

## MOVEIT DMZ: BERICHTERSTATTUNGSFUNKTIONEN

Die MOVEit DMZ-Software für sichere Datei- und Nachrichtentransfers und Speicherserver bietet neben mehr als 90 vordefinierten Berichten auch die Möglichkeit der Erstellung einer unbegrenzten Anzahl von benutzerdefinierten Berichten. Diese können allesamt für die Daten ausgeführt werden, die MOVEit DMZ automatisch in seiner sicheren, integrierten Datenbank protokolliert. Das vorliegende Dokument enthält Informationen über die vordefinierte Dateiübertragung, Secure Messaging, Benutzerstatus, die Benutzerverwaltung, Sicherheitsereignisse, Speicher- und Leistungsberichte, die benutzerdefinierte Berichterstattung und die Funktionen zum automatischen Planen und Abrufen von Berichten.

### DATEIÜBERTRAGUNGSBERICHTE

In diesen Berichten werden Informationen zu sicheren Dateitransfers gemäß den Protokolleinträgen zusammengefasst. Dabei werden Organisationseinheiten und Uploads/Downloads jeweils separat aufgeführt.

- Gesamt: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach Benutzer: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach Gruppe: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach IP-Adresse: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach Schnittstelle: Gesamtzahl bis heute oder nach Monat, Woche oder Tag

Für jeden dieser Dateiübertragungsberichte stehen folgende Optionen zur Verfügung:

- SizeUnits („K“, „M“ oder „G“; gibt die Dateigröße wieder) <sup>1</sup>
- StartDate (z. B. „2004-10-01“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge vor diesem Datum ignoriert). Hinweis: Es können Makros verwendet werden <sup>2</sup>
- EndDate (z. B. „2004-10-31“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge nach diesem Datum ignoriert). Hinweis: Es können Makros verwendet werden <sup>2</sup>

<sup>1</sup> Für die Erstellung von Informationen zur Dateigröße in diesen Berichten wird MOVEit DMZ v.3.3 oder höher benötigt.

<sup>2</sup> Beispiele für Makros: [jjjj]-[mm-3]-[tt] oder [jjjj]-[mm]-15.

### AKTIVITÄTSBERICHTE FÜR SICHERE NACHRICHTEN

In diesen Berichten werden Informationen zu sicheren Nachrichtentransfers gemäß den Protokolleinträgen zusammengefasst. Dabei werden Organisationseinheiten und Beiträge/Lesevorgänge jeweils separat aufgeführt.

- Gesamt: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach Benutzer: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach Gruppe: Gesamtzahl bis heute oder nach Monat, Woche oder Tag

Für jeden dieser Aktivitätsberichte für sichere Nachrichten stehen folgende Optionen zur Verfügung:

- SizeUnits („K“, „M“ oder „G“; gibt die Dateigröße wieder) <sup>3</sup>
- StartDate (z. B. „2004-10-01“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge vor diesem Datum ignoriert)
- EndDate (z. B. „2004-10-31“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge nach diesem Datum ignoriert)

<sup>3</sup> Für die Erstellung von Informationen zur Nachrichtengröße in Berichten wird MOVEit DMZ v.3.3 oder höher benötigt.

## BENUTZERSTATUSBERICHTE

In diesen Berichten werden Benutzer (und Gruppen) mit aktuellem Status und Berechtigungen aufgeführt.

- Aktive Benutzer
- Inaktive Benutzer
- Passwort läuft bald ab
- Gruppenzusammenfassung
- Gruppenmitgliedschaft
- Benutzerliste für Prüfer
- Standardberechtigungen für Basisordner
- Ordnerberechtigungen
- Adressbücher für sichere Nachrichten
- Kontingent: Beliebige, Definierte, Neue oder Größer als

Es wird empfohlen, während der Sicherheitsprüfung die folgenden Berichte auszuführen:

- Gruppenzusammenfassung
- Gruppenmitgliedschaft
- Benutzerliste für Prüfer
- Standardberechtigungen für Basisordner
- Ordnerberechtigungen
- Adressbücher für sichere Nachrichten

## SICHERHEITSEREIGNISBERICHTE

Die folgenden Berichten enthalten Hinweise auf mögliche Angriffsversuche gegen MOVEit DMZ und sollten während der Sicherheitsprüfung ausgeführt werden.

- **Verdächtige Benutzernamen:** viele Versuche oder verschiedene IP-Adressen
- **Verdächtige IP-Adressen:** viele Versuche oder verschiedene Benutzernamen
- **Gesperrte IP-Adressen:** Aktuell oder in der Vergangenheit
- **Gesperrte Benutzernamen:** Aktuell oder in der Vergangenheit

Für jeden dieser Sicherheitsereignisberichte stehen folgende Optionen zur Verfügung:

- **IPThreshold** (Mindestanzahl unterschiedlicher IP-Adressen für „viele verschiedene IP-Adressen“ – Standard = 5)
- **UsernameThreshold** (Mindestanzahl unterschiedlicher Benutzernamen für „viele verschiedene Benutzernamen“ – Standard = 5)
- **AttemptThreshold** (Mindestanzahl an Versuchen für „viele Versuche“ – Standard = 10)
- **StartDate** (z. B. „2004-10-01“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge vor diesem Datum ignoriert).
- **EndDate** (z. B. „2004-10-31“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge nach diesem Datum ignoriert)

## SPEICHERBERICHTE

In diesen Berichten wird angezeigt, wie viele Dateien, Nachrichten und archivierte Protokolldateien zurzeit in MOVEit DMZ gespeichert sind und wie viel Festplattenspeicher diese einnehmen.

- **Speicher:** gesamt, nach Ordner oder nach Benutzer
- **Speicher:** nach Ordner einschließlich Unterordner

Für jeden dieser Speicherberichte stehen folgende Optionen zur Verfügung:

- **SizeUnits** („K“, „M“ oder „G“; gibt die Dateigröße wieder)

## PERFORMANCE-STATISTIKBERICHTE

In diesen Berichten werden die vom MOVEit DMZ SysStat-Dienst erstellten Statistiken untersucht, für die normalerweise zwölf mal pro Stunde Daten erfasst und in die MOVEit DMZ-Datenbank eingetragen werden. Hinweis: Die Verwendung des SysStat-Dienstes ist nur mit MOVEit DMZ v.3.2 oder höher möglich.

Einige dieser Berichte werden stets in weitere Kategorien unterteilt. Dazu gehören unter anderem: Höchst-, Mindest- und Durchschnittswerte und Aufschlüsselung in Gesamtsystem, DMZCore, DMZISAPI, IIS, MySQL, DMZFTP, DMZSSH, DMZScheduler, DMZResiliency und Central-Anwendung. Es gibt einige Ausnahmen, die im Folgenden beschrieben werden.

- CPU-Leistung: alle oder nach Stunde oder nach Tag
- Festplattenleistung: alle oder nach Stunde oder nach Tag <sup>4</sup>
- Verarbeitungsleistung: alle oder nach Stunde oder nach Tag
- Speicherleistung: alle oder nach Stunde oder nach Tag <sup>5</sup>
- Prozessleistung: alle oder nach Stunde oder nach Tag
- Thread-Leistung: alle oder nach Stunde oder nach Tag
- Sitzungsleistung: alle oder nach Stunde oder nach Tag <sup>6</sup>
- Leistungszusammenfassung: alle oder nach Stunde oder nach Tag <sup>7</sup>

<sup>4</sup> In Festplattenberichten wird der auf den verschiedenen Festplatten verfügbare Speicher aufgeführt.

<sup>5</sup> In Speicherberichten werden virtueller und physischer Speicher separat aufgeführt.

<sup>6</sup> In Sitzungsberichten werden alle Sitzungen und aktive Sitzungen separat aufgeführt.

<sup>7</sup> Zusammenfassungsberichte enthalten Gesamtangaben zu CPU, freiem Festplattenspeicher, Verarbeitungen, Prozessen, Speicherauslastung und aktiven Sitzungen.

Für jeden dieser Leistungsberichte stehen folgende Optionen zur Verfügung:

- SizeUnits („K“, „M“ oder „G“; gibt die Dateigröße wieder)
- StartDate (z. B. „2004-10-01“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge vor diesem Datum ignoriert)
- EndDate (z. B. „2004-10-31“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge nach diesem Datum ignoriert)

## BENUTZERVERWALTUNGSBERICHTE

In diesen Berichten werden Benutzerverwaltungsaktivitäten gemäß den Protokolleinträgen zusammengefasst. Dabei werden Organisationseinheiten jeweils separat aufgeführt.

- Gesamt: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Nach Aktivität: Gesamtzahl bis heute oder nach Monat, Woche oder Tag
- Für jeden Benutzerverwaltungsbericht stehen folgende Optionen zur Verfügung:
- StartDate (z. B. „2004-10-01“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge vor diesem Datum ignoriert)
- EndDate (z. B. „2004-10-31“ oder “” (keine Angabe); wenn festgelegt, werden Protokolleinträge nach diesem Datum ignoriert)

## BENUTZERDEFINIERTER BERICHTE

Neben den oben beschriebenen vordefinierten MOVEit DMZ-Berichten können auch benutzerdefinierte Berichte festgelegt, ausgeführt und automatisiert werden. Diese müssen definierte Felder und Tabellen enthalten und können optional auch Kriterien, Gruppierungen, Reihenfolgen und Beschränkungen umfassen.

Vor dem Ausführen eines benutzerdefinierten Berichts überprüft MOVEit DMZ automatisch, ob für die benutzerdefinierte Abfrage gültige Tabellen verwendet werden. Darüber hinaus fügt MOVEit DMZ zusätzliche Kriterien hinzu, um zu verhindern, dass benutzerdefinierte Abfragen Unternehmensgrenzen überschreiten und sicherzustellen, dass die entgeltliche Abfrage sicher und schreibgeschützt ist.

## AUSFÜHREN UND ABRUFEN VON BERICHTEN

Berichte können bei Bedarf automatisch während der nächtlichen Durchführung von MOVEit DMZ-Aufgaben ausgeführt werden. Eine Ausführung auf On-Demand-Basis ist ebenfalls möglich. Über Schaltflächen und Verknüpfungen kann ein Bericht sofort aktiviert werden und entweder heruntergeladen und/oder in einem Webbrowser angezeigt oder ausgeführt und in einem MOVEit DMZ-Ordner gespeichert werden. Geplante Berichte können an bestimmten Tagen ausgeführt werden. Diese werden in einer durch Komma getrennte Liste von Wochentagen („Di, Mi, Do“) und/oder Tagen des Monats („1, 15“) definiert.

Berichte können mit verschiedenen Clients von MOVEit oder Drittanbietern über HTTP Secure (HTTPS), Secure FTP über SSH (SFTP und SCP2) oder Secure FTP über SSL (FTPS) vom MOVEit DMZ heruntergeladen werden. (Die Clients sind in dem Dokument „MOVEit DMZ Compatible Clients“ nach Protokoll und Betriebssystem aufgeführt.)

Mit MOVEit Central-Aufgaben können Berichte automatisch vom MOVEit DMZ heruntergeladen werden und in das lokale Dateisystem oder freigegebene Netzwerkordner kopiert, über FTP oder FTPS, SFTP oder HTTPS übertragen oder an E-Mail-Nachrichten angehängt und über SMTP gesendet werden. Im Rahmen der gleichen Aufgabe können die Berichte bei Bedarf außerdem mithilfe des MOVEit Central S/MIME-Objekts oder der OpenPGP-Funktion zusätzlich verschlüsselt werden.

Mit Drittanbieter-Anwendungen können neue benutzerdefinierte Berichte dynamisch erstellt sowie vordefinierte und bestehende benutzerdefinierter MOVEit DMZ-Berichte gestartet und die Ergebnisse abgerufen werden. Dies kann durch Verwendung einer lokal installierten Kopie der MOVEit DMZ API Java-Klasse oder der MOVEit DMZ API-Windows-COM-Komponente geschehen, um per Fernzugriff über die optionale MOVEit DMZ-API-Schnittstelle auf die Berichterstattungsfunktionen zuzugreifen.

Weitere Informationen erhalten Sie bei der File Transfer Division von Ipswitch oder unter [www.IpswitchFT.com](http://www.IpswitchFT.com).



File Transfer Division von Ipswitch kontaktieren