DATASKOPE

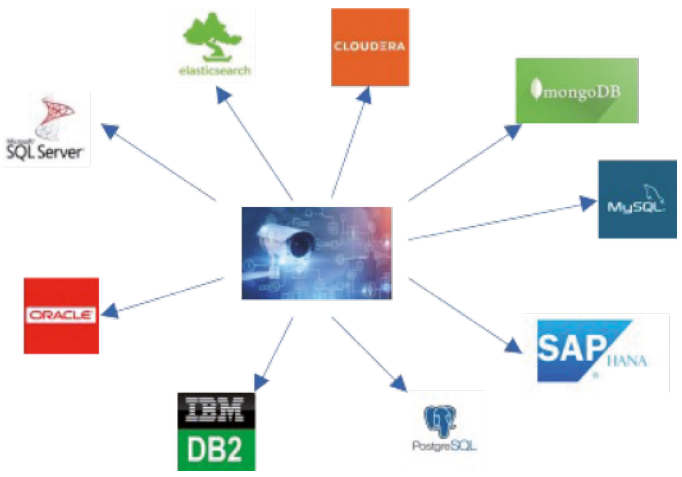
Veri Güvenliği ve Uyumluluğu
için Üstün Veri Tabanı Etkinliği
İzleme ve Önleme Çözümü

DATASKOPE NEDİR ?

Dataskope, tüm veri tabanlarınızda gerçekleşen her türlü aktiviteyi izlerken, kişisel ve hassas verilerinize yapılacak herhangi bir kötü niyetli müdahaleyi tespit etmenize ve önlem almanıza yardımcı olur.

Dataskope, tüm aktiviteleri kaydedip, denetim ve uyumluluk gereksinimlerini karşılamak için raporlama ve analiz sunar. Ayrıcalıklı kullanıcı ve uygulama erişimi izleme, yerel veri tabanı günlük kaydı ve denetim işlevlerinden bağımsız olarak gerçekleştirilir.

Ayrıca, yönetici aktivitelerini izleyerek ayrı görevlerin ayrılmasını sağlayarak ayrıcalıklı kullanıcılar için dengeleyici bir kontrol işlevi görebilir.



Neden veri tabanlarınızı yakından izlemeniz ve veri sızıntılarını hemen önlemeniz gerekiyor?

Veri tabanları, önemli, kişisel ve hassas bilgileri depolarlar. Genel olarak şirketler, işlerinin başarılı olabilmesi ve ihtiyaç duydukları tüm görevleri yerine getirmek amacıyla bir dizi farklı veri tabanı teknolojisini yönetmek zorundadırlar. Veri tabanlarına, farklı kaynaklardan gelen ve çeşitli sorgular çalıştıran çok sayıda kullanıcı ve uygulama tarafından erişilir.

Veritabanı etkinliğinin denetlenmesi ve kaydedilmesi, veri gizliliği yasalarına uygunluğun sağlanmasında önemli bir rol oynar. Bu sürekli uygulama, GDPR, HIPAA, SOX, PCI gibi yasal zorunluluklardan kaynaklanan bir gerekliliktir. Şirketler, veri tabanlarına sürekli olarak yönlendirilen talepleri izlemek ve aynı zamanda anormal aktiviteyi tespit ederek veri sızıntılarını önlemek için bu yeteneğe ve kolaylığa ihtiyaç duyarlar.

Güvenlik için acil olarak uygun cevaplar gerektiren birkaç önemli sorunlu soru ortaya çıkıyor:

•Veri tabanı sistemlerine izinsiz ve plansız erişimi nasıl izleyebilirim?
•Geliştiricilerin ve veri tabanı yöneticilerinin üretim sistemlerindeki faaliyetlerini nasıl izleyebilirim ve denetleyebilirim?
• Hassas ve kişisel bilgilere erişimi nasıl izleyebilirim?
• Bu farklı veri tabanlarında kişisel ve hassas bir sütuna kim erişebilir?
• Aynı müdahaleci, çeşitli veri tabanlarına mı bağlandı?
• Faaliyetlerdeki anormallikleri tanımlayabilir mi?
• Kullanıcı tarafından hangi sorgular gönderildi?
• Uygulama tarafından hangi sorgular gönderildi?
• Farklı veri tabanlardaki sütunu kim, ne zaman güncelledi?
• Bağlı kullanıcı meşru mu?
• Belirli bir veri tabanı tablosuna belirli bir erişim engellenebilir mi?
• Meşru olmayan bir erişim algılanabilir mi?
• Meşru olmayan bir erişim derhal rapor edilecek mi?
• Meşru olmayan bir rapor iptal edebilir mi?

Soruların listesi büyüyebilir.

Dataskope kullanarak hangi faydaları elde edersiniz?

Dataskope, ilgili RDBMS sunucusunun denetim alt sistemini etkinleştirmeyi gerektirmeksizin veri tabanı etkinliklerini izler; bu da büyük bir performans avantajıdır. Denetim kayıtlarını sınıflandırır ve ilişkilendirirken, bunları veri tabanı dışında saklayarak görev ayrımı ilkesine uyar ve farklı veri tabanları üzerinde analiz yapmayı mümkün kılar. Bir hizmet hesabının yalnızca tanımlanmış bir kaynaktan veri tabanına erişebilmesini ve yalnızca yetkilendirilmiş sorgu grubunu çalıştırabilmesini sağlar. Bu, hizmet hesabının tehlikeye düşmesi veya normalde kullandığı sistemden ya da hesap kimlik bilgileri beklenmeyen bir sistemden bağlantıda görünürse tespit etmek için kullanılabilir.

Dataskope ajanları yerel veri tabanı kayıtlarına dayanmadan tüm SQL ifadelerini (DML, DDL, DCL ve TCL) kaydedebilir, böylece performans düşüşlerini azaltır.

Dataskope' un ana özellikleri nelerdir?

Oturum Açma: Veri tabanına yapılan başarılı ve başarısız oturum açma işlemlerini takip etmenizi sağlar.

Veri içerik değişimi: SELECT, UPDATE, DELETE, EXEC, vb. komutların takibini sağlar.

Erişimlerin Takibi: Hassas verilere kimin eriştiğinin takibini sağlar. Beklenmeyen bir durum meydana geldiğinde uyarılar oluşturabilir ve/veya bunun olmasını önleyebilirsiniz.

Veri Tabanı Yönetici Denetimi: Kullanıcı yaratma, silme vb. işlemlerin takip eder ve aksiyon almanızı sağlar.

Sınıflandırılmış Denetim: Kullanıcı, veri tabanı, tablo, komut bazında işlemlerin kimler tarafından görüntülenebileceğine karar vermenizi sağlar.

Raporlama: ISO27001, COBIT, PCI, SOX gibi standartlara uygun raporlar almanızı sağlar.

Dataskope'dan hangi performans ve ölçeklenebilirliği bekleyebiliriz?

Dataskope ölçeklenebilirlik göz önünde bulundurularak geliştirilmiş kurumsal düzeyde bir çözümdür. Fiziksel veya sanal makineler üzerine depolanma veya donanım sınırlamaları olmadan dağıtılabilir. İhtiyaçlarınız büyüdükçe daha fazla kaynak ekleyebilirsiniz.

Dataskope hangi işletim sistemlerini destekliyor?

Dataskope sunucusu şu an Windows üzerinde çalışıyor fakat yakında Linux üzerinde de çalışıyor olacak. Dataskope ajanı C++ dilinde yazılmış olup Windows, Linux/Unix dağıtımları gibi ana işletim sistemlerinde çalışabilir (örneğin: Redhat, Suse, AIX, Solaris).

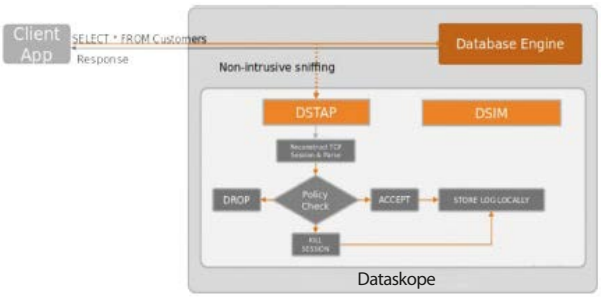
Dataskope hangi veri tabanı sistemlerini destekliyor?

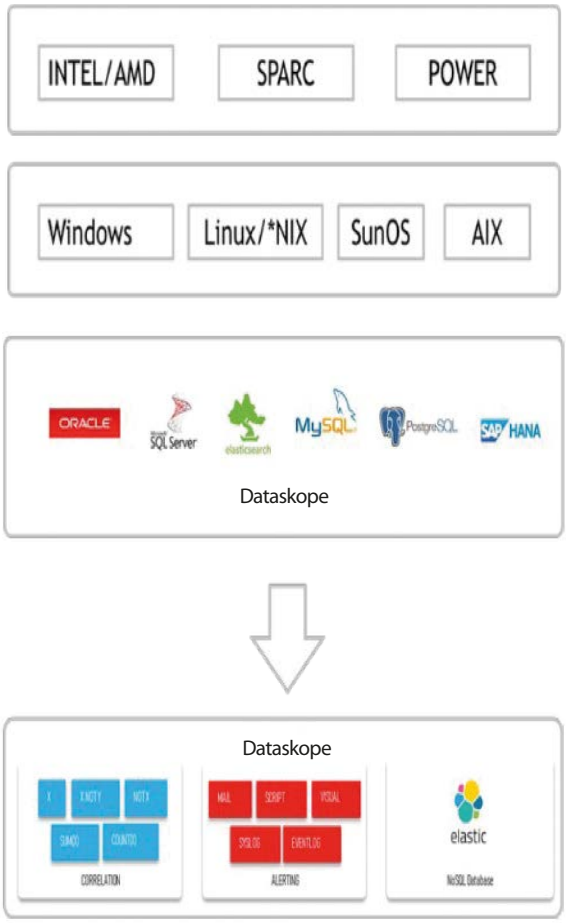
Tüm büyük İlişkisel Veri tabanı Yönetim Sistemleri (RDBMS) ürünleri desteklenmektedir: MS SQL SERVER, Oracle/Exadata, Teradata, DB/2, MySQL, PostgreSQL, vb.

Bir dizi Büyük Veri çözümü de desteklenmektedir: MongoDB, Cloudera, ElasticSearch.

Dataskope ajanı nasıl çalışır?

Ajanlar sorguları yakalamak için ağ trafiğini izler. Oracle Bequeath bağlantıları gibi yerel faaliyetler izlenir ve yakalanır. Dataskope ajanları, ara birim olarak çalışmadıkları için herhangi bir hizmet kesintisine neden olmazlar ve bu nedenle bir arıza noktası riski taşımazlar.





Dataskope hangi güvenlik özelliklerini sunuyor?

Dataskope sunucusu, güvenilir bir Windows sunucusu veya sahip olduğunuz bir Linux sunucusunda çalışır. Diğer sistemlerin aksine, gizlenen herhangi bir şifre yoktur. Dataskope sunucusuna giriş yapmak ve bakım görevlerini gerçekleştirmek için tüm şifrelere erişim sağlar. Günlük bütünlüğü sağlamak için her denetim kaydı bir karma değer ile saklanır.

Dataskope, yalnızca yetkilendirilmiş bir operatör tarafından görüntülenebilme sağlamak için yerel, LDAP kimlik doğrulama ve rol tabanlı yetkilendirmeyi destekler. Kimin-neyi-görebileceği ve kimin-neyi-yapabileceği belirlenebilir. Tüm operatör faaliyetleri kaydedilir.

Dataskope, gizliliği nasıl sağlar?

Dataskope, duyarlı/kişisel bilgileri (kredi kartı numaraları, e-posta adresleri, tıbbi kayıtlar vb.) tanıyabilir ve maskeleyebilir.

Dataskope, "runas", "su" ve "sudo" işlemlerinin arkasındaki gerçek kullanıcıyı keşfetmenizi sağlayan yerleşik kullanıcı kimliği zinciri tespiti sağlar.

Gelişmiş bir karmaşık olay işleme motoru, günlük toplama politikalarını ve uyarıları ilişkilendirmenize, aramanıza ve tanımlamanıza olanak tanır.

```
action_type:        query
auth_machine:       localhost.localdomain
auth_pid:           4117
auth_program_nm:    ********************domain (TNS V1-V3)
auth_sid:           oracle
auth_terminal:      pts/1
capture_type:       parse
client_app_name:    java
client_flags:       3
client_hostname:    localhost.localdomain
client_ip:          127.0.0.1
client_platform:    x86_64/Linux 2.4.xx
client_port:        53554
client_protocol_ver: 6.5
correlation_id:     3e13f276-cb1a-4bab-aadf-b1732663aa18
db_protocol:        TCP
db_type:            oracle
db_user:            SYSTEM
execute_options:    32865
os_user:            oracle
params_count:       0
port:               1521
query:              select * from dual where 1=1**********4
query_len:          114
result:             Completed
```

Dataskope, kötü amaçlı sızmaları algılayabilir ve zarar vermesini önleyebilir mi?

Dataskope, olağandışı faaliyetleri veya yetkisiz bağlantıları tespit etmeyi mümkün kılan karmaşık kurallar sunar. Böyle bir olayın tespiti durumunda, Dataskope faaliyeti iptal edebilir, bağlantıyı sonlandırabilir ve ayrıca uyarılar gönderebilir.

ALERT
INTRUSION DETECTED

Feature	DS
Windows Support	✓
Linux support	✓
Agent can audit client application	✓
Agent can audit application server	✓
Agent can audit database server	✓
Scalable architecture	✓
Distributed architecture	✓
Integrated with LDAP	✓
Integrated with SIEM products	✓
Role based authorizations	✓
Masking of sensitive information	✓
API support	✓

İLETİŞİM İÇİN

Telefon: +90 (212) 924 2030 **E-Posta:** info@kafein.com.tr **Web Sitesi:** www.kafein.com.tr

kafein technology solutions