DMZ wenden Sie sich an das MOVEit-Supportteam von Ipswitch. Informationen zu Lizenzierung und Preisen von MOVEit DMZ erhalten Sie beim Vertriebsteam von Ipswitch MOVEit.

IPSWITCH File Transfer
Simple. Secure. Managed.

Kontaktinformationen der File Transfer Division von Ipswitch