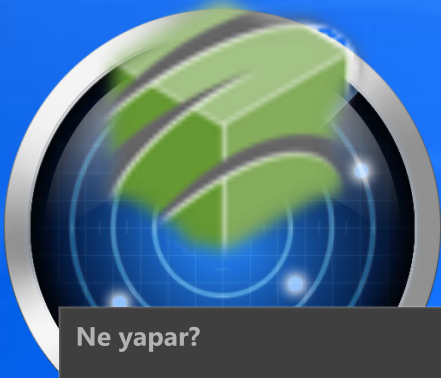




Diagnose & secure your network

YATEM LogCollector®

Active Directory Monitor™

Ne yapar?



Microsoft Active Directory sistemi üzerinde hızlı, maliyet etkin ve dayanıklı bir "değişiklik izleme" imkanı sağlar.



Kim?
Ne Zaman?
Nerede?
Ne Yaptı?

Sistem yükü?



İşlemci ve ağ üzerinde neredeyse yokmuş gibi çalışır.

Rapor ve Sorgulama



Arayüz ve raporlar aradığınız bilgiye kolayca ulaşmanızı sağlar.

Hızlı, basit, sade



Kurulum sadece dakikalar alır. Ayarlarla sizi yormaz. Öğrenilmesi ve kullanılması basittir.

Kapsamlı ve dayanıklı

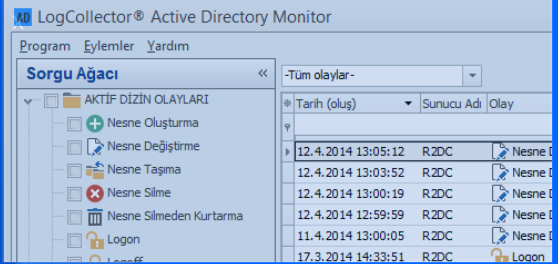


Ağınızın büyüklüğü, karmaşası ve hızı ne olursa olsun uzun süre sorunsuz çalışır.

Yasal Uyumluluk



5651 sayılı yasaya uyumluluğunuzu destekler.



“

"LogCollector Active Directory Monitor", kullanıcılar tarafından Microsoft Windows Active Directory sunucularında yapılan değişiklik girişimlerini gerçek zamanlı olarak izleyen, kaydeden ve analiz etmenizi sağlayan bir yazılım çözümüdür. Böylece, Etki Alanı sunucusu (DC) üzerinde yapılan değişiklikleri kontrol altına alarak kontrolünüz dışındaki girişimleri saptama ortamı oluşturmuş olursunuz.

”

Temel Kazanımlar

- **Farkındalık sağlar.** Ağınızda olanları ilk fark eden siz olursunuz.
- **Yatırım maliyetlerinizin korur.** Değerli emek ve maliyetlerle oluşturduğunuz ağınıza ve kurumsal verilerinizi titizlikle korumanızı sağlayarak yatırımlarınızı düşük maliyet ve iş gücü ile korumanıza destek olur.
- **Kolay ve esnek raporlama sağlar.** Her türlü isteğinize uyum sağlayabilen karmaşık raporları dahi saniyeler içinde ve kolayca hazırlayabilirsiniz.
- **Sürdürülebilir güvenlik altyapısına destek verir.** Güvenlik politikalarınızın etkinliğinin korunması ve geliştirilmesinde gerçek zamanlı ve ön kestirimli bilgiler sunarak, sürdürülebilir bir güvenlik altyapısı kurulmasını sağlar.
- **Hazır ve özel raporlama olanağı sağlar.** Yazılım kutudan kullanıma hazır raporlar ile birlikte gelmektedir. Bunun yanında uyarı veya otomatik olarak kullanılabilir özel raporlar hazırlamaya da olanak sağlamaktadır.
- **Ölçeklenebilir.** Yazılım ölçeklenebilir bir yapıda oluşturulmuştur. DC ve kullanıcı sayısının miktarına ve ağ iletişim yapısının durumuna uygun olarak değişik çalışma tekniklerini desteklemektedir.
- **Zaman kazandırır.** Sistem yöneticisine merkezi kontrol sağlaması nedeniyle zaman kazandırır.

Ne Yapabilirsiniz?

- "D" "Domain Controller" sunucusuna kimler işlem yapıyor?
- "Active Directory" üzerinde yetkisi olmadığı halde işlem yapmaya çalışanlar kimler?
- "Domain Admins", "Administrators" gibi kritik gruplara kullanıcı eklendiğinde e-posta ile bilgilim olsun istiyorum.
- Tüm DC lerde son 7 günde oluşturulan kullanıcılar neler?
- "K" kullanıcısının son 30 gün içinde gerçekleştirdiği tüm Active Directory düzenleme faaliyetleri neler?
- "K" kullanıcısını kim, ne zaman, hangi bilgisayardan sildi?
- Kullanıcıların hangi sunucuda hangi saatlerde ne tür işlem yaptığını grafik olarak görmek istiyorum.
- Halen hesabı kilitlemiş kullanıcılar hangileri?
- Gruplar üzerinde yapılan değişiklikleri her gün saat 17'de PDF formatında adresime e-posta olarak gönderilmesini istiyorum.



Özellikler

Genel

- **Lisanslama:** Sunucu ve kullanıcı başına lisanslama yapılmaktadır.
- **Veritabanı:** Toplanan veriler MS SQL veya PostgreSQL Server veritabanında saklanır.

Olay Toplama

- **Mimari:** Ajan tabanlı olarak çalışmaktadır.
- **Olaylar:** Microsoft Active Directory nesneleri üzerinde oluşturma, değiştirme, taşıma, silme ve silmeden kurtarma olaylarını toplamaktadır. Ayrıca, kullanıcıların oturum açma, oturum sonlandırma ve grup politikası değişikliklerini bilgilerini de toplamaktadır.
- **Olay Detayı:** Her olay için, hangi kullanıcı (kim), hangi sunucuda (nerede), hangi nesne üzerinde (neyi), hangi zamanda (ne zaman), gerçekleştirdiği işlem (ne) bazında tespit edilmektedir. Nesneler üzerinde yapılan değişikliklerin önceki ve sonraki değerleri birlikte gösterilmektedir.
- **Gerçek Zamanlı Toplama:** Olay gerçekleştiği anda gecikmeksizin ajan tarafından kayıt altına almaktadır.
- **Çevrimdışı Çalışma:** Ajan yazılımı, ağ bağlantısının olmadığı durumlarda da gerçek zamanlı çalışmasını sürdürür, topladığı bilgileri korur, bağlantı sağlandığı anda merkeze aktarır. Böylece ağ kesinti halinde olay kaybı oluşmaz.
- **Ajan Koruması:** Ajan yazılımı ve topladığı veriler merkeze gönderilme öncesinde disk üzerine koruma altındadır. LogCollector dışında kullanıcıların müdahalesine ve erişime kapalıdır.
- **Ajan Performansı:** LogCollector ajanı, oluşan olayları kaçırmadan toplayarak işleyen güçlü ve sürekli geliştirilen takip motoruna sahiptir.
- **Ajan İzi:** LogCollector ajanı; CPU, bellek ve ağ kullanımında çok düşük profilli çalışma (footprint) özelliği ile benzerleri arasında oldukça iddialıdır.
- **Ayıklama (Noise Reduction):** LogCollector ajanı etkin ayıklama teknolojisi ile gözlemlediği olayların tamamını değil, uçta filtreleme yaparak sadece istenenleri merkeze göndermektedir. Her olay için bir kayıt ilkesi ile çalışmaktadır. Böylece gereksiz bilgilerin toplanması ile CPU, disk, ağ ve veritabanı üzerinde gereksiz yük oluşumu ajanlar düzeyinde engellenmektedir.
- **Veri Bütünlüğünün Korunması:** Her kayıt, değişmezlik garantisini sağlamak amacıyla olayın için olduğu yerdeki ajan tarafından hazırlanan MD5 özet (hash) bilgisi ile saklanmaktadır.

Olayların Sorgulanması, Analizi ve Raporlama

- **Gerçek Zamanlı Olay İzleme:** LogCollector, toplanan olayların gerçek zamanlı olarak izlenmesi, analizi, ekran ve yazıcı raporları alınabilmesi için güçlü bir arayüze sahiptir.

- **Dinamik Sorgular:** LogCollector görüntüleme arayüzü, veritabanında istenen verilere ulaşmak için dinamik sorgular oluşturmaya destekleyerek basit ve esnek arayüzlere sahiptir.
- **Sorgu Performansı:** LogCollector, veritabanından biriken çok miktarda veri üzerinde oldukça hızlı analiz ve inceleme yapma olanağı sağlar.
- **Hazır Sorgu ve Raporlar:** Arayüz üzerinde, önceden hazırlanmış çok sayıda sorgu, rapor ve grafikler raporlar yer almaktadır.
- **Etkileşimli Grafiksel Analiz – Ara yüzler üzerinde görülen tablosal veriler grafik olarak ta görülebilir ve üzerinde çok seviyeli ayrıntıya inme (drill down) analizleri yapılabilir.**
- **Veri Aktarma:** Ekranda görüntülenen veri ve raporları metin, PDF, CSV/Excel, HTML, ve XML biçiminde dışarıya aktarılabilir.
- **Otomatik Raporlar:** Raporların zamanlı ve otomatik olarak hazırlanarak (PDF, Excel, metin vb.) disk üzerinde saklanması ve/veya belirtilen adreslere e-posta ile gönderilmesi mümkündür.
- **Otomatik Uyarılar (alarm):** Belirlenecek koşullara uygun olay oluşması durumunda istenen adreslere uyarı (e-posta) gönderme özelliğine sahiptir.

Yönetim

- LogCollector, izleme yapılacak bilgisayarlara ajanların kurulması, kaldırılması ve durumlarının gerçek zamanlı olarak izlenmesi için merkezi yönetim arayüzüne sahiptir.

Arşivleme

- LogCollector, veritabanında belirli bir zaman öncesine ait verilerin arşivlenmesi için bir arayüze sahiptir.
- Arşivleme elle veya zaman dayalı otomatik olarak yapılabilir.
- Arşivlenen verileri çevrimdışı olarak analiz etmek için aynı arayüz kullanılabilir.

Sistem Gereksinimleri

Merkezi Sunucu Bilgisayarı:

- CPU: 2 GHz Pentium tabanlı veya üstü
- İşletim sistemi: Microsoft Windows 7/2003/2008/2012
- Bellek: >1 GB RAM
- Microsoft SQL Server 2008+ veya PostgreSQL 9+
- Disk alanı: 100 MB+ kurulum için. Veriler için yeteri kadar.
- Görüntüleme: 1280x1024 veya üstü

Ajan Kurulumu:

- İşletim sistemi: Windows 7 ve Server 2012/2008/2008 R2/2003/2003 R2/2000
- Mimari: 32/64 bit
- Disk alanı: 100 MB+



YATEM Bilişim ve Teknoloji Sistemleri A.Ş.

E-posta: yatem@yatem.com.tr

Tel : +90 (312) 479 4088 Faks: +90 (312) 479 4088

http://www.yatem.com.tr

YETKİLİ DİSTRİBÜTÖR