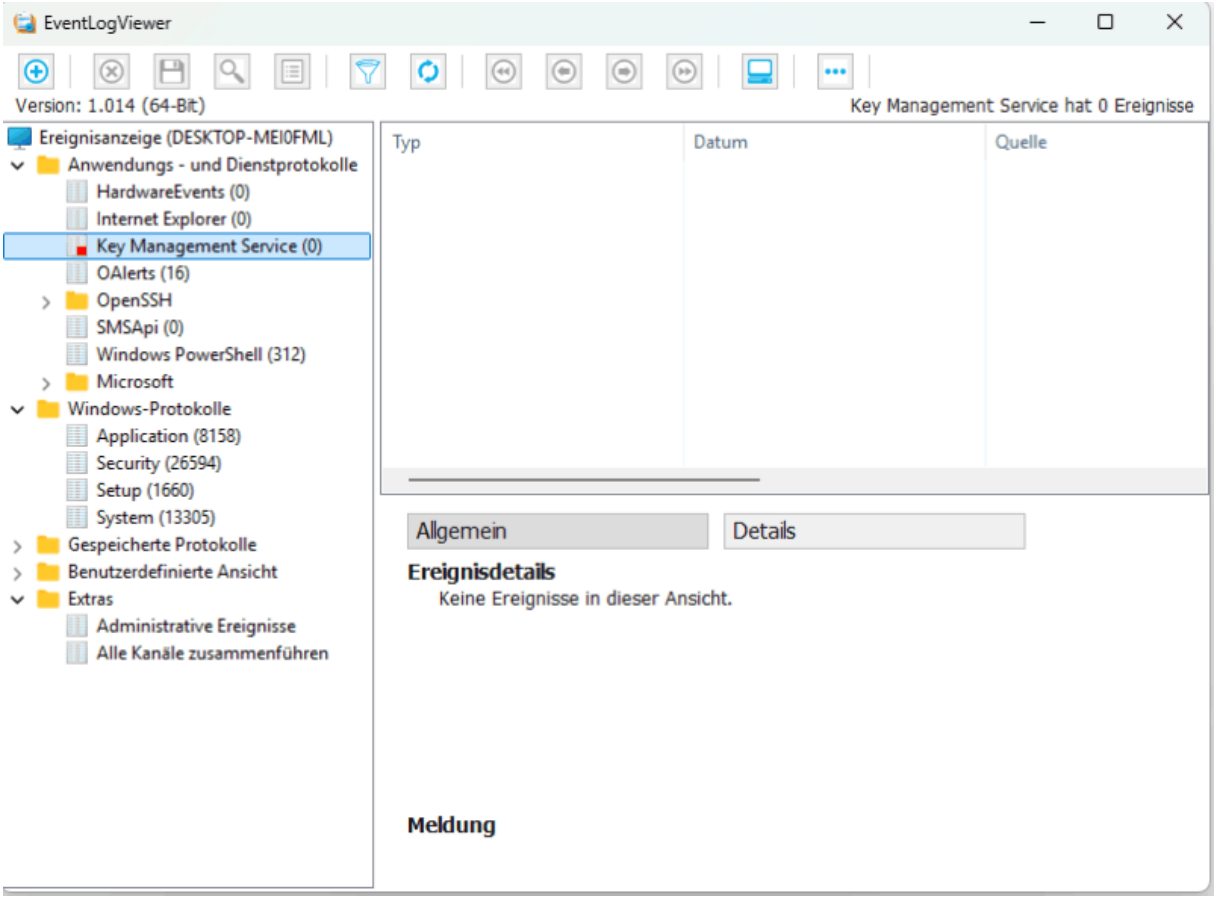

EventLogViewer - Fichier d'aide

Utilisez EventLogViewer pour filtrer et trouver des informations sur chaque journal.

Pour faciliter le dépannage, EventLogViewer affiche les journaux d'événements avec les messages système et d'application contenant des erreurs, des avertissements et des informations sur des événements spécifiques que les administrateurs peuvent analyser pour prendre les mesures nécessaires.

Structure d'EventLogViewer
EventLogViewer se compose de cinq sections :
1) Journaux des applications et des services : cette section contient de nombreuses options, telles que les événements matériels, le service de gestion des clés, OpenSSH et Windows PowerShell.
2) Journaux Windows : contient les sous-sections Application, Sécurité, Configuration et Système.
3) Journaux enregistrés : permet d'ouvrir les journaux enregistrés.
4) Vue personnalisée : permet de créer des vues personnalisées avec différents filtres.
5) Outils : permet d'afficher les événements administratifs et de fusionner tous les canaux.

Niveaux et définitions d'EventLogViewer
L'Observateur d'événements affiche quatre niveaux principaux : Erreur critique, Erreur, Avertissement et Informations.

Utilisez EventLogViewer pour filtrer et rechercher des informations sur n'importe quel journal.

Trouvez tous les détails possibles sur tous les éléments enregistrés. Spécifiez le type d'informations à enregistrer dans les journaux d'événements. Les informations peuvent inclure : types d'événements, catégories, identifiants d'événements, utilisateurs, ordinateurs, événements à différentes heures/dates, texte dans la description, texte dans la vue XML…

Recherche d'événements
Recherchez des événements grâce à un algorithme ultra-rapide. La recherche prend en charge la casse, la correspondance de chaîne entière, les caractères génériques et les expressions régulières !
Les journaux d'événements Windows indiquent l'ordre et le type d'événements ayant conduit à une condition ou une situation particulière.
Les journaux d'événements Windows incluent :
Journal des événements système
Journal des événements de sécurité
Journal des événements d'application
Service d'annuaire
Service de réplication de fichiers

Instructions :

Modification des paramètres de l'Observateur d'événements
Ajustez les paramètres de l'Observateur d'événements en faisant un clic droit sur le journal et en sélectionnant « Propriétés ». Les paramètres suivants du journal des événements peuvent être ajustés :
Taille maximale du journal
Écraser les événements si nécessaire
Écraser les événements de plus de x jours
Ne jamais écraser les événements (effacer manuellement le journal)
Utilisation d'une connexion bas débit (Windows)
Pour modifier les paramètres de l'Observateur d'événements
Cliquez avec le bouton droit sur le fichier journal approprié (Application, Sécurité, Système, Service d'annuaire ou Service de réplication de fichiers).
Cliquez sur Propriétés.

Exportation des journaux d'événements
Les journaux d'événements peuvent être enregistrés pour consultation ultérieure ou pour l'historique. Les fichiers journaux d'événements peuvent être enregistrés sous forme de fichiers d'événements (*.evt), de fichiers texte (*.txt) ou de fichiers texte délimités par des virgules (*.txt).
Pour enregistrer les journaux d'événements
Cliquez avec le bouton droit sur le fichier journal approprié (Application, Sécurité, Système, Service d'annuaire ou Service de réplication de fichiers).
Cliquez sur « Exporter le fichier journal sous ».
Nommez le fichier et cliquez sur « Enregistrer ».

Suppression des journaux d'événements
Effacez les journaux d'événements en sélectionnant « Effacer tous les événements » dans le menu Action après avoir sélectionné le fichier journal approprié. Vous pouvez enregistrer le journal des événements avant de l'effacer.
Pour effacer les journaux d'événements
Sélectionnez le fichier journal approprié (Application, Sécurité, Système, Service d'annuaire ou

Service de réplication de fichiers).
Cliquez avec le bouton droit sur le fichier journal approprié.
Cliquez sur « Effacer le journal ».

Sélection des ordinateurs
Sélectionnez un ordinateur de votre réseau pour afficher ses journaux d'événements dans l'Observateur d'événements.
Pour sélectionner des ordinateurs dans l'Observateur d'événements
Cliquez sur l'icône « Sélection d'ordinateurs ».
Sélectionnez « Se connecter à un autre ordinateur ».
Saisissez le nom de l'ordinateur pour lequel vous souhaitez afficher les journaux d'événements, puis cliquez sur « OK ».

Filtrage des événements
Spécifiez le type d'informations à enregistrer dans les journaux d'événements. Ces informations peuvent inclure :
Événements à différentes heures/dates
Types d'événements
Source de l'événement
Catégorie
ID d'événement
Texte dans la description
Texte dans la vue XML
Utilisateur
Ordinateur
Pour filtrer les événements
Cliquez avec le bouton droit sur le fichier journal approprié (Application, Sécurité, Système, Service d'annuaire ou Service de réplication de fichiers).
Cliquez sur « Filtrer le fichier journal ».
Saisissez les informations à filtrer, puis cliquez sur Appliquer.

Recherche d'événements
La recherche prend en charge la casse, la correspondance de chaînes entières, les caractères génériques et les expressions régulières !
Dans le masque de recherche, indiquez le type d'événement à rechercher :
Type d'événement
Source
Catégorie
ID d'événement
Ordinateur
Utilisateur
Description
Pour rechercher des événements
Sélectionnez le fichier journal approprié (Application, Sécurité, Système, Service d'annuaire ou Service de réplication de fichiers).
Cliquez avec le bouton droit sur le fichier journal approprié.
Cliquez sur Rechercher.
Cliquez sur Annuler lorsque vous avez terminé.

Opérateurs d'expression régulière pris en charge pour la recherche
. Point : correspond à n'importe quel caractère, sauf un saut de ligne.
^ Accent circonflexe : correspond au début de la ligne ou de la chaîne recherchée par l'expression régulière.
$ Dollar : correspond à la fin de la ligne ou de la chaîne recherchée par l'expression régulière.
*** Astérisque : correspond à zéro ou plus + Plus : correspond à un ou plusieurs**
? Question : correspond à zéro ou à l'un des caractères précédents.
{n} : correspond à l'expression précédente exactement n fois.
{n,} Correspond à n fois ou plus
{n,m} Correspond à l'expression précédente au moins n fois et au plus m fois.
[abc] Correspond à a, b et c.
[^abc] Un accent circonflexe ^ au début du crochet signifie « non », auquel cas il correspond à tout sauf a, b ou c.
[a-zA-Z] Plages de caractères, le jeu de caractères des plages { a-z | A-Z }
\s Correspond à un espace, \t \f \r \n \v et aux espaces
\S Correspond à un caractère autre qu'un espace.
\w Correspond à un caractère alphanumérique., [a-zA-Z0-9_]
\W Correspond à un caractère non alphanumérique.
\d Correspond à un chiffre [0-9].
\D Correspond à un caractère non numérique.
| Opérateur OU (|) : Par exemple, l'expression régulière four|4 accepte les chaînes « four » ou « 4 ».