

## MOVEIT DMZ: VERWALTETER DATEITRANSFER-SERVER

MOVEit DMZ ist ein besonders sicherer Unternehmensdaten-transfer-Server mit durchgehend verschlüsselter Übertragung und Speicherung von Daten und Dateien, der leistungsstarke Verwaltungs- und Berichterstattungsfunktionen bietet.

Der MOVEit DMZ-Server unterstützt schnelle, einfache und sichere durchgehend verschlüsselte Übertragung und Speicherung von vertraulichen Informationen im Internet, egal ob Datei, Nachricht oder Webposting, und ermöglicht Unternehmen und Behörden so, ihre vertraglichen, branchenspezifischen und behördlichen Datenschutz- und Sicherheitsstandards einzuhalten. Diese Dokument gibt einen Überblick über die grundlegenden und optionalen Funktionen von MOVEit DMZ sowie Informationen zur Lizenzierung und zu den technischen Einzelheiten.

**SICHERHEIT.** MOVEit DMZ ist darauf ausgelegt, sicher auf einem mit dem Internet verbundenen, sicherheitsverstärkten Windows-Server in einem von mindestens einer Firewall geschützten Demilitarized Zone (DMZ)-Netzwerksegment ausgeführt zu werden. Vom Internet und dem lokalen vertrauenswürdigen Netzwerk aus kann sicher auf MOVEit DMZ zugegriffen werden, ohne das die Firewall von der DMZ ins lokale Netzwerk geöffnet werden muss. MOVEit DMZ schützt sich und die empfangenen Daten mithilfe eigener integrierter Komponenten: FIPS 140-2-validierte Verschlüsselung, 256-Bit-AES-verschlüsselte Speicherung sowie Authentifizierung und Zugriffskontrollen. Das bedeutet, dass die Sicherheit von MOVEit DMZ, seinen Benutzern und Daten nicht von der Sicherheit des zugrundeliegenden Betriebssystems abhängt.

**KOMPATIBILITÄT.** Dank der mehrfachen Protokollunterstützung von MOVEit DMZ können Mitarbeiter, Kunden und Partner schnell, einfach und sicher Dateien aller Größen und Typen über MOVEit DMZ übertragen, und zwar mit normalen Webbrowsern, sicheren FTP SSL (FTPS/TLS)- und SSH2 (SFTP/ SCP2)-Clients sowie allen AS2- und AS3-Clients.

**BEREITSTELLUNGEN MIT SCHICHTENARCHITEKTUR.** Verteilte Architektur ermöglicht die Bereitstellung mehrerer DMZ-Knoten in Form einer Webfarm. Administratoren können MOVEit DMZ jetzt auf einem Server bereitstellen, den verschlüsselten Datenspeicher auf einem zweiten Server und die Konfigurationsdatenbank auf einem dritten Server. Mit dieser flexiblen Architektur werden Leistung, Verfügbarkeit und Sicherheit der MOVEit DMZ-Lösungen ausgeweitet.

**FLEXIBILITÄT.** MOVEit DMZ-Administratoren können Benutzer mit Änderungs-, Profil- und Klonfunktionen verwalten sowie sie zu Gruppen zusammenfassen, die von Gruppenadministratoren verwaltet werden. Außerdem können sie einstellen, dass MOVEit DMZ bei eingehenden Dateien E-Mail-Benachrichtigungen versendet.

### NUTZUNGSBEDINGUNGEN DER BASISLIZENZ

- Unbegrenzte Benutzer und Dateitransfers
- Kann auf einem (1) Produktionssystem und einem (1) Nicht-Produktionssystem ausgeführt werden (physisch oder virtuell und ohne Beschränkung der Anzahl bzw. des Typs der CPUs)
- Unbeschränkte Nutzung der MOVEit Wizard- und MOVEit Xfer-Clients für sicheren Transfer

### FUNKTIONEN DER BASISLIZENZ

- HTTPS und FTPS/TLS (SSL) (FTPS IMPLICIT, TLS-P, TLS-C, Passiv)
- Unterstützung für SFTP/SCP2 (SSH2)-Transfer
- Serverseitige FTPS-NAT-Unterstützung
- AS2- und AS3-Datei- und MDN-Transferserver (erfordert die Verwendung von MOVEit Central mit aktivierter Central AS-Option)
- FTP-Transferunterstützung
- SMTP für Benachrichtigungen bei Datei- und Nachrichteneingang sowie administrativen Ereignissen
- FIPS 140-2-validierte Kryptographie
- AES 256-Bit-verschlüsselte Speicherung von Dateien, Nachrichten und anderen Daten
- Integriertes Berechtigungssystem
- MD5- und SHA1-Integritätsprüfung für Nicht-Ablehnung
- Unterstützung von Wiederaufnahme und Wiederholung des Transfersversuchs für garantierte Lieferung
- Benutzergruppen und Gruppenadministratoren
- Benutzerprofile, Klonen und Altern
- Unterstützung für Microsoft SQL Server und MySQL
- Authentifizierung mit bis zu 3 Faktoren: FTPS- und HTTPS-Clientzertifikate, öffentliche SFTP SSH-Schlüssel (Fingerprint), Kennwörter und IP-Adressen
- Entspricht den FFIEC-Authentifizierungsregeln
- Gesicherte Prüfprotokolle
- Vordefinierte und benutzerdefinierte Berichte
- Sicherer Remote-Verwaltungszugriff mithilfe normaler Webbrowser
- Entspricht den Spezifikationen RFC 959, 1122, 1123, 1579, 2228, 4217 sowie der IETF-Arbeitsgruppe „Securing FTP with TLS“
- Entspricht der NIST-Richtlinie SP 800-88 zum sicheren Löschen von Daten
- Bereitstellungen mit Schichtenarchitektur

**INTEGRATION IN SQL SERVER-DATENBANK.** Administratoren können entweder die eingebettete MOVEit-Datenbank verwenden oder eine Integration in Microsoft® SQL Server oder Microsoft SQL Server Express für Benutzerauthentifizierungs- und Serversystem-Konfigurationen wie Zugriffskontrollen, Benutzerberechtigungen und Kennwortrichtlinien vornehmen.

**COMPLIANCE.** Mit MOVEit DMZ können Lizenznehmer die Einhaltung von unternehmensinternen, vertraglichen, branchenspezifischen und behördlichen Datenschutz- und Sicherheitsauflagen gewährleisten und darstellen, einschließlich FISMA, GLBA, HIPAA, PCI DSS, PIPEDA, MA 201 CMR 17 und SOX. Alle Transfer- und Verarbeitungsaktionen und -fehler werden in der kommerziell lizenzierten, gesicherten Datenbank von MOVEit protokolliert. Mehr als 90 vordefinierte, integrierte Berichte können auf die Datenbank ausgeführt werden (benutzerdefinierte Berichte ebenfalls), und es können Datensätze für die Verwendung in Drittanbieteranwendungen zur Rechnungs- und Berichterstellung extrahiert werden.

**WERT.** Mit der MOVEit DMZ-Basislizenz kann die Software auf einem Produktions- und einem Nicht-Produktionssystem ausgeführt werden, mit unbegrenzter Benutzer- und Transferzahl. Die Lizenz umfasst außerdem die uneingeschränkte Nutzung der MOVEit Wizard- und MOVEit Xfer-Clients.

Damit die MOVEit DMZ-Basislizenz erschwinglich bleibt, werden die folgenden integrierten Funktionen als separat lizenzierte und zu bezahlende Optionen angeboten, die jederzeit hinzugefügt werden können.

**EXTERNE AUTHENTIFIZIERUNGSOPTION.** MOVEit DMZ verfügt über eine eigene, sichere Datenbank zur Authentifizierung von Benutzern. Mit dieser Option kann die Authentifizierung jedoch auch mithilfe einer oder mehrerer externer Benutzerdatenbanken (wie Active Directory) durchgeführt werden, und zwar mit einer beliebigen Kombination der Protokolle LDAP, Secure LDAP oder RADIUS Server. LDAP-Benutzer- und -Gruppenreplikation, Benutzerablauf und benutzerdefinierte Zuordnung von LDAP-Benutzerdatensätzen zu MOVEit DMZ-Benutzerprofilen werden unter dieser Option unterstützt. Dies gilt ebenfalls für SSO (Single Sign-on) über CA SiteMinder Web Access Manager und mit US Department of Defense CAC (Common Access Cards).

**OPTION FÜR SICHERES MESSAGING.** Autorisierte MOVEit DMZ-Benutzer können mithilfe dieser Option Nachrichten erstellen (mit oder ohne Dateianhang), diese an andere autorisierte Benutzer dieser MOVEit DMZ senden und ihre Nachrichten abrufen und auf diese antworten. Diese Nachrichten sind keine sicheren E-Mails sondern eine separate, parallele, durchgehend verschlüsselte Lösung, die normale Webbrowser als Clients nutzt, Autorisierung und Authentifizierung erfordert und verwendet wird, wenn Nachrichten (und Dateianhänge) sensible Informationen enthalten. Mit dieser Option können unbegrenzt Nachrichten gesendet/empfangen werden.

**API-SCHNITTSTELLENOPTION.** Bietet Drittanbieter-Programme (einschließlich Webanwendungen) mit programmatischem Zugriff auf die Transfer-, Speicherungs- und Benutzerdatenbankdienste von MOVEit DMZ, und bietet dem Benutzer Ordner-, Berechtigungs- und Berichterstellungsfunktionen. Diese Option umfasst unbeschränkte Nutzung der MOVEit DMZ API Javaklassen-, COM-Komponenten- und Befehlszeilen-Schnittstellen.

**OPTION FÜR MEHRERE ORGANISATIONEN.** Die MOVEit DMZ-Basislizenz gilt für eine einzelne Organisation, die Software ist jedoch darauf ausgelegt, eine bestimmte Anzahl weiterer Organisationen

## HOST-SPEZIFIKATIONEN

- Wird als Dienst unter Windows Server 2008 und 2003 ausgeführt
- Wird unter VMware ESX und Microsoft Virtual Server unterstützt

## EXTERNE AUTHENTIFIZIERUNGSOPTION

- Unterstützt mehrere Datenbanken und Protokolle
- LDAP- und Secure LDAP-Protokolle für Active Directory (AD)-, eDirectory-, iPlanet- und Tivoli-Benutzerdatenbanken
- LDAP-Benutzer- und -Gruppenreplikation
- Benutzerdefinierte LDAP-Zuordnung von Benutzerdatensätzen zu MOVEit DMZ-Benutzerprofilen
- RADIUS Server-Protokoll für Border Manager- und Internet Authentication Services (IAS)-Benutzerdatenbanken
- RADIUS für ODBC-kompatible Datenbanken
- LDAP- und RADIUS-Konfigurationstests
- SSO-Unterstützung für CA SiteMinder
- SSO-Unterstützung für US DoD CAC-Karte

## OPTION FÜR SICHERES MESSAGING

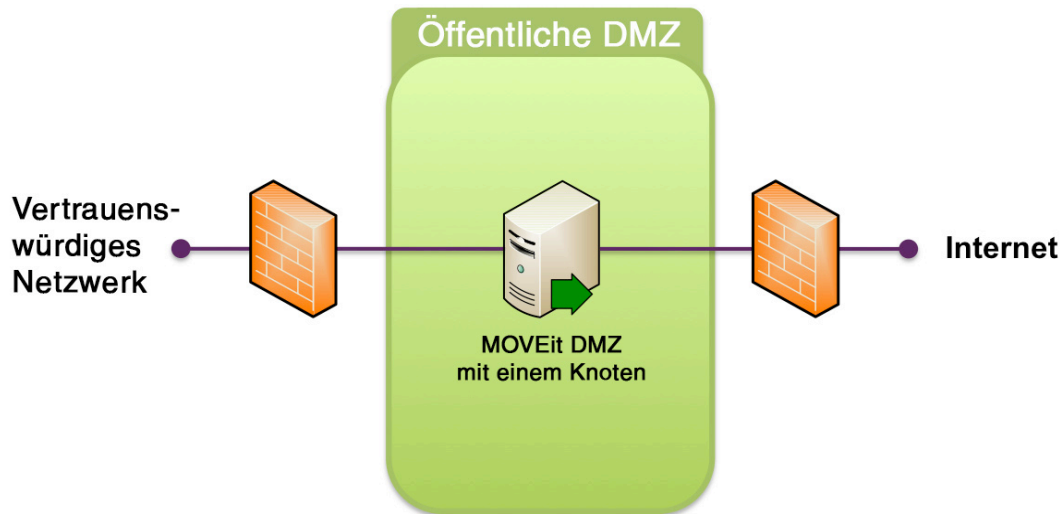
- Firefox, Internet Explorer, Mozilla, Netscape, Opera und Safari werden unterstützt
- Sicherer Nachrichtentransfer mit HTTPS
- SSL-verschlüsselter Transfer und AES-verschlüsselte Speicherung von Nachrichten/Dateien
- Nachrichtentwürfe und -vorlagen
- Wörterbücher für Rechtschreibprüfung
- Detaillierter und gesicherter Prüfpfad

## API-SCHNITTSTELLENOPTION

- Erstellen, Übertragen, Speichern und Löschen von Dateien und sicheren Nachrichten
- Erstellen, Verwalten und Löschen von Ordnern, Benutzern und Berechtigungen
- Ausführen vordefinierter Berichte, Erstellen und Ausführen benutzerdefinierter Berichte, Abrufen der Berichte
- Verwenden der MOVEit DMZ-Benutzerdatenbank sowie der sicheren Datei- und Nachrichtenspeicherung
- API-Javaklassen- und Befehlszeilen-Client erfordert Sun Java Version 1.4.2 oder höher
- API COM-Komponenten- und Befehlszeilen-Client wird unter Windows Vista Business Edition, 2003, XP, 2000 und NT 4.0 ausgeführt

## HOCHVERFÜGBARKEITS-OPTION

- Überwachungsfreies, automatisiertes Failover zwischen zwei nebeneinanderliegenden MOVEit DMZ-Produktionsservern
- Skalierbarkeit über zwei oder mehr Systeme
- Kontinuierliche Aktualisierung von Einstellungen, Statistiken und Statusinformationen
- Implementierung erfordert zwei identische DMZ-Lizenzen, Hardware- oder Software-Lastausgleich und einen NAS



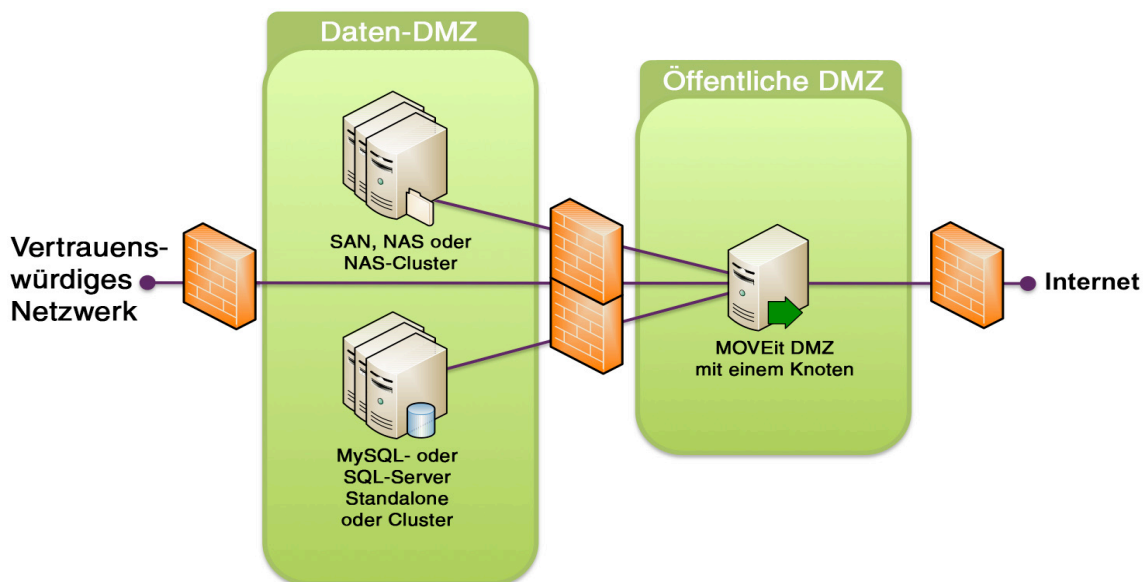
MOVEit DMZ einfache Bereitstellung mit einem Knoten

zu unterstützen, mit jeweils eigener eindeutiger URL sowie eigenen Benutzern, Administratoren, Berechtigungen, Protokollen, Dateien, Ordnern, Branding und verschlüsselter Speicherung. Dies bedeutet, dass eine einzige Ausgabe der MOVEit DMZ-Software, die auf einem einzigen Host ausgeführt wird, zwei oder mehr Agenturen, Abteilungen und Filialen unterstützen kann.

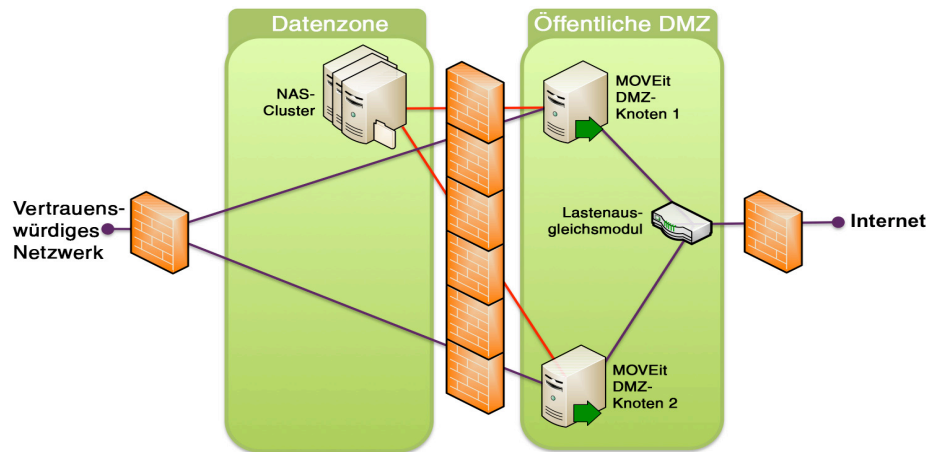
**SPRACHOPTIONEN FÜR ENDBENUTZER.** Mit dieser Option können Endbenutzer die Web-Benutzeroberfläche in Französisch oder Spanisch anzeigen.

**HOCHVERFÜGBARKEITS-OPTION.** MOVEit DMZ weist eine flexible Architektur auf, die dank der sofort einsatzbereiten Konfiguration mit Hochverfügbarkeit und automatischem Failover einen unterbrechungsfreien Betrieb rund um die Uhr gewährleistet. MOVEit DMZ kann auch mithilfe von Drittanbieter-Anwendungen für Lastausgleich und Clustering konfiguriert werden, um die reibungslose Bereitstellung mehrerer MOVEit DMZ-Server in einer Webfarm sicherzustellen.

Im oben abgebildeten Diagramm werden die Netzwerkstandorte und Transferprotokolle sowie die Firewall-Portanforderungen der MOVEit DMZ-Server und der kompatiblen Clients dargestellt. Wie die Pfeile andeuten, werden alle Verbindungen zu MOVEit DMZ von den Clients initiiert. Als reines Serverprodukt kann MOVEit DMZ keine Dateien in das lokale vertrauenswürdige Netzwerk verschieben. Dies bedeutet, dass Dateien und Nachrichten sicher über einen MOVEit DMZ-Server ausgetauscht werden können, ohne dass Firewall-Ports von der DMZ zum lokalen internen Netzwerk geöffnet werden müssen. Das Öffnen solcher Ports führt zu Lücken in der äußeren Sicherheitszone, wodurch das interne Netzwerk internetbasierten Sicherheitsrisiken ausgesetzt wird.



MOVEit DMZ 6.0 Multi-Tier-Bereitstellung

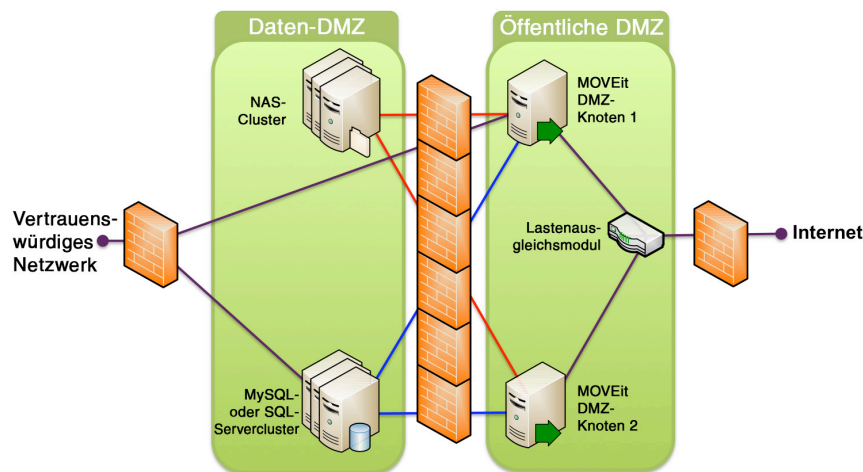


MOVEit DMZ „Flexible“ Bereitstellung mit zwei Knoten

Es gibt zwei verschiedene Möglichkeiten, MOVEit DMZ auf einer hochverfügbaren Basis zu implementieren, wobei beide Skalierbarkeit, automatisiertes Failover und Multi-Tier-Bereitstellung für verbesserte Sicherheit bieten.

Im oben abgebildeten Diagramm wird die flexible MOVEit DMZ-Methode dargestellt. Bei diesem Ansatz repliziert die MOVEit-Software automatisch ihre Konfigurations- und Berechtigungsdaten zwischen den MySQL-Datenbanken, die in jede MOVEit DMZ integriert sind. Die MOVEit-Software verwaltet auch das automatische, unbeaufsichtigte Failover zwischen den MOVEit DMZ-Knoten, falls einer dieser Knoten ausfallen sollte. Außerdem ermöglicht die Software die Bereitstellung des MOVEit DMZ 256-Bit AES-verschlüsselten Dateispeichersystems auf einem NAS oder NAS-Cluster, der sich in einem separaten Netzwerksegment befinden muss. Mit dieser Funktion können alle von MOVEit DMZ empfangenen Dateien in einem nicht-öffentlichen Segment mit beschränktem Zugriff gespeichert werden.

Im unten abgebildeten Diagramm wird die MOVEit DMZ Hochverfügbarkeits-Webfarm-Methode dargestellt. Bei diesem Ansatz profitiert MOVEit DMZ von vorhandenen Anwendungs-, Datenbank- und Netzwerkspeicher-Serverclustern und Replikation. Die MOVEit DMZ-Anwendung liegt auf zwei oder mehr Webfarm-Knoten im öffentlichen DMZ-Segment, während der Lastausgleich das Failover zwischen beiden übernimmt. Das MOVEit DMZ 256-Bit AES-verschlüsselte Dateispeichersystem wird auf einem NAS oder einem NAS-Cluster ausgeführt, und die MOVEit DMZ-Konfigurations- und -Berechtigungsdaten liegen entweder in einem MySQL- oder einem Microsoft SQL-Servercluster, die beide in nicht-öffentlichen Netzwerksegmenten mit beschränktem Zugriff liegen können. Bei diesem Ansatz befindet sich also nur die MOVEit DMZ-Anwendung im internetseitigen DMZ-Segment.



MOVEit DMZ 6.0 HA Webfarm-Bereitstellung mit zwei Knoten

Für weitere Informationen zu MOVEit DMZ sowie für Anfragen zu Lizenzierungs- und Preisangeboten und/oder einer kostenlosen Live-Online-Webpräsentation oder einer Bewertung vor Ort wenden Sie sich bitte direkt an Ipswitch.