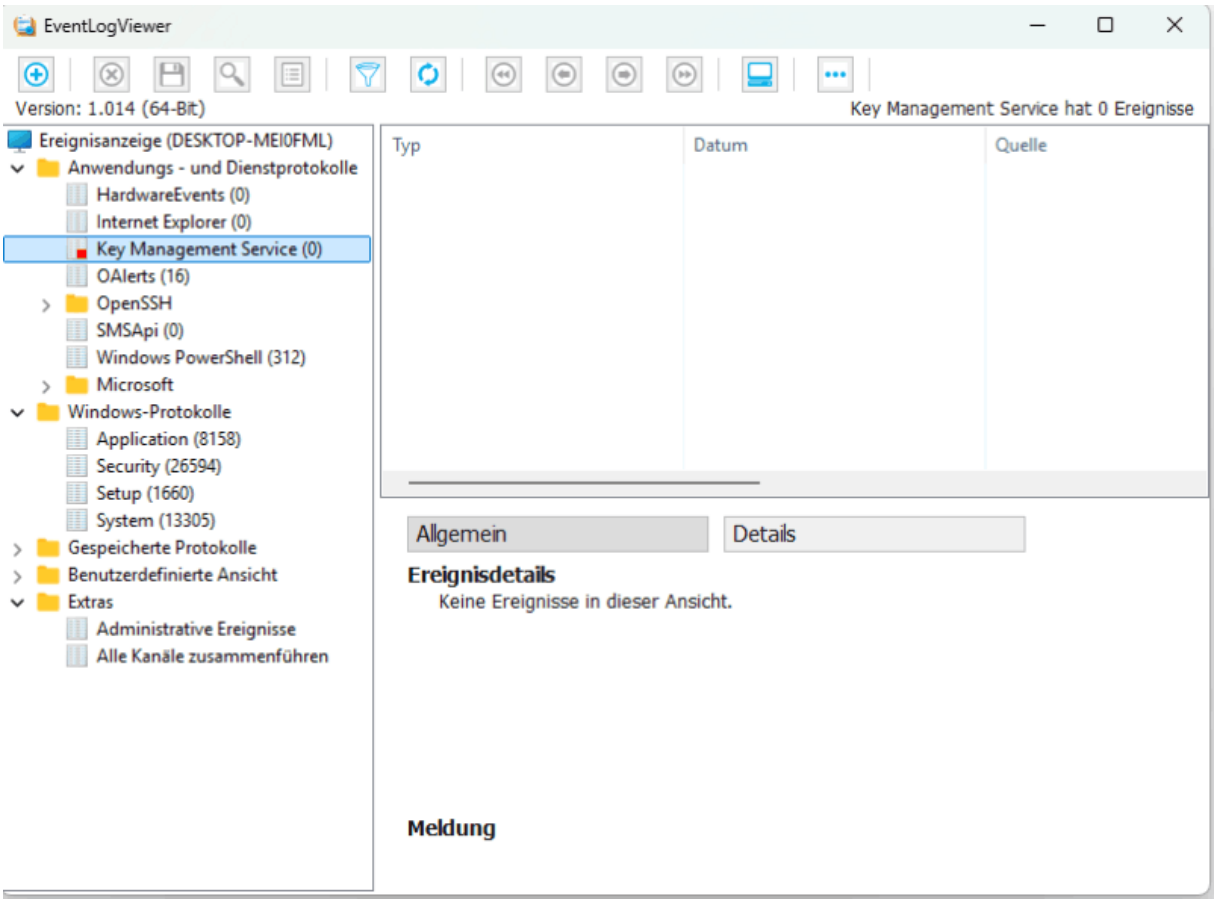


**EventLogViewer - Hilfedatei**

**Verwenden Sie den EventLogViewer, um Details zu jedem Protokoll zu filtern und zu finden**

Zur Unterstützung der Problembehebung zeigt der **EventLogViewer Ereignisprotokolle mit System - und Anwendungsmeldungen an**, die Fehler, Warnungen und Informationen zu bestimmten Ereignissen enthalten, die Administratoren analysieren können, um die erforderlichen Maßnahmen zu ergreifen.

**Aufbau des EventLogViewers**
**Der EventLogViewer besteht aus fünf verschiedenen Abschnitten:**
1) **Anwendungs- und Dienstprotokolle** - Dieser Abschnitt enthält viele Optionen, wie z. B. Hardwareereignisse, Schlüsselverwaltungsdienst, OpenSSH und Windows PowerShell...
2) **Windows-Protokolle** - enthält die Unterabschnitte Anwendung, Sicherheit, Setup und System.
3) **Gespeicherte Protokolle** - dient zum Öffnen gesoeicherter Protokolle.
4) **Benutzerdefinierte Ansicht** - dient zum Erstellen benutzerdefinierter Ansichten mit verschiedenen Filtern
5) **Extras** - Anzeigen Administrativer Ereignisse und Alle Kanäle zusammenführen

**EventLogViewer-Ebenen und -Definitionen**
Es gibt vier Hauptebenen, die die Ereignisanzeige zu verschiedenen Zeiten anzeigt: Kritischer Fehler, Fehler, Warnung und Informationen.

**Verwenden Sie den EventLogViewer, um Details zu jedem Protokoll zu filtern und zu finden**
Finden Sie alle möglichen Details aller protokollierten Elemente. Geben Sie den Typ der

Informationen an, die in den Ereignisprotokollen aufgezeichnet werden sollen. Die Informationen können Folgendes umfassen: Ereignistypen, Ereignistypen, Kategorie, Ereignis-ID, Benutzer, Computer, Ereignisse für verschiedene Uhrzeiten/Datumsangaben, Text in Beschreibung, Text in XML-Ansicht...

**Suchen von Ereignissen**
Suchen Sie nach Ereignissen mit einem superschnellen Suchalgorithmus. Die Suche unterstützt Groß/Kleinschreibung, ganze Zeichenfolge vergleichen, Wilcard und RegEx!

**Windows-Ereignisprotokolle teilen Ihnen die Reihenfolge und den Typ von Ereignissen mit, die zu einem bestimmten Zustand oder einer bestimmten Situation geführt haben.**
**Zu den Windows-Ereignisprotokollen gehören:**
Systemereignisprotokoll
Sicherheitsereignisprotokoll
Anwendungsereignisprotokoll
Verzeichnisdienst
Dateireplikationsdienst

**Anleitung:**

**Ändern der Ereignisanzeige Einstellungen**
Passen Sie Ereignisanzeige Einstellungen an, indem Sie mit der rechten Maustaste auf das Protokoll klicken und auf Eigenschaften klicken.
Folgenden Ereignisprotokolleinstellungen können angepasst werden:
**Maximale Protokollgröße**
Überschreiben von Ereignissen nach Bedarf
Überschreiben von Ereignissen, die älter als x Tage sind
Ereignisse nie überschreiben (Protokoll manuell löschen)
Verwenden einer Low-Speed-Verbindung (Windows)
**So ändern Sie Ereignisanzeige Einstellungen**
Klicken Sie mit der rechten Maustaste auf die entsprechende Protokolldatei (Anwendung, Sicherheit, System, Verzeichnisdienst oderDateireplikationsdienst).
Klicken Sie auf Eigenschaften.

**Exportieren von Ereignisprotokollen**
Ereignisprotokolle können für einen späteren Verweis oder für Verlaufsdaten gespeichert werden. Ereignisprotokolldateien können als Ereignisdateien (*.evt), Textdateien (*.txt) gespeichert werden. oder durch Trennzeichen getrennte Textdateien (*.txt).
**So speichern Sie Ereignisprotokolle**
Klicken Sie mit der rechten Maustaste auf die entsprechende Protokolldatei (Anwendung, Sicherheit, System, Verzeichnisdienst oderDateireplikationsdienst).
Klicken Sie auf Protokolldatei exportieren unter.
Geben Sie einen Namen für die Datei ein, und klicken Sie auf Speichern.

**Löschen von Ereignisprotokollen**
Löschen Sie Ereignisprotokolle, indem Sie alle Ereignisse löschen im Menü Aktion auswählen, nachdem Sie die entsprechende Protokolldatei ausgewählt haben. Sie haben die Möglichkeit, das Ereignisprotokoll zu speichern, bevor Sie es löschen.

**So löschen Sie Ereignisprotokolle**
Wählen Sie die entsprechende Protokolldatei aus (Anwendung, Sicherheit, System, Verzeichnisdienst oder Dateireplikationsdienst).
Klicken Sie mit der rechten Maustaste auf die entsprechende Protokolldatei.
Klicken Sie auf Protokoll löschen

**Auswahl von Computern**
Wählen Sie einen beliebigen Computer in Ihrem Netzwerk aus, um seine Ereignisprotokolle in Ereignisanzeige anzuzeigen.
**So wählen Sie Computer in der Ereignisanzeige**
Klicken Sie auf des Symbol Computerauswahl
Wählen Sie Verbindung mit einem anderen Computer herstellen aus.
Geben Sie den Computernamen ein, auf dem Ereignisprotokolle angezeigt werden sollen, und klicken Sie auf OK.

**Filtern von Ereignissen**
Geben Sie den Typ der Informationen an, die in den Ereignisprotokollen aufgezeichnet werden sollen. Die Informationen können Folgendes umfassen:
Ereignisse für verschiedene Uhrzeiten/Datumsangaben
Ereignistypen
Ereignisquelle
Kategorie
Ereignis-ID
Text in Beschreibung
Text in XML-Ansicht
Benutzer
Computer
**So filtern Sie Ereignisse**
Klicken Sie mit der rechten Maustaste auf die entsprechende Protokolldatei (Anwendung, Sicherheit, System, Verzeichnisdienst oder Dateireplikationsdienst).
Klicken Sie auf die Protokolldatei filtern.
Geben Sie die entsprechenden Informationen ein, die Sie filtern möchten, und klicken Sie dann auf Übernehmen.

**Suchen von Ereignissen**
Die Suche unterstützt **Groß/Kleinschreibung, ganze Zeichenfolge vergleichen, Wilcard und RegEx**!
**In der Suchmaske geben Sie an, welcher Ereignistyp gefunden werden soll:**
Ereignistyp
Quelle
Kategorie
Ereignis-ID
Computer
Benutzer
Beschreibung
**So finden Sie Ereignisse**
Wählen Sie die entsprechende Protokolldatei aus (Anwendung, Sicherheit, System, Verzeichnisdienst oder Dateireplikationsdienst).
Klicken Sie mit der rechten Maustaste auf die entsprechende Protokolldatei.
Klicken Sie auf Suchen.

Klicken Sie auf Abbrechen , wenn Sie fertig sind.

**Unterstützte RegEx-Operatoren für die Suche**

. Punkt, entspricht jedem einzelnen Zeichen außer einer neuen Zeile.

^ Caret-Zeichen, entspricht dem Anfang der Zeile oder Zeichenfolge, die der reguläre Ausdruck durchsucht.

$ Dollar, entspricht dem Ende der Zeile oder Zeichenfolge, die der reguläre Ausdruck durchsucht.

* Sternchen, entspricht null oder mehr + Plus, entspricht einem oder mehr

? Frage, entspricht null oder einem der vorhergehenden Zeichen.

{n} Entspricht dem vorhergehenden Ausdruck genau n-mal.

{n,} Entspricht n-mal oder öfter

{n,m} Entspricht dem vorhergehenden Ausdruck mindestens n-mal und höchstens m-mal.

[abc] Entspricht einem beliebigen von a, b und c.

[^abc] Ein Caret-Zeichen ^ am Anfang der eckigen Klammer bedeutet „nicht“. In diesem Fall entspricht es allem außer a, b oder c.

[a-zA-Z] Zeichenbereiche, der Zeichensatz der Bereiche { a-z | A-Z }

\s Entspricht einem Leerzeichen, \t \f \r \n \v und Leerzeichen

\S Entspricht einem Nicht-Leerzeichen.

\w Entspricht einem alphanumerischen Zeichen., [a-zA-Z0-9_]

\W Entspricht einem nicht-alphanumerischen Zeichen.

\d Entspricht einer Ziffer [0-9].

\D Entspricht einer Nicht-Ziffer.

| ODER-Operator (|): Beispielsweise akzeptiert der reguläre Ausdruck four|4 die Zeichenfolgen „four“ oder „4“.