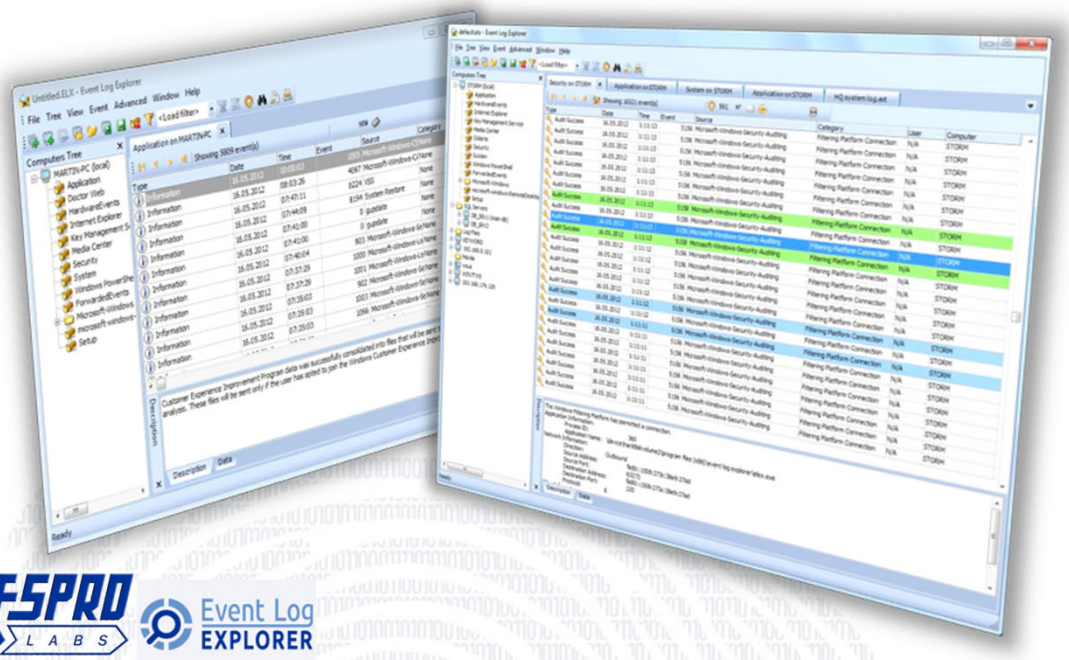
DIFOSE



FSPRO LABS Event Log EXPLORER

FSPRO EVENT LOG EXPLORER

Event Log Explorer, olay günlüğü araştırma üretkenliğini artırmaya yardımcı olur

Windows Yöneticileri için

- Olayları herhangi bir kritere göre filtreler
- Kullanıcı kimlik bilgilerini depolar
- Yoğun işgücü gerektiren görevleri otomatikleştirir
- Olayları izler ve bildirir

Adli Araştırmacılar için

- Ayrıntılı bilgileri alır
- Hasarlı olay günlüğü dosyalarını okur
- Excel'e ve diğer biçimlere aktarır
- Maliyetleri düşürür

ÜRÜN HAKKINDA

Event Log Explorer, Microsoft Windows olay günlüklerine kaydedilen olayları görüntülemek, analiz etmek ve izlemek için etkili bir yazılım çözümüdür. Olay Günlüğü Gezgini, olay günlüklerinin (güvenlik, uygulama, sistem, kurulum, dizin hizmeti, DNS ve diğerleri) analizini büyük ölçüde basitleştirir ve hızlandırır.

Event Log Explorer, standart Windows Olay Görüntüleyicisi işlevselliğini genişletir ve birçok yeni özellik getirir. Event Log Explorer'i deneyen kullanıcılar tarafından, Windows Olay Görüntüleyicisi'ne göre üstün bir çözüm olarak görülmektedir.

ÖZELLİKLERİ VE AVANTAJLARI

- **Olay günlüklerine anında erişim**
- **Etkili filtreleme**
- **Olay Günlüğü toplama**
- **Olayları dışa aktarma ve rapor oluşturucu**
- **Çalışma Alanları**
- **Veritabanı Depolama**
- **Belirli olaylar olduğunda uyarı verme**

AVANTAJLARI

- Yerel ve uzak sunucularda ve iş istasyonlarında Windows olay günlüklerine ve olay günlüğü dosyalarına erişin
- Hem klasik Windows NT olay günlüğü biçimi (EVT dosyaları) hem de yeni (Crimson) olay günlüğü biçimi (EVTX dosyaları) desteği
- Yüksek performans - tüm olaylar ya belleğe ya da optimize edilmiş bir dahili yerel veritabanına yüklenir
- Olay günlüğü toplama - farklı olayları tek bir yerde birleştirebilirsiniz
- Kullanıcı tercihlerine bağlı olarak sekmeli belge ve çoklu belge kullanıcı arayüzü
- Windows olay günlüklerini önceden filtrelemek için yükleme seçeneklerini günlüğe kaydetme
- Etkinlik açıklama metni dahil herhangi bir kritere göre gelişmiş filtreleme
- Favori bilgisayarlar ve günlükleri bir ağaçta gruplandırılır
- Windows olay günlüklerinin manuel ve otomatik olarak yedeklenmesi
- Yer imleri ile hızlı gezinme
- Tanınmış olay bilgi tabanlarıyla uyumluluk
- Olay Kimliğine göre renk kodlaması
- Farklı formatlarda yazdırma ve dışa aktarma
- Analitik raporlar - özet tablolar ve pivot grafikler
- EVT dosyalarına doğrudan erişim, hasarlı EVT dosyalarını okuma ve seçilen olaylardan EVT dosyası oluşturma
- Eski Windows'ta yeni EVTX dosyalarının okunmasını sağlayan EVTX dosyalarına doğrudan erişim
- Programa göre bazı olay günlüğü görevlerini çalıştırmak için zamanlayıcı
- Kimlik Yöneticisi
- Olay listesi herhangi bir sütunda ve herhangi bir yönde sıralanabilir
- Zaman düzeltme
- Sunucu içe aktarma

EKSTRA ÖZELLİKLER

- **Veritabanı depolama**

Event Log Explorer, sunuculardan ve iş istasyonlarından olayları toplar ve bunları MS SQL Server veritabanına aktarır. Manuel toplama kuralları kullanılarak istenildiği kadar veritabanı tablosu oluşturulabilir.

- **Yalnızca gerekli olayları filtreleme**

Kendi toplama kurallarınızı kullanarak, hangi olayların hangi makinelerden toplanacağını seçebilirsiniz. Olayları filtrelemek, ağ trafiği ve veritabanı depolamasından tasarruf sağlar.

- **Belirli olaylar hakkında uyarı**

Sistemleriniz tarafından oluşturulan olayları izlemek ve belirli bir olay tetiklendiğinde bilgilendirilmek için Event Log Explorer'i kurabilirsiniz. Sorunlar tarafından etkilenmeden önce haberdar olmanıza ve bu sayede önlem almanıza yardımcı olur.

- **Katılımsız aktarma**

Event Log Explorer, olayları SQL Server veritabanı, Excel kitapları, PDF dosyaları, HTML vb. gibi farklı biçimlere aktarmak için bir dizi komut satırı yardımcı programıyla birlikte gelir.