Oracle'da Güvenlik

Kerem ERZURUMLU
A0064552

İçindekiler

Oracle'da güvenliği inceleyecek olduğumuzda inleme işlemini üç ana başlık altında yapmamızın doğru olacağını görürüz. Öncelikle güvenliğin ilk aşaması olan veritabanına olan bağlantıların kontrolü yapılmalıdır. Bahsi geçen kontrolden sonra bağlı kullanıcının veritabanı üzerindeki yetkilerinin kontrolü ve yapacağı işlemlerin onaylanması gelir. En son aşamada ise kullanıcıların sistemde gerçekleştirmiş olduğu işlemlerin kayıtları sonradan incelemeye alınabilmek amacı ile kayıt altında tutulmalıdır.

Bu nedenle bu yazımızı üç ana başlık altında inceleyeceğiz; 1) Veritabanı Erişim Kontrolü, 2) Yetkiler ve Roller, 3) Denetle İşlemleri.

1. Veritabanı Erişim Kontrolü

Güvenliğin ilk aşaması olan erişim kontrolü günümüz teknolojilerinde kullanıcı bazlı yapılmaktadır. Kullanıcının onaylanması için pek çok mekanizma mevcuttur ve Oracle bu mekanizmalardan bir çoğunu öntanımlı olarak desteklemektedir. En popüler ve Oracle tarafından kullanılan kullanıcı tanımla yöntemleri başlıca

- İşletim sistemi aracılığı ile onaylama,
- Ağ servisleri aracılığı ile onaylama,
- Oracle veritabanı kullanıcıları aracılığı ile onaylama,
- Uygulama sunucuları aracılığı ile onaylamadır.

Yukarıdaki yöntemlerler genellikle basitlik açısından yanlızca biri seçilerek kullanılır. Buna karşın Oracle bu yöntemlerin birden çoğununda aynı anda kullanılmasına olanak sağlamaktadır. Oracle veritabanı yöneticileri için kendi özel onaylama mekanizmasını güvenlik nedeni ile kullanmaktadır.

1.1 Normal Kullanıcıların Onaylanması

a) İşletim Sistemi Aracılığı ile Onaylama

Bazı işletim sistemleri Oracle'ın sisteme girmiş olan kullanıcı bilgisini,kullanıcı onaylaması esnasında kullanmasına izin verir. Böylece Oracle'a bağlanacak olan kullanıcılar ikinci bir kullanıcı adı/şifresi onaylamasına maruz kalmaz. Bu sistemin başlıca avantajları;

- Kullanıcıların Oracle'a ulaşımı hızlanır.
- Kullanıcı yönetimi işletim sistemine verilmiştir. Oracle'ın kullanıcı adı ve şifresi gibi bilgileri tutmasına gerek kalmamıştır.
- Oracle kullanıcı isimleri girdileri ile işletim sistemi denetleme işlemleri kayıtları uyuşur.

b) Ağ Servisleri Aracılığı ile Onaylama

a. **Üçüncü Firma Tabanlı Onaylama:** Eğer ağ servisleri onaylama hizmeti sunuyor ise (DCE, Kerberos yada SESAME gibi) Oracle "Oracle Gelişmiş Güvenlik" aracılığı ile bu servisler aracılığı ile onaylanmış kullanıcıları kabul edebilir.

b. **Kamusal Anahtar Tabanlı Onaylama:** Bu sistem her Oracle kullanıcısının bir sayısal sertifikası olduğunu varsayar ve kendisine bağlanan kullanıcıların bu sayısal sertifikalar aracılığı ile onaylar. PKI yöntemi beraberinde şu bileşenleri getirir;

- Güvenli oturum anahtarı ve anahtar onaylama işlemleri "Güvenli Soket Katmanı" (SSL) üzerinden yapılır.

- Oracle Çağrı Arayüzü sorguları ve kullanıcıya özgü bilgileri kişisel anahtar ile şifreler.
- "Oracle Cüzdanları" kullanıcıların kişisel anahtarlarını, kullanıcı sertifikalarını, ve güvenilir noktaları tutan bir mekanizmadır.
- "Dizin Tabanlı Oracle Güvenlik Yöneticisi" kullanıcı erişim bilgilerini ve yetkilerini tek bir merkezden toplamak amacı ile hazırlanmış LDAP uyumlu olarak çalışabilen bir dizin yöneticisidir ve Oracle veritabanı sunucusuna kullanıcı bilgilerini sunar.

c. **Uzak Onaylama:** Oracle "Uzak Çevirmeli Bağlantı Kullanıcı Servisi"ni (Remote Dail-in User Service – RADIUS) "Gelişmiş Güvenlik" seçenekli "Oracle Enterprice Edition" ile desteklemektedir.

c) Oracle Veritabanı Aracılığı ile Onaylama

Genel olarak tercih edilen mekanizma olan yerel onaylama, Oracle'ın kullanıcı bilgilerini kendi içerisinde tutması ve her bağlantı isteminde kullanıcı verilerini bu bilgilerden onaylaması mantığına dayanır. Kullanıcılar şifrelerini değiştirmek istediklerinde şifrelerini Oracle üzerinden değiştirmeleri gerekir.

Bu yöntemde diğer yöntemlerde olmayan bazı özelliklerin tanımlanması mümkündür. Örneğin "Bağlantı Esnasında Şifreleme" Oracle ile ilk bağlantı esnasında kullanıcı adı/şifresi gönderilirken verilerin DES algoritması ile şifreleneceğini böylece ağı gizlice dinleyen bir saldırganın şifreyi öğrenmesi engellenmiş olur.

"Hesap Kilitleme" özelliği sayesinde aynı kullanıcıya ait belirli bir sayıda hatalı sisteme giriş denemesinden sonra hesabın belirli bir süre için geçersiz olması sağlanabilir. Bu sistem özellikle brute-force tipi saldırılara karşı son derece başarılıdır.

"Şifre Geçerlilik Zamanı ve İptali" ile kullanıcıya verilen şifrelerin belirli süreler ile geçersiz olması sağlanabilir yada belirli süreler sonunda değiştirilmesi zorunlu tutulabilir. Bunun yanı sıra kullanıcıya yeni şifresinin eski şifresinden en az 5 karakter farklı olması gibi zorunluluklarda getirilmesi mümkündür.

"Şifre Karmaşıklığı" özelliği sayesinde kullanıcıların şifreleri için çeşitli sınırlamalar getirilerek şifrelerin tahmininin güçleşmesi sağlanabilir.

d) Uygulama Sunucu Aracılığı ile Onaylama

İnternet teknolojileri geliştikçe veritabanlarının internette kullanımı daha da yaygınlaştı. Bilindiği üzere 3 katmanlı mimaride tüm veritabanı işlemlerini uygulama katmanı yapmaktadır. Bu durumda Oracle'a bağlanmak için gerekli olan tek kullanıcı adı/şifresi uygulama sunucusu tarafından kullanılmakta olandır.

Geri kalan tüm yetkilendirme işlemlerinin tamamı uygulama sunucusu tarafından ele alınır ve burası tarafından gerçekleştirileceğine yada iptal edileceğine karar verilir. Fakat bu durumda yapıaln işlemlerin tamamı aynı kullanıcıdan gerçekleşmiş gibi görüleceğinden dolayı Oracle'ın kendi denetleme kayıtlarının yanı sıra başka bir denetleme mekanizması daha gerekmektedir.

1.2 Veritabanı Yöneticilerinin Onaylanması

"Veritabanı Yöneticileri" veritabanına özgü açma/kapama gibi işlemleri gerçekleştiren kişilerdir ve normal kullanıcıların onaylama mekanizmaları gibi onaylanamazlar. Veritabanı yöneticileri ya şifre dosyasından yada işletim sistemi tarafından onaylanmalıdır. "Uzak Veritabanı Yöneticileri" için önce bağlantılarının güvenli olup olmadığı kontrol edilir. Eğer bağlantı güvensiz ise şifre dosyasının kullanılması zorunludur. Eğer bağlantı güvenli ise işlemler "Yerel Veritabanı Yöneticisi" için yürütülenle aynı şekilde yürütülür. Öncelikle işletim sistemi bazlı mı onaylama yapılacağına bakılır. Eğer işletim sistemi bazlı onaylama yapılmayacak ise şifre dosyası kullanılır.

1.3 Kullanıcı Limitleri

Sistemde tanımlı olan her bir kullanıcı için ayrı ayrı sistem kaynakları üzerinde sınırlandırmalar koyabilirsiniz. Böylece zaten sınırlı olan işlemci zamanı gibi kaynakların kullanıcılar tarafından aşırı şekilde kullanmasını engellemiş olursunuz.

"`Kullanıcı Limitleri`" özelliği, çok büyük ve çok kullanıcılı sistemler için donanımlarının çok pahalı olması nedeni ile uygundur. Bunun yanı sıra kullanıcı limitlerini kullanmak kullanıcı açısından sistem başarımını düşürmektedir çünki ilk bağlantı esnasında kullanıcıya özgü bilgilerin yüklenmesi küçükde olsa bir zaman gerektirmektedir.

Sınırlandırılabilecek sistem kaynakları şunlardır;

- **Oturum Düzeyi:** Kullanıcı her veritabanına bağlandığında ayrı bri oturum açılır ve bu oturum sistem'in ana belleğinden ve işlemci gücünden bir miktarı kontrolü altına alır. Bu nedenle oturum esnasında işletilecek komutlar için limitleme gerçekleştirilebilir. Eğer bu limit aşılır ise kullanıcının işlemleri "`geri alınır`" ve limitlerin aşıldığına dair bir mesaj kendisine gösterilir.
- **Çağrı Düzeyi:** Bir SQL sorgusu çalıştırıldığında, sorgu işletilmeden evvel bazı çağrı düzeyleri gerçekleşir. Özellikle iç-içe sorgularda bu düzey katlanarak artar. Oracle ile belirli bir düzeyde limit tanımladığınızda kullanıcının yazdığı bir sorgunun bu limiti aşması durumunda sorgu durdurulur, sorgunun o anki ana kadar olan işlemleri "`geri alınır`" fakat kullanıcının oturumuna zarar verilmez.
- **İşlemci Zamanı:** Bir SQL sorgusu işletimi esnasında işlemciyi de işgal eder. Oracle bir sorgunun işlemciyi en fazla ne kadar süre meşgul edebileceğini sınırlandırabilir. Ve bu sınırı aşan işlemleri otomatik olarak sonlandırır.
- **Fiziksel Okuma:** Belirli bir sayıdaki okuma miktarının üzerine çıkan sorgular otomatik olarak sonlandırılabilir. Burada bahsi geçen okuma bellekden yada diskten olabilir.
- **Oturum Sayısı:** Kullanıcının aynı anda sahip olabileceği oturum sayısının sınırlandırılmasıdır.
- **Boş Zaman:** Kullanıcının bir oturum esnasında en fazla ne kadar süre ile birşey yapmadan durabileceği bilgisidir.

2. Yetkiler ve Roller

2.1 Yetkiler

Yetkiler herhangi bir SQL sorgusu çalıştırma yada başka bir kullanıcının nesnelerine erişim yetkisidir. Her kullanıcıya yanlızca yapacağı işler ile ilgili yetkilerin verilmesi durumunda kullanıcının erişimi büyük ölçüde kontrol altına alınmış olur. Böylece yetkisi olmayan birinin kişilerin maaş bilgilerini değiştirmeleri engellenir.

a) Sistem Yetkileri

Sistem yetkileri herhangi bir işlem yada herhangi bir şema türü içerisindeki bir işlemi gerçekleştirme yetkisidir. Örneğin "tablespace" yaratmak, tablolardan satır silmek sistem yetkileridir. Genel olarak 60'ın biraz üzerinde yetki çeşidi mevcuttur.

b) Şema Nesneleri Yetkileri

Şema nesne yetkileri tanımlı bir tablo üzerinde herhangi bir işlemi gerçekleştirme yetkisidir. Bazı şema nesnelerinin (cluster'lar, indexler, tetikleyiciler gibi) nesne yetkileri yoktur. Bu nesneler sistem yetkileri ile kontrol edilir.

Şema nesne yetkilerini veritabanı yöneticisi yada o nesnenin sahibi başka kişilere verip, alabilir. Eğer yetkiler "GRANT OPTION" ile verilmiş ise yetkilerin verilmiş olduğu kişilerde kendisine verilmiş yetkileri başkalarına verebilir.

c) Tablo Güvenlik Başlıkları

I. DML İşlemleri: DELETE, INSERT, SELECT ve UPDATE yetkileri aynı zamanda DML için DELETE, INSERT, SELECT ve UPDATE işlemlerinin yetkilerinide içermektedir.

II. DDL İşlemleri: ALTER, INDEX ve REFERENCES yetkileri tablo üzerinde uygulanabilecek DDL işlemlerine izin vermektedir.

2.2 Roller

Oracle yetki kontrolünü kolaylaştırma işlemini roller aracılığı ile yapmaktadır. Kısaca rolleri tanımlayacak olursak, bir işlemi gerçekleştirmek üzere gereken yetkilerin bir araya toplanmış halidir denilebilir.

Roler tanımları gereği kullanıcılar ile aralarında "n'e m" lik bir ilişki barındırırlar. Yani bir role bir çok kişi sahip olabilir ve bir kişi birden çok rol üstlenebilir. Rollerde yapıalcak bir değişiklik o rolü oynamakta olan kişilere de aynı anda yansır.

Roller, kendileri yada kendilerini içeren bir rol olmadığı sürece diğer rolleri kapsayabilir.

Rollerin dağıtımı "GRANT ANY ROLE" sistem yetkisine sahip kişiler tarafından yapılmaktadır. Aynı zamanda "ADMIN OPTION" a sahip kullanıcılarda rolleri dağıtma yetkisine sahipdir.

3. Denetleme İşlemleri

3.1 Denetleme Özellikleri

Denetleme seçilmiş olan kullanıcının veritabanı erişimlerini ve işlemlerini kaydetmek ve izlemekdir denilebilir. Normal koşullar altında "denetleme" şüpheli durumlarda inceleme amacı ile yada belirli veritabanı hareketleri hakkında bilgi almak/inceleme yapmak için kullanılır.

Başlıca denetleme türleri "Durum Denetleme", "Yetki Denetleme", "Şema Nesne Denetleme" olarak gruplandırılabilir. "Durum Denetleme" seçilmiş olan SQL sorgularının hangi şema üzerinde çalıştığına bakılmaksızın kaydının tutulmasıdır. "Yetki Denetleme" seçilmiş olan yetkilerin gerekli olduğu işlemlerin yapılmaya çalışılması yada yapılması durumunda kayıt tutan denetleme türüdür. "Şema Nesne Denetleme" ise belirli bir nesne/tablo üzerinde yapılan/yapılamaya çalışılan tüm işlemlerin kaydının tutulmasıdır.

Denetleme kayıtlarında yapılan denetleme türüne bağlı olmakla birlikte "kullanıcı adı", "oturum tanımlayıcısı", "uçbirim tanımlayıcısı", "ulaşılan şema nesnesinin adı", "işlem sonucu", "işlem sonuç kodu", "tarih bilgisi", "kullanılan yetkiler" bilgilerinden bir kümenin kaydını tutar. Bahsi geçen kayıtlar öntanımlı olarak şifrelidir ve normal yollardan ulaşılamaz.

3.2 Denetleme Mekanizmaları

Eğer denetleme mekanizmaları aktif halde ise denetleme kayıtları sorguların çalıştırma safhasında gerçekleştirilir. Eğer kayıt işlemi gerçekleştirilemez ise sorgu geri alınır. Fakat tersi bir durumda; yani kullanıcının hareketini geri alması durumunda kullanıcının geri alınan hareket esnasında meydana getirmiş olduğu kayıtlar silinmez.

Oracle'ın açılması, kapanması ve veritabanına veritabanı yönetici olarak bağlanma işlemleri İşletim Sistemi kayıtlarına tutulur ve bu kayıtlama işleminin iptali söz konusu değildir.

Denetleme mekanizmalarındaki değişiklikler kullanıcıların sisteme bir sonraki girişleri ile aktif hale gelmektedir.