XƏZƏR UNİVERSİTETİ

Fakültə: Mühəndislik və tətbiqi elmlər

Departament: Komputer Elmləri

İxitisas: Informatika

MAGİSTR TEZİSİ

MÖVZU: Oracle Verilənlər bazasında istifadəçi təhlükəsizliyi və bank sektoruna tətbiqi

Magistr tələbə: Roza Misirli

Elmi rəhbər: Ph.D. Leyla Muradxanlı

BAKU - 2016

Xülasə

Dünyada informasiyanın rolunun artması onu saxlayan bazanın təhlükəsizliyi problemini ortaya çıxartdı. İnformasiyanı saxlayan bazalardan biri Oracle verilənlər bazasıdır və OVB-da informasiyanın gizli saxlamaq üçün istifadəçi təhlükəsizliyi hər sektorda əhəmiyyətli olduğu kimi Bank sektorunda da əhəmiyyətlidir. Ona görə də bu magistr diplom işində Oracle verilənlər bazasında istifadəçi təhlükəsizliyinin yaradılması, onun şifrə ilə qorunmada çıxan problemləri, Azərbaycanda bank sektorunda istifadəçi təhlükəsizliyin problemləri, Oracle verilənlər bazası vaultun (OVBV) yaradılması qaydaları və onun şifrə ilə qorunmadan üstün xüsusiyyətləri haqqında, OVBV-un bank sektoruna tətbiqi məsələsindən danışıldı.

Əsas məsələ kimi bank sektorunda Oracle verilənlər bazası administratorunun yarada biləcəyi problemlər və gizli informasiyaları OVBA-dan qorunmağın əhəmiyyəti haqqında məlumat verildi. OVBV-dan istifadə edərək OVBA-nın səlahiyyətinin azaldılması Bank sektorunda təhlükəsizliyi artırmasına səbəb olduğu göstərildi.

Son olaraq isə Azərbaycan bank sektorunda ODV-nin tətbiqi praktik olaraq göstərildi. İlk əvvəl mövcud olmuş OVB-sına OVBV tətbiq etmədən öncə nəyə əhəmiyyət verilməli olduğu haqqında məlumat verildi.Yəni baza qurularaq default istifadəçilərdən əlavə admin səlahiyyətinə malik istifadəçilər yaradıldı. Daha sonra OVBV-nın qurulmasında başlayaraq necə istifadə olunacağı haqqında danışıldı və bank sektorunun təhlükəsizliyini təmin etmək üçün lazım olan tələblər praktik olaraq kompleks şəkildə tətbiq edildi.

Abstract

The increase of role of information led to the problems of database security. One of the databases that store information is Oracle Database and as in all sectors of ODB, in bank sector user privacy and security is important. Therefore, in this master thesis, I wrote about creating user security in ODB, the problems with password protection, problems of user security in Bank sector in Azerbaijan, the rules of creating OVBVand its superior feature to password protected, and applying of OVBVin Bank Sector.

The main object of the project is the problems can be created by Oracle Database Adminstration (ODA) and the importance of protection private information from ODA in bank sector. Reduction of authorization of ODA and using ODV caused to increase of the security in bank sector.

Finally, application of ODV in bank sector is demonstrated. Firstly, it has been explained that before applying of ODV, what should be considered in existing OD.İn addition to default users, admin priviliges users which establishing a new base was created. Then, installation and use of ODV has been decribed and the requirements which are necessary to provide secure of the banking sector was applied as a practice in the complex.

Mündəricat

Cədvəllər, şəkil və qrafiklərin siyahısı

Qısaltmalar siyahısı

VB - Verilənlər bazası

OVB - Oracle verilənlər bazası

OVBA - Oracle verilənlər bazası adminstrator

OAV - Oracle Audit Vault

OVBF - Oracle verilənlər bazası Firewall

OVBV - Oracle verilənlər bazası vault

ODV - Oracle Database Vault (ingilis dilində)

OLT - Oracle Label Təhlükəsizliyi

OVŞVB - Oracle virtual şəxsi verilənlər bazası

DMZ - Demilitarized Zone

GİRİŞ

Müasir dövrümüz informasiya mübadiləsi dövrüdür. İnformasiyanın başqa şəxslərin əlinə keçməməsi üçün onun təlükəsizliyi təmin edilməlidir. İnformasiya təhlükəsizliyi deyəndə, məlumat sistemlərinin icazəsiz müdaxilə edilərək məlumatların dəyişdirilməsindən, silinməsindən və s. əməliyyatlardan qorunması nəzərdə tutulur.

Hər bir dövlətlər, müxtəlif tipli idarələr, dünya səviyyəli təşkilatlar, banklar, məktəblər, univesitetlər, şəxsi biznes təşkilatları və s. məxfi və dəyərli informasiyalar toplayır və onların çoxu bu məlumatları verilənlər bazasında saxlayır. Bu məxfi informasiyaların qanunsuz şəkildə başqa şəxslərin əlinə keçməməsi üçün verilənlər bazasının təhlükəsizliyi yüksək səviyyədə təşkil edilməlidir.

Bank sektorun informasiyaların təhlükəsizliyinə daha çox diqqət verilir, çünki bankda pulu olan hər kəs (müştərinin), lazımlı tədbirlər alınmadığı təqdirdə, "zərər çəkmiş" ola biləcəkdir. Müştərinin etibar etdikləri banklardan müxtəlif yollarla pullarının oğurlanması, müştərinin banka etibarını zədələyir və bankların müştərilərini itirməsinə səbəb olur. Bununla yanaşı məhkəmə qərarları ilə müştərinin zərərinin bank tərəfindən ödənilməsinə hökm edilməsi vəziyyətində banklar maddi zərərlərə də məruz qalırlar. Həm güvən itkisi, həm də maddi itkilər, bankları informasiya təhlükəsizlyinə qarşı tədbirlər almağa məcbur edir.

Banklar informasiyanı verilənlər bazasında saxladığından informasiyanın təhlükəsizliyi verilənlər bazasının təhlükəsizliyindən asılıdır. Verilənlər Bazası fayllarda saxlanılan informasiya yığımıdır. Verilənlər Bazası fayllarında informasiya mətn, cədvəl və başqa şəkillərdə saxlanıla bilər. Əsasən cədvəl şəkilli Verilənlər Bazasından istifadə olunur. Şəbəkə dəstəkli mühitlərdə bazalar üçün alınan təhlükəsizlik tədbirləri əksəriyyətlə qeyri-kafi qalmaqda və təhlükəsizlik pozuntuları yaşanmaqdadır. Yüksək səviyyədə VBİS təhlükəsizliyinin təmin etmək üçün texnoloji tədbirlərdən əlavə olaraq insan faktoru da nəzərə alınmalıdır və texniki səviyyədən inzibati səviyyəyə qədər bütün istifadəçilərdə informasiya təhlükəsizliyi haqqında məlumat vermək lazımdır.

Son dövrlərdə Azərbaycanda eləcədə dünyanın bir çox yerlərində çox istifadə olunanı VB Oracle verilənlər bazasıdır. 1977-ci ildə əsası qoyulan Oracle şirkəti, təhlükəsizliyə böyük əhəmiyyət vermişdir. Bu illər ərzində böyük dövlət qurumları,

ticari şirkətlər və banklar Oracle VB-sından istifadə edib onun təhlükəsizlik sisteminə əhəmiyyət vermişdir. Bu şirkət verilənlər bazası təhlükəsizliyində ən yeni texnologiyaları təqdim etməkdə davam edir. Təqdim edilən bu məhsulların ən böyük xüsusiyyəti bir-biriylə inteqrasiya edərək işləməsi və bir-birini tamamlayıcı xüsusiyyətə malik olmasıdır.

Oracle verilənlər bazasının təhlükəsizliyinin bir çox növü var. Bu növlərdən əsasını Oracle verilənlər Bazasında İstifadəçi Təlükəsizliyi təşkil edir. Oracle-ın 10g versiyasında istfadəçi təhlükəsizliyinə aid Oracle Database Vault və Oracle Audit Vault yenilikləri var və 11g,12c versiyalarında daha da təkmilləşdi. Bu təhlükəsizlik üsulları ilə baza maksimum dərəcədə təhlükəsiz müdafiə olunur.

Biz bu magistr dissertasiya işinin birinci hissəsində əvvəl Oracle Vb-sının istifadəçi adları və onun yaradılmasında istifadə olunan şifrənin mürəkkəbliyi,resurs məhdudiyyəti haqqında məlumat verəcəyik. Daha sonra Oracle Vb-sının istifadəçi təhlükəsizliyi üsulları haqqında məlumat veriləcəkdir.

İkinci hissədə Oracle-ın istifadəçi təhlükəsizliyinə aid yüksək texnologiyalardan danışılacaqdır. İkinci hissənin sonunda işimizin tədqiqat obyekti olan Oracle Database Vault haqqında geniş məlumat verib onu digər yüksək texnologiyalar ilə müqayisə edəcəyik.

Üçüncü hissədə isə əvvəlində bank sektorunda Oracle VB-sının ümumi təhlükəsizliyi haqqında danışılacaq. Daha sonra indi Azərbaycan Banklarında istifadə olunan Oracle VB-sının isitifadəçi təhlükəsizliyi göstəriləcək və onun problemləri haqqında danışılıb indi istifadə olunan üsulla OVBV texnologiyası müqayisə olunacaqdır.

Dördüncü hissədə Oracle Database Vault-un bank sektoruna tətbiqinin əhəmiyyəti haqqinda məlumat veriləcəkdir. Daha sonda bank sektoruna aid Oracle Database Vault-un,Virtual Şəxi Verilənlər Bazasının, Oracle verilənlər bazasında Profil təhlükəsizliyinin tətbiqini praktiki göstəriləcəkdir.

I Fəsil. Oracle verilənlər bazasında ümumi istifadəçi təhlükəsizliyi

Oracle VB-sının təhlükəsizlik növlərindən biri istifadəçi təhlükəsizliyidir. İstifadəçi təhlükəsizliyi vasitəsi ilə bankın bazasına səlahiyyətsiz istifadəçilərin girişinin qarşısı alınır. Oracle VB-sının istifadəçi təhlükəsizliyi 2 yolla həyata keçirmək olar:

1) Oracle VB-sının ümumi istifadəçi təhlükəsizliyi; Burada istifadəçi təhlükəsizliyi deyəndə 2 üsul Profil təhlükəsizliyi və Səlahiyyət təhlükəsizliyi nəzərdə tutulur. Bu təhlükəsizlik hər bir Oracle VB-sında olur.

2) Oracle VB-sının istifadəçi təhlükəsizliyinin yüksək texnologiyaları; Oracle şirkəti bazanın istifadəçi təhlükəsizliyini təmin emək üçün texnologiyalar təqdim edir və bu texnologiyalar ayrıca lisensiya ilə satılır və mövcud bazanın üzərinə quraşdırılır. Bu texnologiyalar haqqında ikinci fəsildə məlumat veriləcəkdir.

Oracle Verilənlər bazasında ümumi istifadəçi təhlükəsizliyi haqqında məlumat verməmişdən əvvəl bazanın istifadəçiləri haqqında qısa məlumat verək.

1.1 Oracle verilənlər bazasında istifadəçilər

Oracle verilənlər bazasına daxil olmaq üçün əvvəlcədən mövcud olmuş istifadəçi adı olmalıdır və bir bazada hər bir istifadəçi adı vahid olmalıdır. Eyni adlı istifadəçi adı bir baza daxilində ola bilməz. Oracle VB-da iki cür istifadəçilər var:

1) Oracle qurularkən yaranan istifadəçilər

Oracle-ın qurularkən bəzi istifadəçilər avtomatik olaraq yaradılır. Bütün verilənlər bazasına SYS, SYSTEM, SYSMAN və DBSNMF administrator istifadəçiləri daxildir. Adminstrator istifadəçiləri yüksək səlahiyyətli istifadəçi adıdır və yalnız bu istifadəçilər bazanı başlatmaq və dayandırmaq, bazanın yaddaşını və saxlanılma yerini idarə etmək, bazanın adi istifadəçi adını yaratmaq və idarə etmək və s. səlahiyyətinə malikdirlər.

Bu administrator istifadəçi adlarının ən yüksəyi SYS istifadəçisidir. SYS-administrator istifadəçi adı bütün administrator funksiyalarını yerinə yetirir. Bazanın verilənlərin lüğəti üçün lazım olan əsas cədvəl və görünüşləri sys sxemasında saxlanılır.

Bu əsas cədvəl və görünüşlər Oracle VB-sının əməliyyatları üçün vacibdir. SYS sxemasında cədvəl yaratmaq məsləhət deyil [1].

Bu administratorda SYSDBA səlahiyyəti var ki, bu səlahiyyət istifadəçiyə bazanı backup və bərpa etməyə icazə verir. Əgər biz SYS istifadəçisinin şifrəsin dəyişmək istəyiriksə, onda ORAPWD əmrindən istifadə edərək yazmaq istədiyimiz şifrəni saxlayan yeni şifrə faylı yaratmaq lazımdır. Cədvəl 1.1-də ORAPWD əmrinin parametrləri göstərilmişdir.

ORAPWD əmrinin ümumi forması aşağıdakı kimidir.

orapwd file=filename [entries=numusers]

[force={y|n}] [ignorecase={y|n}]

Cədvəl 1.1 ORAPWD əmrinin parametrləri

file	Şifrəli fayla ad vermək üçün istifadə olunur.
entries	(Məcburi deyil) Bu fayldan istifadə edə biləcək maxsimum istifadəçi sayını göstərir.
force	(Məcburi deyil) Əgər y qiyməti verərsəz onda mövcüd faylın üzərinə yazılacaqdır.
Ignorecase	(Məcburi deyil) Əgər y qiyməti verərsəz onda case-sensitiv olmayacaqdır.

Bu istifadəçinin parolunu dəyişmək üçün ALTER USER və PASSWORD əmrindən istifadə etmək məsləhət deyildir.

OPAPWD file='orapworcl'

Enter password for SYS : new_password.

Əgər şifrə faylı mövcüd olarsa, onda səhv çıxır:OPW-00005 : File with same name exists-please delete or rename

Bu səhv sizə xəbərdar edir ki, bu adda başqa fayl var və biz fayla başqa ad verək. Əgər faylın üzərinə yazmaq istəyiriksə, onda force=y arqumentindən istifadə edirik. [2]

System-istifadəçisi backup və recovery, VB-sını təkmilləşdirməkdən başqa bütün səlahiyyətləri yerinə yetirir. Bu istifadəçi adının sxemasında cədvəl və görünüş yaratmaq

olur ancaq SYSTEM sxemasından administrator olmayan istifadəçiyə aid cədvəl və görünüşləri saxlamaq üçün istifadə etmək məsləhət deyil.

2) Ehtiyac daxilində yaradılan istifadəçilər

Oracle VB-sı qurulan zaman yaranan istifadəçi adlarından başqa digər istifadəçi adını yaratmaq istəyiirksə, onda CREATE USER əmri ilə yaradılır. İsitfadəçi yaradılarkən ona şifrə qoymaq tələb edilir.

```
SQL> create user roza identified by "oracle2016";
User created.
```

İstifadəçi adı yaradılandan sonra bu istifadəçi adına Connect səlahiyyəti verilməlidir ki, bazaya daxil ola bilsin. Əgər səlahiyyət verilməsə, bazaya qoşularkən səhv baş verir.

Əgər istifadəçinin birinci girişində şifrəsini dəyişmək lazım olarsa, onda istifadəçi adını yaradan zaman Password Expired əmrindən istifadə olunur.

Yaradılmış istifadəçi adının şifrəsini, profilini və s. dəyişmək üçün ALTER USER əmrindən istifadə olunur və bu əmrdən VBA istifadə edərək digər istifadəçilərin şifrəsini, profilini və s dəyişə bilər. Alter user əmrindən adi istifadəçilər də istifadə edib öz şifrəsini, profilini və s. dəyişə bilər.

Yaradılmış istifadəçi adının silmək üçün DROP USER əmrindən istifadə olunur.

```
SQL> drop user roza cascade;
User dropped.
```

İstifadəçi adı silinəndə Cascade xidmətedici sözündən istifadə olunarsa, onda istifadəçi silinəndə onun sxemasındakı obyektləri də silinəcəkdir və Verilənlər lüğətində bu sxemanın adı pozulacaqdır. Cascade xidmətedici sözündən istifadə etməklə bu istifadəçinin sxemasının içindəki bütün konstrantlar da silinəcəkdir.

Əgər istifadəçi bazaya qoşulu olarsa onda onu bazadan silmək mümkün olmayacaqdır. Bazaya qoşulan istifadəçini silmək üçün biz bu istifadəçi üçün session SİD və serial nömrəsini tapmalıyıq, bu istifadəçini bazadan çıxartmalıyıq ondan sonra bu istifadəçini silə bilərik. Silmək istədiyimiz istifadəçinin session id-ni və serial nömrəsini tapmaq üçün V$SESSION kitabxanasından istifadə edirik. Sonra KILL əmrindən istifadə edib bu istifadəçinin bağlantısını öldürürük.

Əgər biz istifadəçi adının bazaya müvvəqqəti qoşulmasını istəmiriksə, onda bu istifadəçi adını Account Lock əmri ilə klidə salmaq olar.

Əgər klidli olan istifadəçi bazaya qoşularsa, onda *"ERROR: ORA-28000: the account is locked. "* səhvi ekrana çıxır.

Əgər klidli olan istifadəçinin bazaya qoşulmasın istəyiriksə, onda Alter User əmrində Account UNLOCK əmrindən istifadə edirik.

1.2 Oracle verilənlər bazasında Profil təhlükəsizliyi

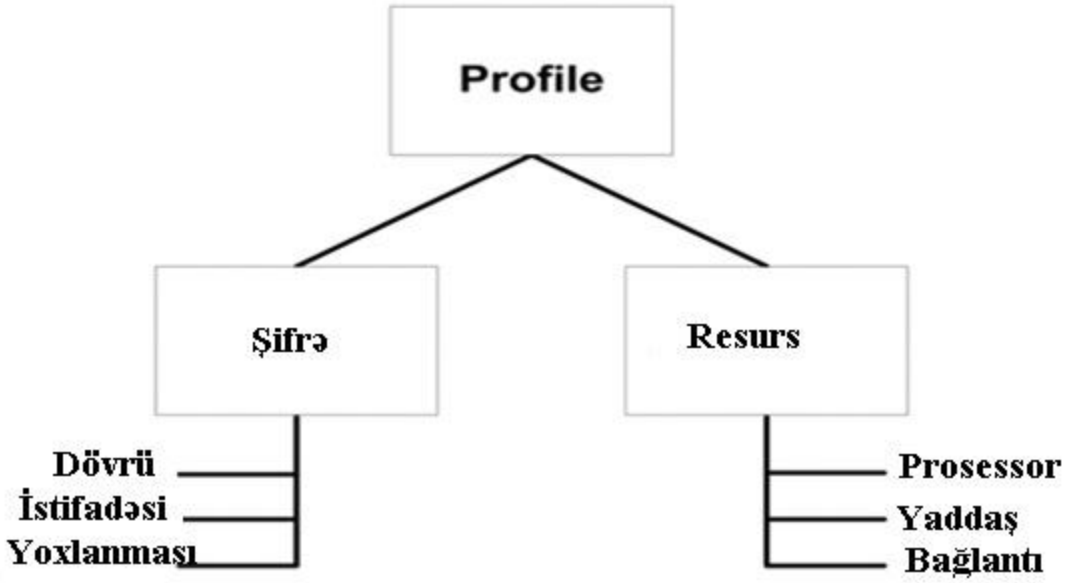
Oracle Vb-nın təhlükəsizliyi deyəndə həm şəbəkə təhlükəsizliyi həmdə istifadəçi təhlükəsizliyi nəzərdə tutulur. Oracle VB-sında informasiyanın təhlükəsizliyini təmin etmək üçün şəbəkə təhlükəsizliyi ilə yanaşı verilənlər bazasının istifadəçi təhlükəsizliyinə də əhəmiyyət verilməlidir. Oracle İstifadəçi təhlükəsizliyi ilə istifadəçi adları digər səlahiyyətsiz şəxslərdən mühafizə olunur yəni, istifadəçi adlarına səlahiyyətli istifadəçidən başqa istər daxili hətta administratorların istərsə də xarici şəxslərin girişinə qadağa qoyulur.

Azərbaycan Banklarında Oracle istifadə təhlükəsizliyi profil üzərində həyata keçirilir. VB-nın resurslardan istifadənin limitini təyin edən parametrlər toplusu profile adlanır. Profile CREATE PROFILE əmri ilə yaradılır. Yaradılmış profile istifadəçiyə CREATE USER, yaxud ALTER USER əmri ilə verilir.

İstifadəçi profili istifadəçilərin şifrələrinin parametrlərini və resursların istifadəsinə məhdudiyyəti idarə edir. Şəkil 1.1-dən görürük ki, Profil təhlükəsizliyin 2 növü var:

1) Şifrə təhlükəsizliyi

2) Resurs təhlükəsizliyi



Şəkil 1.1 Profil təhlükəsizliyin növü

1.2.1 Oracle istifadəçi təhlükəsizliyin Şifrə Profili ilə idarə edilməsi

İstifadəçi yaradılanda ona default şifrə profili təyin olunur. Şifrə Profili ilə Oracle istifadəçilərin istifadəçi adı klidə düşməmişdən əvvəl neçə dəfə uğursuz cəhdlərin sayını, hansı növ şifrədən istfadə edə bilməsini və oracle onu şifəni dəyişməyə məcbur etməmişdən əvvəl neçə gün köhnə şifrə ilə girə bildiklərini və s. göstərir. Şifrə profilin bütün parametrləri aşağıda qeyd etdiyimiz kimidir:

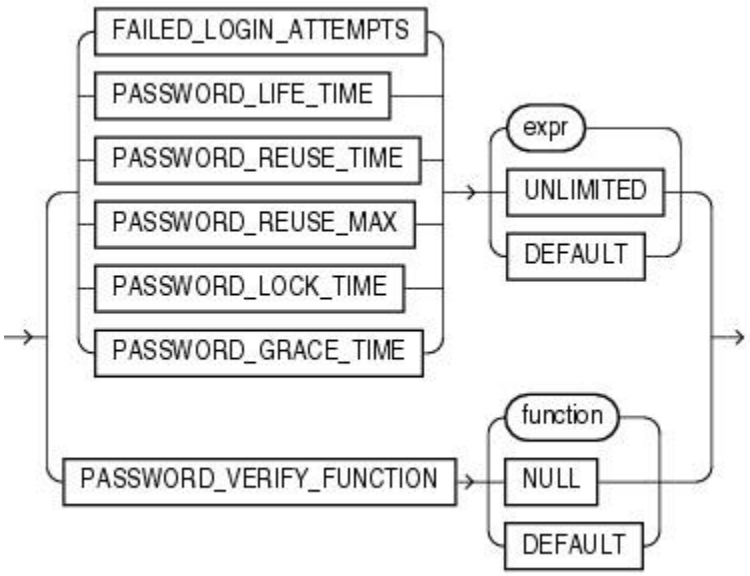
FAILED_LOGIN_ATTEMPTS-Oracle istifadəçisinin hesabının bloklanmasına səbəb olan uğursuz giriş cəhdinin maksimum sayını göstərir. Oracle 11g-də default olaraq 10-dur.

PASSWORD_LIFE_TIME- Bir şifrənin davamlılıq müddətini, yəni bir şifrənin maksimum istifadə ediləcəyi müddəti göstərir. Oracle 11g-də default olaraq 180-dır.

PASSWORD_GRACE_TIME- Bu parametri ilə göstərilən müddət başa çatdıqdan sonra istifadəçiyə şifrəni dəyişmək üçün verilən əlavə gün sayını göstərir. Default olaraq 11g-də 7 gün təyin olunur.

PASSWORD_LOCK_TIME- Uğursuz cəhddən sonra hesabın neçə müddət blokda qalacağını göstərir. Default olaraq 11g-də bir gün təyin olunur.

PASSWORD_REUSE_MAX - Bir şifrənin yenidən istifadə edilməsi üçün lazım olan minimum fərqli parol sayını göstərir. Şəkil 1.2-də Şifrə profilin parametrləri verilmişdir.



Şəkil 1.2 Şifrə profilin parametrləri

PASSWORD_REUSE_TIME - Bir şifrənin təkrar istifadə edilməsi üçün keçməsi lazım olan minimum müddəti göstərir.

PASSWORD_VERIFY_FUNCTION- bu funksiya şifrənin gücünü müəyyən edir.

Default şifrə profil təhlükəsizliyi güclü təyin etmir. Ona görə də biz daha güclü təhlükəsizliyi təmin etmək üçün istədiyimiz parametrdə şifrə profile yarada bilərik və bir bazda da istifadəçilərə adi müxtəlif parametrli profil yaratmaq olur. [3]

Yaradılmış profilin parametrini dəyişmək istəsək onda ALTER PROFİLE əmrindən istifadə olunur. Yaradılmış profili mövcud olan istifadəçi adına vermək üçün ALTER USER əmrindən istifadə olunur. Əgər limit parametrləri təyin olunubsa, istifadəçi limiti keçməməlidir. Əgər istifadəçi limiti keçərsə, onda istifadəçinin hesabı bloka düşür və hesabın blokdan PASSWORD_LOCK_TIME parametrində göstərilən vaxtdan tez çıxarılması üçün administrator

ALTER USER USERNAME ACCOUNT UNLOCK

əmri ilə yerinə yetirir.

Bankın Oracle VB-sinin Progress profilində bu parametrlərin qiyməti Cədvəl 1.2-dəki kimidir:

Cədvəl 1.2 Bankın Progress profili

FAILED_LOGIN_ATTEMPTS	7 cəhd
PASSWORD_LIFE_TIME	45 gün
PASSWORD_GRACE_TIME	Unlimited
PASSWORD_LOCK_TIME	0. 0006 gün
PASSWORD_REUSE_MAX	10
PASSWORD_REUSE_TIME	Unlimited

İstifadəçi adının hücumculardan qorunması üçün onun şifrəsi asan olmamalıdır. Asan şifrəli istifadəçi adı hücumçular tərəfindən tez sındırılır. Mürəkkəb şifrə yaratmaq üçün aşağıdakı təkliflərdən istifadə etmək məsləhət görülür.

- Şifrənin uzunluğu ən azı 8 simvol, ən çoxu 30 simvol ola bilər;
- Şifrədə ən az 1 böyük hərf, bir kiçik hərf, bir rəqəm və bir xüsusi simvol olması lazımdır;
- Şifrə rəqəmlə başlaması lazım deyil;
- Şifrə lüğətdə axtarılan sözün olması və çox işlənən sözün olması məsləhət deyil;

Şifrə yaradılanda çətin yaradılmalı və hətta yadda saxlamaq belə çətin olmalıdır. İstifadəçilərə mürəkkəb şifrə yaratmağın vacibliyi öyrədilməlidir. Məsəl üçün "dissertation" şifrəsi belə yazılmalıdır ki, mürəkkəb olsun. D@33e%t2t@1n

Oracle Vb-sının 11g-dən əvvəlki versiyalarının şifrəsi case-insensitive-dir yəni burada böyük və kiçik hərflər fərqlənmir. Oracle 11 g-də isə default olaraq şifrələr güclü təhlükəsizlik üçün case-sensitive-dir yəni burada böyük və kiçik hərflər fərqlənir. Ancaq SEC_SENSİTİVE-LOGON parametri ilə şifrəni case-sensitive-liyini idarə etmək olar. Default alaraq SEC_SENSİTİVE-LOGON parametri TRUE qiymət alır. Əgər onun qiymətini FALSE etsək və bazanı yenidən başlatsaq onda şifrə case-insensitive olacaqdır[4].

Əgər Oracle VB-sını 10g-dən 11g-yə yeniləsək onda istifadəçi yenilənəndən sonra şifrəni birinci dəfə dəyişdirənə qədər onun şifrəsi case-insensitive olur, dəyişəndən sonra

case-sensitive olacaq. DBA_USERS cədvəlinin PASSWORD_VERSIONS sütununda istifadəçilərin şifrələrin hansı versiyada olduğu göstərilir.

SQL>select username, password_versions from dba_users;

USERNAME PASSWORD_VERSIONS

RON 10g 11g

JANE 11g

RONB 10g

RON adlı istifadəçi adının şifrəsi 10g-də yaradılmışdır, şifrə11g-də dəyişdirilmişdir. JANE istifadəçi adının şifrəsi 11g-də yaradılmışdır. RONB adlı istifadəçi adının şifrəsi 10g-də yaradılmışdır, şifrə 11g-də dəyişdirilməmişdir. RONB adlı istifadəçinin şifrəsi böyük hərflə olur yəni o 10g-dəki şifrəsi ilə girmək istəsə, hər bir hərifini böyük hərflə yazmalıdır.

Oracle 11g şifrə faylını dəstəkləyir və bu şifrə faylının ignorecase parametri ilə şifrənin case-sensitive-liyini idarə edə bilərik. Bu ignorecase parametrinin default qiyməti n-dir yəni case-sensitive aktiv olur.

orapwd file=orapw entries=100 ignorecase=n

Əgər ignorecase=y olarsa, onda şifrə case-insensitive olur, yəni şifrənin böyük və kiçik hərflə yazılması fərq etməz.

Əgər Oracle 10g-də yaradılmış şifrə faylı varsa, onda baza yenilənəndən sonra bu faylı da yenidən yaratmaq lazımdır.

SHA-1 kriptokrafiya alqoritmi şifrə əsasında təhlükəsizlik qorxusuna qarşı şifrəyə qarışıq hərflər, xüsusi simvollar və çox ölçülü hərflər daxil edilir. Bu alqoritm istifadəçiyə mürəkkəb şifrə yaratmağa imkan verir və təcavüzkarın bazaya girişini çətinləşdirir.

1.2.2 Oracle verilənlər bazasında İstifadəçilər üçün resurs məhdudiyyətinin nizamlanması

Oracle VB-sında hər istifadəçi üçün sistem resursuna məhdudiyyət qoymaq olar. Resurs məhdudiyyətini qoymaq çox istifadəçili sistemlər üçün faydalıdır. Resursun bir və çox istifadəçi tərəfindən həddsiz sərfi bazanın başqa istifadəçilərinə ziyanlı təsir edir. Tək istifadəçili yaxud az miqyaslı çox istifadəçili VB sistemlərində resurs sərfinə məhdudiyyət qoymaq vacib deyildir.Çünki istifadəçilərin artıq resurs sərfi ziyanlı təsir etmir. [5]

Bazanın resursu VB Resurs İdarə etmə sistemi vasitəsi ilə idarə olunur. Bundan başqa profil vasitəsi ilə resursları idarə etmək olar. Belə ki, çoxlu istifadəçiyə default profil və ya fərdi profil yaradaraq resursları nizamlamaq olar.

Oracle VB-sı təhlükəsiz işçilərinə resursu məhdudiyyətləşdirən profil gücləndirməyə icazə verir. 3 növ resurs var : 1) bağlantı resursuı 2) session resursu

3) Müraciət etmə resursu.

Əgər bağlantı resursu limiti pozularsa qoşulan session artıq olarsa, onda tranzaksiyalar geri qayıdır və həmin session sona çatır.

Əgər session resursunun və müraciət etmə resursunun limiti pozularsa, onda əməliyyat dayandırılacaq, bütün cari statement-lər geri qayıdacaq və səhv çıxacaqdır.

Sistem resurslarının parametrləri aşağıdakılardır və Şəkil 1.3-də göstərilib.

1. Connect_Time- Bir session üçün maxsimum bağlantıda ola biləcək dəqiqələrlə vaxtı bildirir.

2. İDLE_TİME- session-un maxsimum vaxt qeyri-aktiv ola bilməsini dəqiqələrlə göstərir.

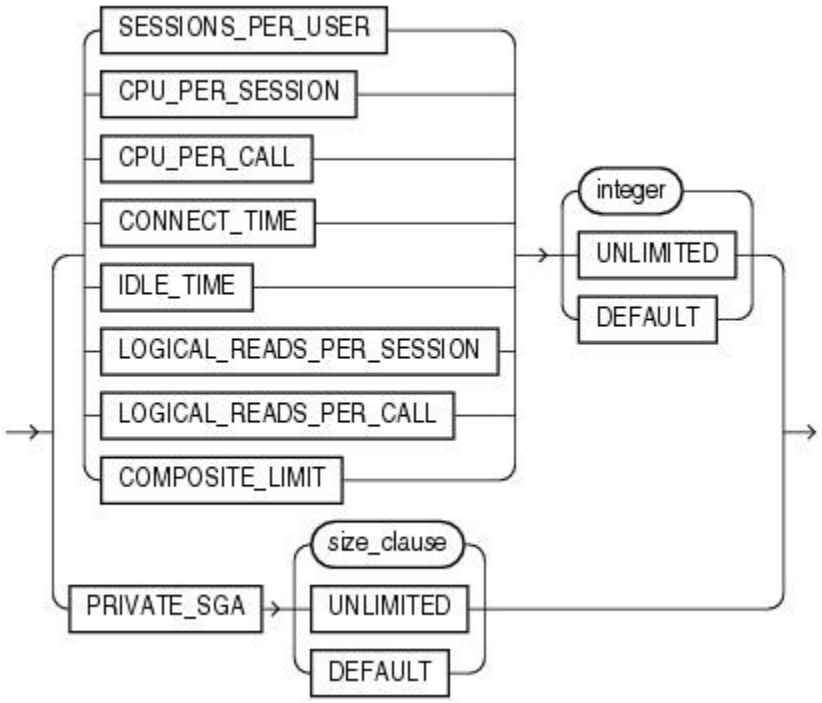
3. Sessions_per_user - Bir user eyni anda aça biləcəyi maxiumum session sayını ifadə edir.

4. CPU_PER_SESSION- Session əsasında istifadə edilə biləcək olan maximum CPU time qiymətini ifadə edir (bu qiymət (microsecond) burada saniyənin yüzdə biri olaraq ifadə edilir)

5. CPU_PER_CALL-Sessiion əsasında işlədilən sql və ya plsql 'lə əməliyyatlarında istifadə edilən maxiumum CPU time qiymətini ifadə edir. (qiymət mikrosecond)

6. LOGİCAL_READS_PER_SESSİON- Bir session-un oxuya biləcəyi maximum block sayını ifadə edİr. Burada oxunan blokun diskdən və ya memory oxunmasının fərqi yoxdur.

7. LOGİCAL_READS_PER_CALL - Session içərisində işlədilən sql və ya plsql 'lərdə oxuna biləcək olan maximum block sayını ifadə edir.



Şəkil 1.3 Sistem resurslarının parametrləri

8. COMPOSITE_LIMIT- Bu parametr ilə bir Session istifadə edə maximum qaynaq miqdarıdır. Bu qaynaq cpu_per_session, connect_time, logical_reads_per_session və private_sga dəyərlərinin cəmini ifadə edir.

9. Session SGA içərisindən istifadə edə biləcəyi maksimum ölçünü ifadə edir. Ancaq bu parametr paylanmış server olaraq yaradılmış olan instance 'larda etibarlıdır.[1,4]

Eyni bir profile həm şifrə parametrini həm də resurs parametrini özündə saxlaya bilir.

```
SQL> create profile conn_prof limit
 2 connect_time 240
 3 idle_time 30
 4 failed_login_time 5
 5 password_life_time 60
 6 password_reuse_time 60;
Profile created.
```

Təhlükəsizliyə görə default profildən istifadə etməmək və hər baza üçün yeni profile yaratmaq məsləhət görülür. Resursların artıq sərfi bazanı yükləyib çökdürə bilər ki, bu da bazanın bütün məlumatlarının itirilməsinə səbəb ola bilər.

1.3 Oracle verilənlər bazasinda Səlahiyyət təhlükəsizliyi

Oracle səlahiyyətlərin əsasını verilənlərə keçidi qadağa edən yaxud icazə verən imtiyazlar təşkil edir. İmtiyazlar dedikdə istifadəçinin SQL statement-lərin növlərinə hüququ, obyektlərə hüququ, paket yaxud prosedurları çalışdırmaq hüququ nəzərdə tutulur. Oracle-ın əmrləri və obyektləri müxtəlif olduğundan imtiyazlarda müxtəlif olur. Ümumilikdə imtiyazlar 2 yerə bölünür: Obyekt imtiyazları və Sistem imtiyazları. Obyekt imtiyazları istifadəçi tərəfindən müəyyən obyekt üzərindəki əməliyyatları təyin edir. Sistem imtiyazları istifadəçi tərəfindən administrator tapşırıqlarını yerinə yetirirməyi təyin edir. [6]

Baza daxilində çoxlu istifadəçilər var, onların çoxlu obyektlər üzərində çoxlu imtiyazları, çoxlu istifadəçinin imtiyazları idarə etmə üçün hüquqları vardır. Bu səbəbdən imtiyazları qruplaşdıran rollar yaradılır və bu rollar istifadəçiyə təyin edilir. İmtiyazları rollara təyin etmək olur yaxud rolları rollara təyin etmək olur.

1.3.1 Obyekt imtiyazların idarə edilməsi

Obyekt imtiyazları obyekt üzərində SQL statementləri icra etməyə yaxud obyektlərə girişə hüquq verir. Sxema obyekt imtiyazları xüsusi sxema obyekti üzərində müəyyən əməliyyatlar etməyə hüquq verir. Bu imtiyazlar isitfadəçiyə yaxud rollara verilir və aşağıdakı növləri var.

- Alter- cədvəli dəyişmək;
- Connect- bazaya qoşulmaq (create session);
- Delete –obyektlerdəki sətrləri silmək;
- Execute- procedurları, funksiyaları, paketləri icra etmək;
- Debug-çalışan kodun sazlanmaına icazə verir;
- Flashback – obyektlərdə flaskback əməliyyatına icazə verir;
- İndex- Başqa istifadəçinin cədvəlində indeks yaratmağa icazə verir;
- İnsert - Başqa istifadəçinin cədvəlinə məlumat daxil etməyə icazə verir;
- Query rewrite- view-dan seçilmiş sorğunun üzərinə yenidən yazır;
- Read – direktoriyanın növünün bazanın obyektlərinə tətbiqi;
- References - select imtiyazı olmadan cədvəlin üzərinə xarici açarı yaratmağa icazə verir;
- Select- başqa istifadəçiyə obyektdəki məlumatları seçməyə icazə verir;
- Under – subview və subtype icazə verir;
- Update – obyektlərə dəyişməyə icazə verir;
- Write- xarici table məlumatları yazır;

Obyekt sahibi və administrator səlahiyyətli şəxslər Grant əmrindən istifadə edərək başqa istifadəçiyə obyekt imtiyazlarıı verə bilər və Revoke əmri ilə başqa istifadəçidən öz obyektlərinin imtiyazını silə bilər. [7]

SQL > grant select on scott. emp to ronb;

Grant succeeded.

SQL > grant update, insert, delete on scott. dept to ronb;

Grant succeeded.

SQL > revoke delete on scott. dept from ronb;

Revoke succeeded.

Obyekt imtiyazları Grant Option ilə də verilə bilər. Bu əmr imtiyazları çoxlatmağa icazə verir. Misal üçün əgər scott adlı istifadəçi ronb istifadəçiyə öz obyekti olan emp cədvəlinə select etməyə icazə veribsə onda ronb bu imtiyazı başqa istifadəçilərə verə bilməz.

SQL > connect scott

Enter password : *******

Connected

SQL > grant select on emp to ronb;

Grant succeeded.

SQL > connect ronb

Enter password : *******

Connected.

SQL > select count(*) from scott. emp;

Count(*)

16

1 row selected.

SQL > grant select on scott. emp to jones;

grant select on scott. emp to jones;

*

ERROR at line 1

ORA-01031 : insufficient privileges

Əgər ronb adlı istifadəçinin də onda olan imtiyazların başqa istifadəçiyə verməyini istəyiriksə, onda scott adlı istifadəçi ronb adlı istifadəçiyə səlahiyyəti belə verməlidir.

SQL > connect scott

Enter password : *******

Connected

SQL > grant select on emp to ronb with grant option;

Grant succeeded.

SQL > connect ronb

Enter password : *******

Connected.

SQL > grant select on scott. emp to jones;

Grant succeeded.

Həmçinin Obyekt sahibi və administrator səlahiyyətli şəxslər all [privileges] əmri ilə bütün imtiyazlar başqa istifadəçiyə verilə bilər yaxud mövcud olan bütün imtiyazlar silinə bilər. Əgər silmə CASCADE CONSTRAİNTS parametri ilə silinərsə onda imtiyazı silinən istifadəçinin digər istifadəçiyə verdiyi imtiyazlarda silinəcəkdir.

SQL > revoke all on scott. dept from ronb cascade constraints;

Revoke succeeded.

DBA_TAB_PRIVS Verilənlər lüğətinin aşağıdakı sütunu var.

- GRANTEE- imtiyaz verilən istifadəçinin yaxud rolun adını saxlayır.
- OWNER - obyektin sahibinin adını saxlayır.
- TABLE_NAME - imtiyaz verilən obyektin adını göstərir.
- GRANTOR – İmtiyaz verən istifadəçinin adı
- PRİVİLEGE –verilən imtiyaz
- GRANTABLE – Grant Option parametrindən istifadə edəndə edilib edilmədiyni göstərir və Yes/No qiymətin alır.

Obyekt imtiyazını başqa istifadəçiyə verəndə imtiyaz verilən istifadəçi həmin obyektin bütün sütunları üzrə imtiyaza malik olur. Ancaq biz imtiyaz verilən istifadəçinin müəyyən sütunu görüb müəyyən sütunu görməməsin istəyiriksə onda biz sütun imtiyazdan istifadə edirik.

SQL> grant update (hiredate) on emp to jane;

Grant succeeded.

SQL> connect jane

Enter password : ******

Connected.

SQL> update scoot. emp set sal=sal+1;

update scoot. emp set sal=sal+1;

*

ERROR at line 1;

ORA-01031: insufficient privileges

SQL> update scoot. emp set hiredate = hiredate +1;

14 rows updated.

Qeyd edək ki, bu imtiyaz ancaq İnsert və update əmrləri üçün işləyir, Select əmri üçün işləmir. Sütun imtiyazlarına baxmaq üçün DBA_COL_PRIVS view –da baxmaq olar.[3,6]

1.3.2 Sistem imtiyazların idarə edilməsi

Sistem imtiyazları sistem səlahiyyətlərini yerinə yetirməyi idarə edir və bu imtiyazlar GRANT əmri ilə verilir, REVOKE əmri ilə mövcud səlahiyyət silinir. Sistem imtiyazları verilən istifadəçi verilən əmri istənilən obyektə tətbiq edə bilir. [7]

SQL> grant Update any table to ronb;

Grant succeeded.

Burada ronb adlı istifadəçi istənilən sxemadakı istənilən cədvəldə məlumatları dəyişə bilər. Sistem imtiyazların sayı 200-ə yaxındır və onlar Admin option parametri ilə verilsə demək imtiyaz verilən istifadəçi başqa istifadəçiyədə sahib olduğu imtiyazı verə bilər.

SQL > grant create any trigger to ronb with admin option;

Grant succeeded.

1.4 Oracle verilənlər bazasinda istifadəçi identifikasiyası

Verilənlərə, resurslara yaxud applicationlara giriş etmək istəyən istifadəçilərin, cihazların və başqa entitilərin kimlik təsdiqi etmək lazımdır. Kimlik təsdiqi-İdentifikasiya təhlükəsiz şəkildə verilənlərə, resurslara yaxud applicationlara giriş etməyi təmin edir.

İstifadəçi İdentifikasiya-verilənlərə, resurslara yaxud applicationlara giriş etmək istəyən istifadəçilərin kimliyinin təsdiqi prosesidir.

Biz Oracle VB üçün VB istifadəçilərini və VB olmayan istifadəçiləri təsdiq edə bilərik. Sadəlik üçün bütün VB istifadəçiləri üçün bir üsuldan istifadə edilir. Ancaq Oracle daha güclü təhlükəsizlik üçün bir VB istifadəçiləri üçün bir və daha identifikasiya üsullarından istifadə etməyi təklif edir. Bundan başqa Oracle-da VB administratorlarının təsdiqi üçün xüsusi identifikasiya prosedurası var çünki administratorlar xüsusi VB əməliyyatlarını-söndürmək yaxud başlatmaq kimi əməliyyatları yerinə yetirir ki, bunu administrator olmayan istifadəçilər yerinə yetirə bilmir.

Oracle-da VB administratorunun yeni SYSDBA yaxud SYSOPER səlahiyyətli istifadəçilərin identifikasiyası üçün aşağıdakı üsullar var:

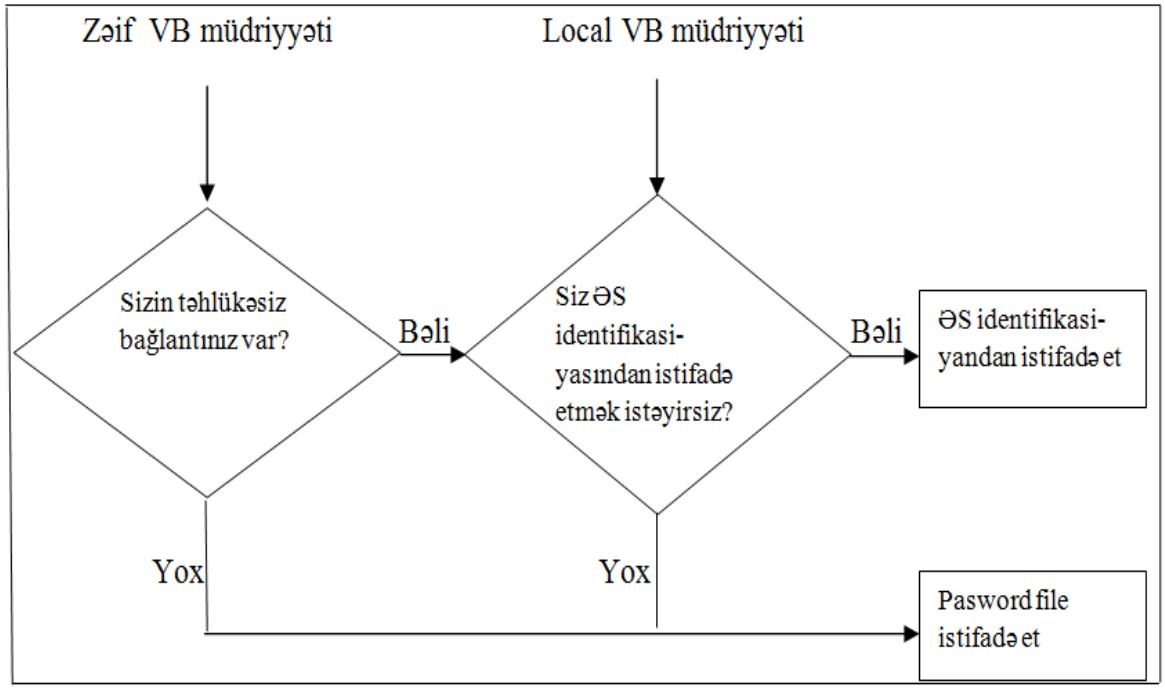
1)VBA üçün Güclü identifikasiya və Mərkəzləşdirilmiş İdarəetmə- Güclü identifikasiya SYSDBA və SYSOPER istifadəçilərinin girişini idarə edir. Administrator üçün bu növ identifikasiyada aşağıdakı hallarda istifadə olunur.

Şifrə faylın zəifliyi haqqında narahatlıq olanda.

Ciddi təhlükəsizlik tələb olunanda

Bazada idarəetməni ayırmaq istəyəndə Oracle İnternet Directory-dan istifadə olunur [8]

Şəkil 1.4-də identifikasiya seçimi arxitekturası verilmişdir.



Şəkil 1.4 VBA üçün Güclü identifikasiya və Mərkəzləşdirilmiş İdarəetmə identifikasiyası

Oracle İnternet Directory administratorların müəyyənləşdirilməsi üçün environment-dən asılı oalraq aşağıdakı üsullardan birini istifadə edir.

1) Directory identifikasiyası

2) Kerberos identifikasiyası

3) Secure Socket layer identifikasiyası

Güclü identifikasiya-dan istifadə üçün Ldap_Directory_Sysauth başlatma parametrinin qiymətini yes etmək lazımdır.

Alter System Set Ldap_Directory_Sysauth = Yes;

Ldap_Directory_Access parametrinin qiymətini Password yaxud SSL etmək lazımdır.

Alter System Set Ldap_Directory_Access = Password;

Alter System Set Ldap_Directory_Access = SSL;

Directory identifikasiyasından istifadə olunarsa, onda roza adlı istifadəçi odb adli serverə SYSDBA kimi qoşulmaq istəsə, SQL* Plus belə yazmalıdır.

Connect roza@odb as SYSDBA

Enter Password : roza123;

Kerberos və Secure Socket layer identifikasiyasından istifadə olunarsa, onda odb adlı serverə SYSDBA kimi qoşulmaq lazım olarsa, SQL* Plus belə yazmalıdır. Connect /@odb as SYSDBA

Əgər Ldap_Directory_Access parametrinin qiyməti NONE olarsa onda administratorlar üçün Güclü identifikasiyadan istifadə etmək olmur.

2)Əməliyyat Sistemi identifikasiyası-Bu identifikasiyadan istifadə etmək üçün əvvəlcə istifadəçi üçün əməliyyat sisteminin istifadəçi accountu açılmalıdır. Bu istifadəçini ƏS-nin OSDBA və OSOPER qrupuna daxil edilməlidir. Remote_Login_Passwordfile parametrinin qiyməti NONE təyin edilməlidir.Bunu edəndən sonra istifadəçi administrator kimi bazaya aşağıdakı əmrlə qoşula bilər. [9]

connect / as sysdba

connect / as sysoper

Bu qoşulma heç də etibarlı deyildir. Ona görə də bu bağlantını etibarsız etmək lazımdır. Bunun üçün $ORACLE_HOME/network/admin ünvanda yerləşən Sqlnet. ora faylına aşağıdakı əmri əlavə etməliyik.

Sqlnet. Authentication_Services=(None)

3)Şifrə fayl identifikasiyası-Əgər Administratorlar ƏS-nin OSDBA və OSOPER qrupuna daxil deyillərsə, onda onlarin VB-ə qoşulması üçün passüord file içinə daxil edilməlidir.

Şifrə fayl aşağıdakı əmr vasitəsilə yaradılır.

orapwd file=filename [entries=numusers]

[force={y|n}] [ignorecase={y|n}]

Oracle adi istifadəçilərə verilənlər bazasına girməyə icazə verməmişdən əvvəl aşağıdakı üsullarla onların kimliyini müəyyən edir [8,9].

1)Verilənlər bazasının identifikasiyası-burada istifadəçinin təsdiqi, müəyyənləşdirilməsi VB tərəfindən olur.

2)External identifikasiyası- istifadəçinin təsdiqi,müəyyənləşdirilməsi əməliyyat sistemi yaxud şəbəkə sistemi tərəfindən olursa,buna external identifikasiyası deyilir.

3)Global identifikasiyası və səlahiyyəti-Global rola malik istifadəçilərin təsdiqi, müəyyənləşdirilməsi Təhlükəsiz Soket Səviyyəsi tərəfindən olarsa,buna global identifikasiyası deyilir.

4)Proxy identifikasiyası-istifadəçinin identifikasiyası üçün middle-tier server istifadə edən prosesdir.

II Fəsil. Oracle VB-da istifadəçi təhlükəsizliyi üçün yüksək texnologiyalar

Oracle şirkəti verilənlərin təhlükəsizliyini yüksək səviyyədə təşkili üçün yüksək texnologiyalar təqdim edirlər. Texnologiyaların hər biri müxtəlif xüsusiyyətə malikdir. Xüsusiyyətlərinə görə texnologiyalar 4 qrupa bölünürlər.

1) Monitoring & Blocking (Nəzarət və Bloklama) - ən yaxşı təhlükəsizlik monitoring & blocking-sız tamamlanmır. Bu qrupa daxil olan texnologiyanın işi birinci başlayır və o, bazaya səlahiyyətsiz qoşulmaq istəyən istifadəçiləri blok edir.

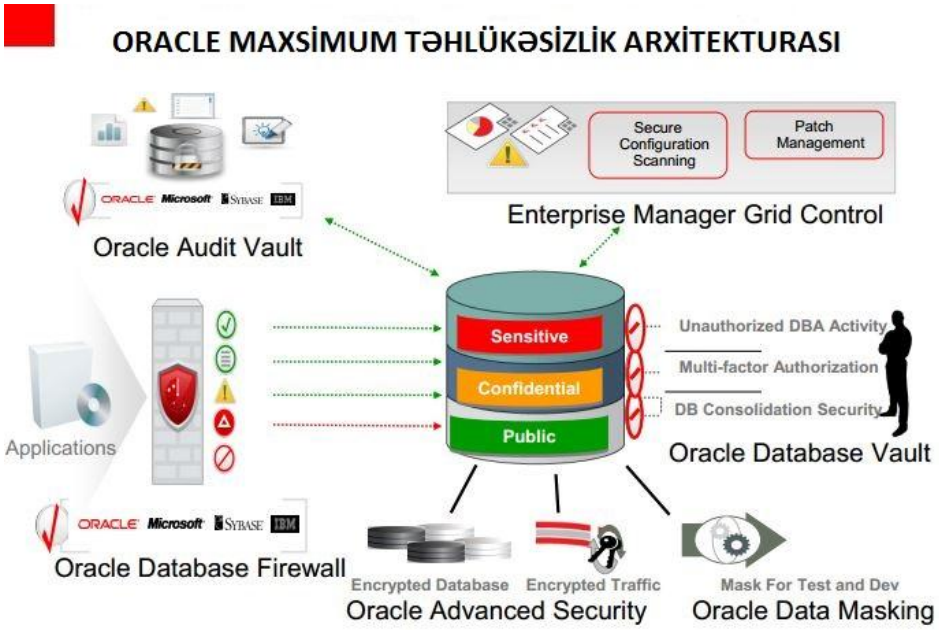
2) Access Control - (Girişə nəzarət)VB-sına keçidi nəzarət edirlər. Bu qrupa daxil olan texnologiyalar yüksək səlahiyyətli istifadəçilərin cədvələ girişinə qadağa qoyur.

3) Auditing & Tracking - verilənləri izləyib təhlükəsizliyi qoruyurlar.

4) Encryption & Masking - verilənlərin qorunması üçün xaricdən keçiddi nəzarət edir. Şəkil 2.1-də hər bir qrupa aid texnologiyalar verilmişdir.

Şəkil 2.1 Oracle VB-sının isitifadəçi təhlükəsizlik istiqaməti

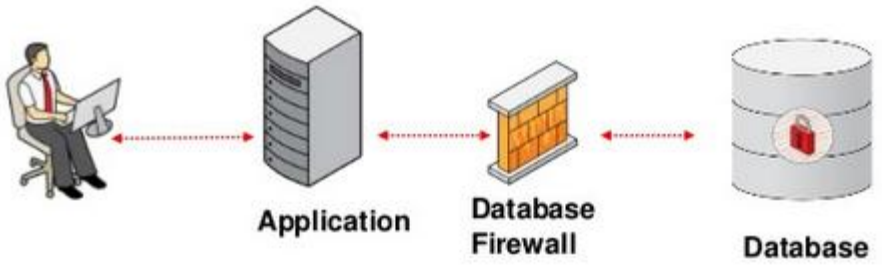
Bazada istifadəçi təhlükəsizliyini təmin etmək üçün göstərilən texnologiyalardan birini və ya bir neçəsini eyni zamanda istifadə etmək olar. Maxsimum təhlükəsizliyi təmin etmək üçün oracle audit vault, oracle database firewall, enterprise grid control, oracle database vault, oracle advanced security, oracle data masking texnologiyalarını birlikdə istifadə etmək lazımdır. Şəkil 2.2-də maksimum təhlükəsizliyin arxitekturası verilmişdir.



Şəkil 2.2 Oracle Maxsimum təhlükəsizlik arxitekturası

2.1 Oracle verilənlər bazası Firewall (OVBF)

OVB Firewall, Oracle-ın təhlükəsizlik sistemlərindən biridir və Monitoring & Blocking qrupuna daxildir. O, daxili və xarici hücumların verilənlər bazasına çatmasının qarşısının alınmasına kömək edir və vb üçün ilk müdafiə vəzifəsini daşıyır. O, Oracle VB-da verilənləri qoruyur və hücumları blok edir. O, şifrələmə və istifadəçi identifikasiyası kimi, mövcud təhlükəsizlik xüsusiyyətlərini artırmaq və zəifliklər qiymətləndirməyi təmin edir. Quraşdırılması, idarəçiliyi olduqca asandır. Rəqib məhsullara görə də olduqca aşağı xərc tələb edir Oracle Database Firewall şəbəkədə quraşdırılan və idarə olunan bir məhsuldur.[10] OVBF, şəbəkədə verilənlər bazasına edilən SQL sorğularını analiz edir, izləyir , bloklayır, dəyişdirir ya da birbaşa olaraq verilənlər bazasına çatdırması vəzifəsini daşıyır. İnkişaf etdirilən xüsusi sorğuları sayəsində SQL Injection hücumlarını asanlıqla başa düşür, bu tipli hücumları bloklaya bilir və istənildiyi halda müəyyən alıcılara mail olaraq göndərə bilir. Şəkil 2.3-də OVBF-ın artitektutası verilmişdir.

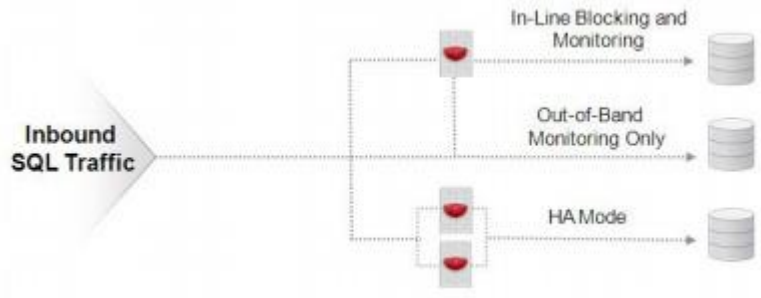


Şəkil 2.3 Oracle Database Firewall

SQL Injection hücumlarını SQLin sorğusunun araşdıraraq anlaya bilir. Çox yüksək səviyyədə bazasının təhlükəsizliyini təmin edir.

Oracle VB Firewall şəbəkədə, verilənlər bazası və application server üzərində yerləşir. Müşrərilər onların biznes tələblərinə uyğun növ Firewall-lar seçə bilərlər.

- In-line blocking and monitoring mode
- In-line monitoring mode
- Proxy blocking and monitoring mode
- Out-of-band monitoring mode



Şəkil 2.4 Oracle Verilənlər bazası Firewall Mod

2.2 Oracle virtual şəxsi verilənlər bazası (OVŞVB)

Oracle virtual şəxsi verilənlər bazası sətir və sütün səviyyəsində bazaya girişi idarə etmək üçün təhlükəsizlik siyasətini yaratmağa şərait yaradır. OVŞVB tətbiq edilmiş cədvəl, görünüş yaxud sinonimə SQL sorğusu göndəriləndə bu sorğuya dinamik WHERE şərt əlavə edir. VŞVB-nın siyasəti sizin təhlükəsizlik tələblərinizdən asılı olaraq sadə və mürəkkəb ola bilər, ancaq həmişə Oracle təyin etdiyi tətbiqi məzmundan

istifadə edir. Ocacle-ın bu texnologiyası sətir səviyyəsində virtual olaraq informasiyanı səlahiyyətsiz şəxslərdən gizlədir. Bunun sayəsində administratorun, hesabatın, Fəlakətin kəşfinin rahatlığı üçün biz müxtəlif isitfadəçilərin, müxtəlif departamentlərin, müxtəlif şirkətlərin informasiyalarını eyni cədvəldə saxlaya bilərik.

Şəxsi virtual verilənlər bazası birbaşa cədvəllər, görünüşlər yaxud sinonimlər üzərində qorunma təşkil edir. Bu prosess bir başa bu obyektlərə tətbiq edildiyi üçün, istifadəçilər bu obyektə müraciət etdiyi an, təlükəsizlikdən yan keçmək şansı olmur. İstifadəçi birbaşa və ya dolayı yolla ŞVVB-sının qoruduğu bazaya müraciət edirsə, onda bazaya istifadəçinin sorğusuna WHERE şərtini əlavə edir[11].Bu WHERE şərti təhlükəsizlik siyasətini yerinə yetirən funksiya qaytarır. ŞVVB-nin 3 komponenti var

- Application Context
- PL/SQL Function
- Security Policies

ŞVVB siyasəti SELECT, INSERT, UPDATE, INDEX, və DELETE əmrli sorğulara da tətbiq olunur. ŞVVB yerinə yetirmək üçün dinamik WHERE şərtini yaradan funkiya yaradılmalıdır və bu funksiya-ya təhlükəsizlik siyasəti əlavə olunmalıdır. Bu funksiya təhlükəsizlik administratorunun sxemasında yaradılmalıdır və funksiyanın sxema və obyekt adlarından ibarət arqumentləri olmalıdır.

Funksiyanı yaradandan sonra OVŞVB-sının siyasəti yaradılmalıdır. Bu siyasət cədvəl, görünüş və ya sinonim ilə funksiyaya birləşməlidir. Siyasət DBMS_RLS paketindən istifadə edərək yaradılır və bu zaman istifadəçi ya SYS olmalıdır yada istifadəçinin DBMS_RLS paketi üzərində EXECUTE imtiyazı olmalıdır.Sətir səviyyəli OVŞVB başa düşmək üçün misala baxaq.

Scott sxemasında emp və dept cədvəlləri var. Emp cədvəlinin hər bir işçisi dept cədvəlində bir qiyməti var. Bazanın istifadəçiləri emp cədvəlinə sorğu göndərəndə yalnız öz departamentinin işçilərinin məlumatını görsün, dəyişdirsin və ya məlumat daxil etsin.

Sys_context('HR_CONTEXT','DEPT') funksiyasından istifadə edərək istifadəçinin hansı departamentə aid olduğunu təyin etmək olar.

```
SQL> CREATE OR REPLACE
  2 FUNCTION rls_dept (obj_owner in varchar2; obj_name in varchar2)
  3 return varchar2
as
deptno number;
predicate varchar2(200);
begin
deptno:= Sys_context('HR_CONTEXT','DEPT')  ;
if deptno is null then
predicate:= '1=2';
else
predicate:= 'deptno='||deptno";
end if;
return (predicate);
end rls_dept;
Function created;
```

RLS_DEPT funksiyasının qaytardığı predicate dəyişəni dinamik WHERE şərtinə əlavə edilir.

İndi VŞVB-sının siyasətini yazaq.

```
SQL> BEGIN
  2 DBMS_RLS.ADD_POLICY(
  3 object_schema=> 'SCOTT',
  4 object_name=> 'EMP',
  5 policy_name=>'restrict_dept_policy',
  6 function_schema=>'SCOTT'
  7 policy_function=> 'rls_dept'
  8 );
END;
/
PL/SQL procedure successfully completed.
```

İndi bizə istifadəçinin departament nömrəsini əldə etmə üçün context yaratmaq lazımdır.

```
sql> create context HR_CONTEXT using set_hr_context;
context created.
sql> create or replace procedure set_hr_context
 2 (
 3 deptno in number
 4 )
 5 is
 6 begin
 7 dbms_session.set_context('HR_CONTEXT','')
 8 end;
/
Procedure created.
```

Indi bu siyasəti yoxlayaq. Departamentə adi olmayan istifadəçi olarsa, onda o cədvəldə heçnə görməyəcəkdi.

ADD_POLİCY procedurunun bəzi xüsusiyyətləri var ki, onlar vasitəsiylə təhlükəsizliyi daha da gücləndirmək olar.

Statement_types xüsusiyyəti ilə siz istifadəçilərin cədvəl üzərindəki əməliyyatlarını nizamlaya bilərsiz.

Static_policy - siyasətin dinamik, static olmağını müəyyən edir. Default olaraq False qiymətin alır.

Long_Predicate- əgər funksiya nın qaytardığı qiymət 400 baytdan çoxdursa onda bu xüsussiyyətə True qiyməti mənimsətmə lazımdır.

Update_check- Əgər siyasət tətbiq ediməmişdən əvvəl və sonra İnsert və Update sorğusunun qiymətini yoxlamaq istəyiriksə, onda bu xüsusiyyətin qiymətini True edilməlidir.

Sətir səviyyəli təhlükəsizlik kimi sütun səviyyəli təhlükəsizliyi də yaratmaq olar və sütun səviyyəli təhlükəsizlik ancaq cədvəl və görünüşə tətbiq oluna bilər, sinonimə etmək olmaz.[3,11].

VŞVB-sı tətbiq ediləndə istifadəçi məhdudiyyət olduğunu hiss etmir, yəni o bütün informasiya görmək üçün sorğu verəndə, VŞVB- sı sorğunu verən şəxsi görə biləcəyi bütün sətirləri qaytarır, cədvəlin bütün sətirlərini qaytarmır.

VŞVB-nın faydalı xüsusiyyətləri:

1) Verilənlərin təhlükəsizliyi verilənlər səviyyəsində idarə olunur və bütün sorğulara tərbiq olunur.

2) Prosedur və siyasətlər istifadəçilərə, girisi metoduna baxmayaraq bir dəfə qurulur.

3) VB-sında verilənləri məntiq ayırmaq üçün triggerləri, görünüşləri və s. ehtiyacı azaldır, bunun vasitəsilə performs artır və texniki tələb azalır.

2.3 Oracle Label təhlükəsizliyi

Oracle Label təhlükəsizliyi (OLT) Virtual Şəxsi verilənlər bazasının əlavəsi olaraq Oracle-ın 8-ci versiyası ilə çıxmağa başladı və bazanın cədvəlləri üçün sətir səviyyəli təhlükəsizlik təmin edir.

Gizli verilənlərə təcrübəli nəzarət üçün təşkilatlarım verilənlərini təhlüəsiz olaraq bir biirndən ayrı qorumaq lazımdır. Ancaq müştəri həssas məlumatları üçün hər biri üçün ayrıca məlumat bazalarında saxlanılması baha olur və lazımsız yer tutur.

OLT verilənləri eyni cədvəldə yerləşsə də işarə qoyaraq ayırır. Bu bacarıqdan istifadə edərək bazada eyni cədvəldə müxtəlif məlumat saxlamaq olar.

Həssas verilənlərə giriş istifadəçinin işarəsi ilə müqayisə olunur. Əgər istifadəçinin işarəsi sətrin işarəsi ilə uyğun gəlirsə, onda girişə icazə verilir. OLT cədvələ tətbiq edəndə əlavə sütun yaranır və müqayisə bu sütun ilə aparılır və bu təhlükəsizlik texnologiyası yüksək səlahiyyətli şəxslərin keçidini qadağa edir. Bu texnologiya çoxlu təşkilatların, kompaniyaların bir program paylaşmasında faydalıdır [12].

Oracle VB-sını qurarkən default olaraq oracle Label Təhlükəsizliyi qurulmur. OLT-ni mövcud bazanın üzərinə qurmaq üçün Oracle Universal İnsaller texnologiyadan

istifadə edilir. OLT-nin LBACSYS isitfadəçi adı var, bu ad qurulmadan sonra onu aktiv etmək lazımdır.

OLT-nin qurulmasıdan sonra cədvələ tətbiq etmə üçün siyasət yaradılmalıdır və bu siaysətin yaratmaq üçün aşağıdakı addımlar həyata keçirmək lazımdır.

Addım 1 : Siyasəti yaratmaq.

Biz siyasətin adını, label sütununu və məcburu parametrləri təyin etməliyik.

1) Enterprise Manager Database Control ilə LBACSYS istifadəçi adına daxil olaq.

2) Server taba klik edək

3) Security hissəsində Oracle Label Security klik edək. Burda OLT siyasəti səhfəsi mövcuddur.

4) Create buttonuna basırıq və yeni label siyasəti yaratmağa başladırıq.

5) Siyasətin adını, label sütununu və məcburu parametrləri təyin edirik.

Name hissəsində siyasətin adını yazırıq.

Label Column hissəsində Label sütunu üçün ad seçirik. Sonra siyasəti cədvələ tətbiq edəndə, o cədvələ sütun əlavə edirik. Default olaraq işarə sütunun verilənlərinin tip number(10) olur.

Hide Label Column- sütunu gizlətməyi seçə bilərik.

Enabled: Siyasətin aktiv və yaxud passiv olmağını seçə bilərik.

6) Ok düyməsin basırıq.

İndi biz yaratdığımız siyasəti Oracle Label Security Policies səhifəsində görərik.

Addım 2:Yaratdığımız siyasət üçün işarə komponentini yaradaq.

1) Oracle Label Security Policies səhifəsində indicə yaratdığımız siyasəti seçirik.

2) Edit Label Security Policy səhifəsindən, Label Components tabını seçirik.

3) Add 5 Rows ilə siyasət üçün səviyyə müəyyən edirik.

Yaradacağınız səviyyə üçün uzun, qısa adını və tağın nömrəsi daxil edilir. Tağın nömrəsi uyğun səviyyəsinin həssaslığından asılır.

4) Apply düyməsi basılır.

Addım 3: Siyasət üçün Verilənlər işarəsi yaradılır.

1) Label Security Policies səhifəsində işarə əlavə etmək istədiyimiz siyasəti seçirik.

2) Action qutusundan Data Labels seçirik və go düyməsin basırıq. Data labels səhifəsi açılır

3) Add düyməsin basırıq. Create Data Label səhifəsi açılır.

4) Numerik tag hissəsində işarəni vahidliyini təyin etmək üçün nömrə daxil edirik.

Level: siyahıdan səviyəni seçirik.

5) İşarəyə əlavə etmək üçün Compartment seçirik sonra add düyməsin basırıq.

6) İşarəyə əlavə etmək üçün Group seçirik sonra add düyməsin basırıq.

7) Ok düyməsin basırıq.

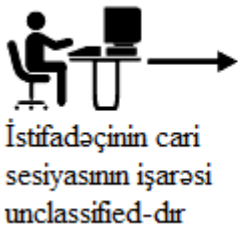
Addım 4: Siyasət üçün səlahiyyətli istifadəçilər müyyən edirik.

Addım5: Baza cədvəlinə siyasət təqdim edirik.

Addım6: Cədvəlin sətrinə işarə əlavə edirik.

İşarələrin 3 növü var: Unclassified, Highly_sensitive, sensitive [3,10].

Şəkil 2.5-də verilmiş cədvələ cari istifadəçinin işarəsinin növü unclassified-dir.



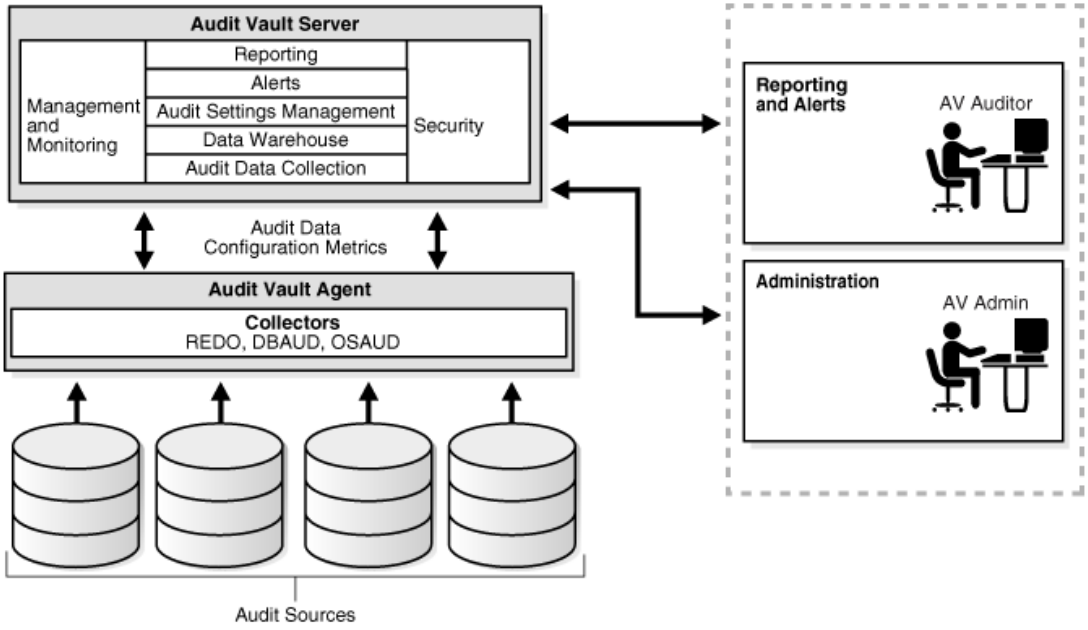
GRADE	RATE	ROW LABEL
Manager	600	UNCLASSIFIED
Senior	400	UNCLASSIFIED
Director	750	HIGHLY_SENSITIVE
Principal	600	SENSITIVE
Senior	450	SENSITIVE

Şəkil 2.5 OLT ilə qorunmuş cədvəl

2.4 Oracle Audit Vault

Oracle AV güclü texnologiyadır ki, o, verilənlərin təhlükəsizliyi üçün yoxlama verilənlərini birləşdirir, aşkar edir, nəzarət edir, xəbərdarlıq edir. OAV həm hansı verilənlərə kimlərin, nə vaxt daxil olduğunu izləyir, həm də verilənlərin izləməsini saxlayan loglar və audit verilənlərin dəyişdirilməməsimə, saxtaşdırılmamasına qaranti verir. Loglarda, audit verilənlərdə bazada olan bütün istifadəçilərin – o cümlədən VBA-

ların bütün əməliyyatları yadda saxlanılır. Bütün əməliyyatlar interveys vasitəsi ilə idarə edilir.



Şəkil 2.6 Oracle Audit Vaultun Arxitekturası

Başqa sözlə, OAV aşağıdakı üstünlükləri vardır.

- Çoxlu sistemdən gələn informasiyanı birləşdirir.
- Ardıcıl və imtiyazlı istifadəçilər ilə bağlı məlumatların dəyişikliklərini aşkar edir.
- Yoxlama fayllarını dəyişdirilmədən və saxtlaşdırılmadan qoruyur.

Şəkil 2.6-də Oracle Audit Vaultun yüksək səviyyəli arxitekturası göstərilmişdir.

Oracle AV-ın 3 anlayışı var: AV Server, AV agents və AV collector.

Bundan əlavə OAV komponentləri də var. Şəkil 2.7-də komponentləri göstərilmişdir.

Hesabatlar- OAV imtiyazlı istifadəçilərin fəaliyyətinə və verilənlər bazasının strukturlarının dəyişikliklərinə geniş nəzarət üçün daxili hesabatlar verir. Hesabatlarda kimin, nə vaxt, harda, nə iş gördüyünü bütün məlumatları ilə göstərilir. Oav-ın ən son versiyası Oracle Application Express texnologiyası üzərində yeni hesabat interfays verir. Bu yeni hesabat rəngli qrafik və diaqramlar yaratmağı, eləcə də yeni formatlı hesabat yaratmağa imkan verir.

Şəkil 2.7 OAV komponentləri

Xəbərdarlıq(Alert) – OAV təhlükəsizlik işçilərinə səlahiyyətsiz və ya süni şəkildə giriş etmiş istifadəçilərin fəalyyətini aşkar edib və xəbərdarlıq edir. OAV sistem və istifadəçilər üçün xəbərdarlıq siqnalları yaradır.

Alert application cədvəldə dəyişilik edəndə, səlahiyyətli istifadəçi yaradanda audit cədvəlinə birləşdirilə bilər. Məsələn, kimsə biznes məlumatlarının saxlayan gizli cədvələ giriş etsə, onda alert yaradıla bilər. OAV alertlərin fəaliyyətinin səbəblərinə adi qrafiki xülasələr verir.

Siyasətlər-Oracle Audit Vault Oracle verilənlər bazasının audit parametrlərini mərkəzləşdirilmiş idarə etməyi, İT təhlükəsizliyin və daxili auditorların iş sadələşdirilməsini təmin edir. Çoxlu işlərdə audit siyasətləri üçün monitorlar tələb edilir. OAV Audit Vault console-dan mərkəzləşdirilmiş audit siyasətini təmir edir. Bu siyasət İT təhlükəsizliyin və daxili auditin işini asanlaşdırır.

Təhlükəsizlik- Audit verilənlər işin fəaliyyətinin vacib yazısıdır. Hesabatların və araşdırmaların bütövlüyünü təmin etmək üçün auditverilənlər dəyişilikdən müdafiə olunmalıdır və verilənlər təhlükəsiz deposunda saxlanılır, şəbəkə üzərindən və OAV daxilində transferdən qorunur [13]

Mənbədən tranfer zamanı audit verilənlər başqaları tərəfindən oxunmasın və saxtalaşdırılmasın deyə şifrələnir.

Audit verilənlər təşkilatların yüksək təhlükəsizliyinə köməkdə və daxili və xarici siyasətə əməl edilməsində vacib rol oynayır.

2.5 Oracle Database Vault

Bir çox firmalarda, banklarda, dövlət qurumlarında bir firewall alaraq təhlükəsizliklə əlaqədar problemlərini həll etdiklərini düşünülür. Ancaq yalnız firewall verilənlərin təhlükəsizliyini təmin etmir. Firewall ilə xaricdən ediləcək hücumlara qarşı tədbirlər alınarkən, daxildən edilən hücumlara qarşı çox tədbir alınmadığı araşdırmalarda ortaya çıxmışdır. Xüsusilə bazanın çalışdığı server üzərində məlumatın qorunması ilə əlaqədar bir iş aparılmır. VBA səlahiyyətinə sahib bir istifadəçinin, bazasında hər cür səlahiyyətə sahib olduğu və hətta fərqli kompüterlərdən bağlanıb eyni əməliyyatları edə biləcəyi düşünüldüyündə, meydana gələ biləcək təhlükəli hallar düşünülmək məcburriyyətindədir. Bir VB admininin bazada necə hər məlumatı görməsi təhlükəlidirsə, eyni zamanda fərqli kompüterlərdən bağlanıb eyni işləri etməsi də təhlükəlidir.Oracle VB təhlükəsizliyi həllərindən biri olan Oracle Database Vault, yuxarıda bəhs edilən problemləri həll etmədə köməkçi olacaq bir tətbiq olaraq təkliflə bilər.

Şəkil 2.8 OVBVkomponentləri

Oracle Database Vault Oracle bazasının xüsusi ərazisinə istənilən istifadəçilərin xüsusiylə də administratorların keçidini məhdudiyyətləşdirir. Burada bazaya giriş günün saatlarına görə, həftənin günlərinə, İP ünvanına, application-nın adına görə və identifikasiya üsullarına və s. görə idarə edir.

O, mövcud bazanın üzərinə quraşdırılır və əsas məqsədi vəzifələri ayıraraq bazanı daxildəki təhlükədən bazanı qoruyur. Məsəl üçün bunun sayəsində biz adminsitratorun işçilərin maaşını, müştərilərin tibbi məlumatlarını və başqa gizli məlumatlarını görməsini məhdudiyyətləşdirə bilər. OVBVtexnologiyası bazanın təhlükəsizliyinə görə SQL əmrlərini idarə etmək üçün istifadə olunur.

ODV sql əmrinin icrasından əvvəl (hətta CONNECT, TABLE, TRUNCATE TABLE, and DROP TABLESPACE əmrlərindəndə əvvəl) yoxlama aparır və bu yoxlama əmrin icrasına icazə verərsə əmrlər icra olunur. Command Control bazaya girişi xüsusi subnetlərə, application server, and program, aplicationdan bazaya gedən müəyyən olunmuş yola görə məhdudlaşdıra bilər.[14]

Faktor qurularaq bazaya girişi IP address, host adı və istifadəçi adına görə yoxlayıb nəzarət edir. Şəkil 2.5-də təhlükəsizliyi təmin etmək üçün ODV-nin komponentleəri verilmişdir.

Realms-Realm baza daxilində "mühafizə olunmuş zona"-dır. Burada olan verilənlər administrator kimi səlahiyyətli şəxslərdən

mühafizə olunur. Oracle Database Vault Administratoru Realm yarada bilir və gizli baza obyektlərini onun daxilinə əlavə edir və lazım olan istifadəçi və ya rollara buraya keçidə icazə verir.

Realm-bir cədvəli, çoxlu cədvəli, bütöv application sxemanı və ya çoxlu application sxemaları mühafizə edə bilər. İkinci növ Realmlər Mandatory Realms adlanır və burada obyekt sahiblərinin öz obyektlərinə girişinə səlahiyyəti olmayan obyektlərin verilənləri saxlanılır.

Command Controls – Command Control yaxud Command Rule təhlükəsizlik siyasəti yaradır, istənilən obyekt üzərində istənilən əmr (SELECT, ALTER SYSTEM, DDL və DML əmrləri) ilə mühafizəni təmin edir. Burada təhlükəsizlik əmrlər ilə qurulur və burada hətta Connect əmri ilə istifadəçinin bazaya girişinin qarşısın almaq olar.

Command rule realmdan mürəkkəb və müxtəlifdi. Realm Any səlahiyyətinə, command rule istənilən əmrə məhdudiyyət qoyur.

Realm yoxlanılıb yalnız uğurlu olandan sonra Command rule qiymətləndirilir. Multi-Factor Authorization-Təhlükəsizlik adminləri Rule set ilə qaydalar təyin edə bilərlər. Bağlantını xüsusi İP adresinə və ya İP-lər qrupuna görə, günün saatalrına, həftənin günlərinə görə məhdudlaşdırılır. Bu məhdudiyyət bütün istifadəçilərə, o cümlədən administratora da tətbiq edilə bilər.

Rule sets – Realms və command rules DV 2 vacib komponentidir ancaq onlar rule sets bağlıdır yəni rule sets yazılan şərtlərin olmasına icazənin olub olmamasını təyin edir. Hər bir qayda PL/SQL ifadəsidir və yazılışında 255 xarakter istifadə oluna bilər. Ancaq biz PL/SQL funksiya və proseduradan da istifadə edə bilərik. Rule-lar rue yaxud false qiymətini qaytarır.

Rule set-in 2 növü var :

OR -əgər hər hansı üzvü true qiymət alarsa, yekun qiymət true olar.

And - əgər bütün üzvü true qiymət alarsa, yekun qiymət true olar.

Convenience rule set aşağıdakılar daxildir:

Enabled- fəaliyyətə icazə verilir.

Disabled- fəaliyyətə mane olur.

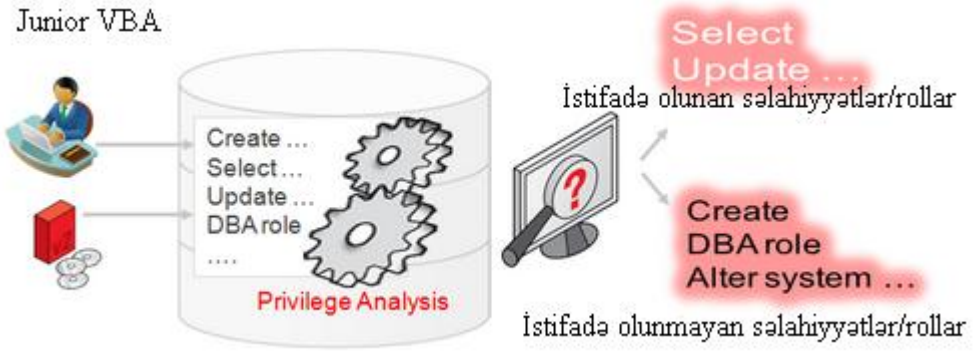
Template rule set aşağıdakılar daxildir:

Allow sesion- Create sesion idarə etmək üçün istifadə olunur. Misal üçün bu qayda Connect command rule yaradarkən istifadə olunur.

Can Grant Virtual Private Database (VPD) Administrator –Bu qaydadan istifadə edərək DBMS_RLS paketi üzərində Grant Execute və Revoke Execute əmrləri idarə edilir [3,13].

Can Maintain Accounts/Profiles- Bu qaydadan istifadə edərək Create User, Drop User, Create Profile, Alter Profile və Drop Profile əmrləri idarə edilir.

Privilege Analysis –Oracle VB-sının 12c versiyasında ODV-un yeni xüsusiyyəti-Privilege Analysis yaradıldı. Privilege Analysis müştərilərə bazada istifadəçilərin və applicationların hansı imtiyazları və rolları istifadə etdiyini görməyə icazə verir. Həmçinin istifadə olunmayan imtiyazları və rolları görməyi də təmin edir. Bu müştərilərə applicationlarını daha çəx təhlükəsiz düzəltməyə və istifadəçilərdən və aplication tərəfindən istifadə olunmayan bütün imtiyaz və rolların silinməsi hücumları azaldır. Privilege Analysis-in arxitekturası şəkil 2.9-da verilmişdir.



Şəkil 2.9 Privilege Analysis

Oracle database Vault qururarkən bazada yeni cədvəllər, görünüşlər, PL/SQL paketləri yaranır. Bu obyektlər 2 sxemada yerləşir.

DVSYS : Bu sxema yerləşən obyektlər Oracle Database Vault üçün Oracle verilənlərin prosesinə lazım olan obyektlərdi. Bu sxema Oracle Database Vault tərəfindən təhlükəsizləşdirilir. DVSYS istifadəçi adı default olaraq klidlənir.

DVF : Bu sxema DBMS_MACSEC_FUNCTION yerləşir. DVF istifadəçi adı default olaraq klidlənir.

DBMS_MACADM paketi DVSYS isitfadəçisi tərəfindən yaradılır və bu paketdə bütün əməliyyatların çoxu xüsusilə Oracle Database Vault Administratorun web console əməliyyatları yerinə yetirilir. Obyektlərdən başqa bəzi istifadəçi adı və rollar da avtomatik yaranır.Avtomatik yaranan rollar səlahiyyət vermək üçün istifadə olunur. OVBVquraşdırılarkən yaradılan istifadəçilər üçün şifrə və rollar təyin +edilməlidir. OVBVOracle Enterprise Manager ilə idarə oluna bilir [3,10,14].

Oracle Database Vault təşkilatların mövcud applicationlarının təhlükəsizliyini artırmaq və normal idarə üçün vəzifələri ayırmaq, məlumatların bütövlüyünü və məlumatların məxfiliyi təmin etmək üçün, ən imtiyaz və digər profilaktik nəzarət etməyə kömək edir.

Database Vault, single-instance Oracle verilənlər bazasına tətbiq edildiyi kimi, RAC arxitekturasındakı strukturlarda da müvəffəqiyyətli bir şəkildə istifadə edilməkdədir.

2.6 ODV-in digər yüksək texnologiyalarla müqayisəsi

Biz bu diplom işində ODV-un bank sektoruna tətbiqindən danışdığımıza görə onun digər texnologiyalardan fərqli cəhətini qeyd edək. Oracle şirkətinin son texnologiyası olan Oracle Audit Vault ilə OVBV bazanın müxtəlif hissəsinin təhlkəsizliyini təmin edir. OVBV qoruyucu nəzarət edir, OAV isə detektiv nəzarət edir.

ODV verilənlərə səlahiyyətli girişi komponentləri vasitəsilə yerinə yetirir və komponentlər ilə səlahiyyətli isitfadəçilərin girişinə qadağa qoyur. Səlahiyyətli istifadəçilər girişinin qarşısın almaqla böyük təhlükənin qarşısı alınır.

OAV isə loqlar vasitəsiylə nəzarət edir və bu loqları silmək olmur. Bu texnologiya müxtəlif bazaları-Microsoft SQL Server, IBM DB2 UDB, and SAP Sybase dəstəkləyir. Audit Vault müxtəlif verilənlər bazası server audit məlumatları birləşdirir. Bu out-of-the-box hesabat böyük bir sıra hesabatlar təhlil edilə bilər. Məhsul da təhlükəsizlik haqqında siqnallar dəstəkləyir. OAV nəzarət edir və o, qadağa qoya bilmir. OVBV ilə əsas fərqi onun qadağa qoymağı bacarmamasıdır və OVBV isə əsas zəif cəhəti audit verilənlərin olmamasıdır.

Oracle VB Firewallun işi birinci başlayır və o səlahiyyətsiz isitfadəçilərin girişinə qadağa qoyur, bəzi hallarda blok edir ancaq səlahiyyətli istifadəçilərin girişinə qadağa qoya bilmir. Bu da onu OVBV texnologiyasından fərqlənir.

Oracle Virtual Şəxsi VB və OLT sətir səviyyəli təhlükəsizliyi təmin edir və yüksək səlahiyyətli şəxslərin gizli məlumatlara girişinə qadağa qoya bilmir ancaq OVBV yüksək səlahiyyətli şəxslərin girişinə qadağa qoyur.

Yuxarıda deyilənlərdən aydın olur ki, ODV-nin digər texnologiyalardan fərqi onun yüksək səlahiyyətli şəxslərə verilənlərin girişinə qadağa qoymasıdır və bu xüsusiyyətinə görə də tətbiq olunan bazada böyük təhlükələrin qarşısın alır. Buna görə də biz ODV-inin Bank sektoruna tətbiqindən danışacağıq.

ODV mənfi xüsusiyyəti onun birlik olub görülən təhlükənin izləyə bilməməsidir.

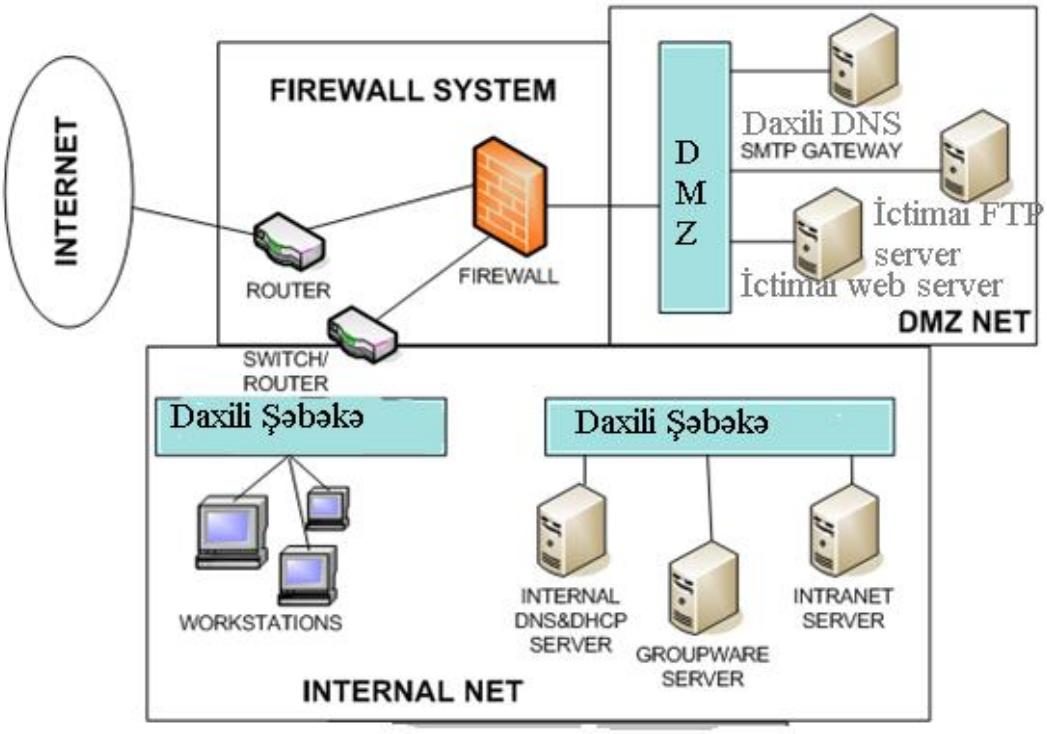
III Fəsil. Azərbaycan Banklarında Oracle VB istifadəçi təhlükəsizliyi

3.1 Azərbaycan Banklarında ümumi təhlükəsizlik

Azərbaycan Banklarında informasiyanın gizli saxlanması üçün təhlükəsizlik sahəsinə xüsusi diqqət ayırırlar. Təhlükəsizlik səviyyəsi güclü olan banklara müştərilər daha çox etibar edir və bank öz maddi səviyyəsini yaxşılaşdırır.

Bank sektorunda təhlükəsizliyi şəbəkə təhlükəsizliyindən başlayır. Şəbəkə təhlükəsizliyi həm daxildən həm də xaricdən bankın şəbəkəsini qoruyur. Xaricdən bankın şəbəkəsi firewall-larla qorunur və onlar xaricdən gələn hücumların qarşısın alır. Firewall-lar şəbəkəni gözlənilməz qonaqdan,hakerlərdən qoruyan komputer təhlükəsizlik sistemidir.

Bir çox banklarda şəbəkə xaricdən Firewall-larla qorunsa da xarici şəbəkə ilə daxili şəbəkə arasında neytral zona yaradılır və bu zonaya DMZ or Demilitarized Zone deyilir. Kompüter təhlükəsizliyi sistemində DMZ bəzən də perimeter şəbəkə adlanan şəbəkə fiziki və ya məntiqi alt şəbəkədir. Bu alt şəbəkə bankın daxili şəbəkəsi ilə xarici şəbəkəsi arasında yaradıldığına

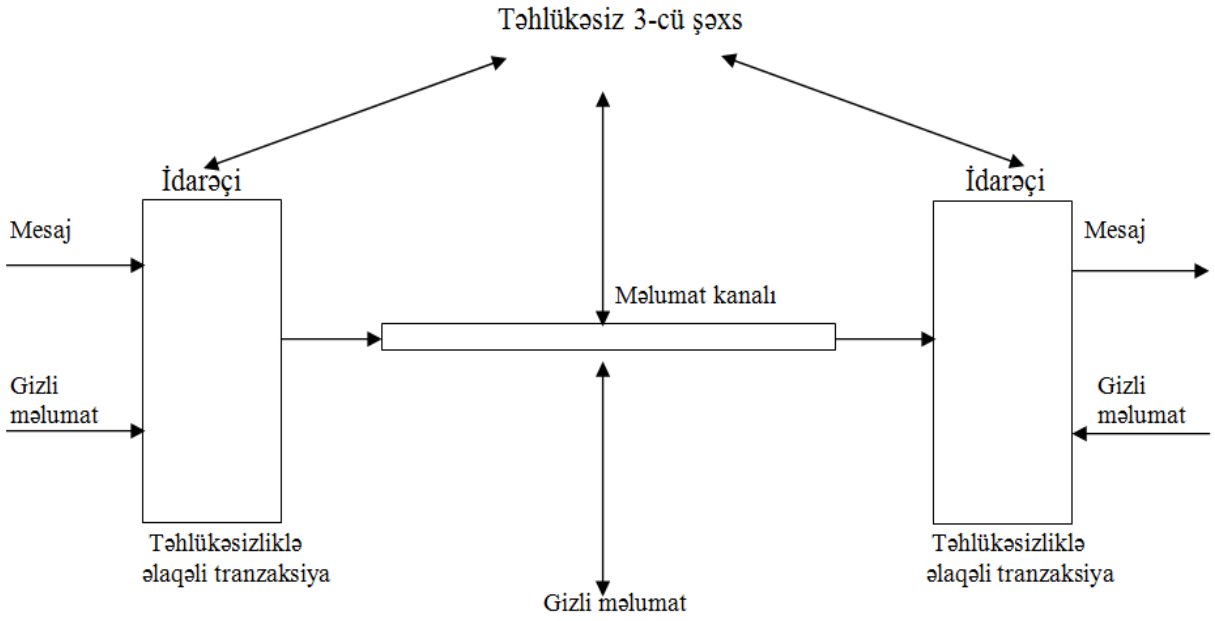


Şəkil 3.1 DMZ olan şəbəkə

görə xaricdən gələn istifadəçilərin girişinin bankın məlumatlarını saxlayan serverə bir başa girişinin qarşısın alır və burada analız olunur. Firewalların qoruya bilmədiyi icazəsiz hücumların qarşısı burda demək olar ki, alınır. Şəkil 3.1-də DMZ ilə firewall olan qarışıq olan şəbəkə verilmişdir.

Şəbəkə təhlükəsizliyinə aid ümumi model Şəkil 3.2-də verilmişdir. Göndərən və alan şəxslərin mesajları arasında gizli məlumat ötürülməsi göstərilibdir. Burada təhlükəsizlik baxımından 4 təməl iş göstərilir.

1. Təhlükəsiz əlaqələr üçün alqoritm
2. Alqoritm ilə qurulacaq gizli məlumatın daşınması
3. Gizli məlumatın paylanması üçün üsul inkişaf etdirmək.
4. Təhlükəsizlik alqoritmini və təhlükəsizlik xidmətini təmin edəcək bir protokol müəyyən etmək.



Şəkil 3.2 Şəbəkə təhlükəsizliyinin ümumi modeli

Şəbəkə təhlükəsizliyinin bir istiqamətidə domain təhlükəsizliyidir. Domain təhlükəsizliyi deyəndə əməliyyat sisteminin təhlükəsizliyi, onun yenilənməsinə nəzarət nəzərdə tutulur. Belə ki, əməliiyat sisteminin yenilənməsi zamanı lazımlı hissələr yenilənməli, lazımsız hissələrin yenilənməsindən imtina edilməlidir. Domain təhlükəsizliyi sistem istifadəçilərin yaratdığı şifrədən asılıdır və istifadəçilər mürəkkəb şifrə yaradarsa, təhlükəsizlik bir o qədər güclü olar. Güclü təhlükəsizlik üçün şifrənin 15 gündən bir dəyişdirilməsi məsləhət görünür.

Bundan başqa domain təhlükəsizliyi zamanı kompüterləri zərərverici proqramlardan - malware-lərdən , viruslardan qorunmaq üçün antiviruslar, antimalware proqramlardan istifadə etmək lazımdır.

Şəbəkə təhlükəsizliyinə aid yenilikləri daim öyrənmək lazımdır və bankın hər bir işçisini şəbəkə təhlükəsizliyinə, bankın ümümi təhlükəsizliyinə aid bilik vermək lazımdır. Bankın işçilərinə e-maillərə gələn tanış olmayan mailli açmamağı, hər sayta girməməyi, hər proqramı kompüterə quraşdırmamağı, proqram quraşdırmaq istəyirlərsə, proqramı bilinməyən saytlardan yükləməməyi, mürəkkəb şifrə yaratmağı və s. haqqında bilik vermək lazımdır.

Ümumi təhlükəsizlikdə fiziki təhlükəsizlik də əhəmiyyətli yer tutur. Fiziki təhlükəsizlik üçün banka daxil olan insanlara nəzarət üçün təhlükəsizlik işçiləri, nəzarət kameraları olmalıdır. Bundan başqa serverləri saxlayan otağın qapısında elekton qıfıl olmalıdır və ora ancaq sistem administratorları daxil olmalıdır və digər şəxslər yalnız onların icazəsi ilə daxil olmalıdır.

3.2 Azərbaycan Banklarında OVB istifadəçi təhlükəsizliyinin müasir vəziyyəti

Azərbaycan Banklarının əksəriyyətində məlumatları saxlamaq üçün Oracle verilənlər bazasından istifadə edirlər. Bankın gizli məlumatlarını, fayllarını və s. saxlayan Oracle verilənlər bazası daxilindən və xaricindən səlahiyyətsiz istifadəçilərdən – hackerlərdən, pis niyyətli şəxslərdən müdafiə olunmalıdır yəni səlahiyyətsiz istifadəçilərin bankın gizli məlumatlarını ələ keçirməsinin qarşısı alınmalıdır. Buna görə də banklarda xaricdən və daxildən Oracle verilənlər bazasının istifadəçi təhlükəsizliyini təmin edilməlidir.

Banklarda daha çox xaricdən gələn hücümların qarşısını almağa diqqət göstərilir və xaricdən Oracle VB-nın istifadəçi təhlükəsizliyini təmin etmək üçün firewall-lardan istifadə edilir və firewall-lar vasitəsilə xarici qüvvələrin bankın gizli məlumatlarını ələ keçirilməsinin qarşısı alınır.

Təəssüf ki, Banklarımızın çoxunda Oracle VB-nın istifadəçi təhlükəsizliyinə daha çox xaricdən müdafiə olunmasına diqqət göstərilir və daxildən müdafiə diqqətdən kənar vəziyyətdə qalır.

Banlarda daxildə Oracle VB-sıın istifadəçi təhlükəsizliyi ki, profile təhlükəsizliyindən və səlahiyyət təhlükəsizliyindən istifadə olunur.

Profile təhlükəsizliyi ilə bir adi istifadəçinin başqa bir adi istifadəçi adına daxil olmasının qarşısı alınır. Bunun üçün Profile yaradılır və onun parametrlərinə uyğun qiymətlər verilir. Əgər bir istifadəçi adına icazəsiz giriş edilərsə, onda şifrə profile-ın FAILED_LOGIN_ATTEMPTS parametrində göstərilən say qədər yalnış yığıla bilər. Göstərilən say yığılarsa, onda istifadəçi adı klidə düşür və nə qədər edilirsə edilsin bu

istifadəçi adına hətta şifrə düzgün yığılsa belə daxil oluna bilinməyəcəkdir. Klidə düşən istifadəçi adı PASSWORD_LOCK_TIME parametrində göstərilən vaxt bitdikdən sonra açılır. İsitfadəçi adının PASSWORD_LOCK_TIME parametrində göstərilən vaxtdan tez açılmasını yalnız administrator açа bilər. Güclü təhlükəsizlik üçün şifrənin yaşama müddətini göstərmək üçün istifadə olunan PASSWORD_LIFE_TIME parametrində göstrərilən günlərin sayı və şifrənin yaşama müddəti bitəndən sonra şifrənin dəyişməsi üçün verilən günlərin sayını göstərən PASSWORD_GRACE_TIME parametrlərdəki günlərin sayını az, yalnış şifrənin neçə dəfə maxsimum yığıla bilməsini göstərən FAILED_LOGIN_ATTEMPTS parametrin qiymətini az, istifadəçi adı klidə düşəndən sonra kliddə qalma müddətini göstərən PASSWORD_LOCK_TIME parametrinin qiymətini çox qoymaq lazımdır. Araşdırılan banklardan görürük ki, bəzi böyük banklarda profile təhlükəsizliyi güclüdür. Ancaq bu istifadəçi təhlükəsizliyinin güclü olması demək deyil cünk profile təhlükəsizliyi administratorlardan və yüksək səlahiyyətli şəxslərdən asılıdır ki, bu da əsas problemdir.

Səlahiyət təhlükəsizliyindən istifadə olunaraq hər bir işçi öz vəzifəsinə düşəm əməliyyatı edir və görür. Bir "Müştəri Xidmətləri"departamentinin işçiləri yalnız özlərinə adi əməliyyatları edir və öz departamentinin işçilərinin etdikləri əməliyyatı görür, başqa bir departamentin məsələn"Kredit" departamentinin əməliyyatlarını görmür.

Bu təhlükəsizlik ilə hər bir işçinin hansı əməliyyat etməsini, dəyişilik etmək, silmək icazəsi olub olmadığı nizamlanır və araşdırılan demək olar bütün banklarda bu təhlükəsizlik növündən istifadə olunduğu göründü. Bu üsul vasitəsiylə adi istifadəçilərin səlahiyyəti nizamlanır və yenə də təhlükəsizlik administratorlardan və yüksək səlahiyyətli şəxslərdən asılıdır ki, bu da əsas problemdir.

Banklarda profil və səlahiyyət təhlükəsizliyi nə qədər güclü olsa da ümümi istifadəçi təhlükəsizliyinə görə çatışmayan xüsusiyyətləri var. Bu üsulların müsbət və mənfi xüsusiyyətləri Cədvəl 3.1-də qeyd olunmuşdur. (İA-İstifadəçi adı)

Cədvəl 3.1 İsitfadə olunan üsulların mənfi və müsbət xüsusiyyəti

İA-nı adi istifadəçilərdən müdafiə	Resurslara məhdudiyət qoymaq	Şifrənin istifadə müddətini təyin etmək	Təkrar şifrədən istifadəni nizamlamaq	Bir istifadəçi obyektinə digər istifadəçinin girişini nizamlamaq	İstifadəçilərin öz vəzifələrinin işlərindən başqa digər işləri etmək imkanı	İş saatalrına, həftənin günlərinə, İP görə istifadəçilərin girişini nizamlamaq	İstifadəçilərin öz yaratdığı obyektə girişini nizamlamaq	Administrator-ların, istənilən istifadəçilərin obyektlərinə girişi nizamlamaq.
+	+	+	+	+	+	-	-	-

Banklarda Oracle VB-sının istifadəçi təhlükəsizliyi kimi bazanın yerləşdiyi serverin şifrəsin gizli saxlayırlar yəni təhlükəsizlik kimi sistem təhlükəsizliyindən istifadə edirlər.

3.3 Azərbaycan Banklarında OVB istifadəçi təhlükəsizliyinin problemləri və həll üsulu

3.2-ci hissədən və Cədvəl 3.1-dən göründüyü kimi Azərbaycan banklarında Oracle VB-sı administratorlardan və ya administrator səlahiyyətli şəxslərdən, təhlükəsiz işçilərdən müdafiə olunmuryəni banklarda bazaya oracle administratorların və təhlükəsizlik sahəsində işləyən işçlərin bankın gizli məlumatlarına girişinə məhdudiyyət qoyulmur və onların istədiyi hesab məlumatlarını, müştərilərin şəxsi məlmatlarını görməsi son dərəcə asandır və bu məlumatları qanunsuz şəkildə ələ keçirib istifadə etməsi çox asan yarana bilən təhlükəli hadisədir. Azərbaycan Banklarında Oracle VB-sının təhlükəsizliyinin səlahiyyətli şəxslərə açıq olması ən böyük problemlərdən biridir.

Dünyanın bir çox böyük banklarında daxildə işləyən işçinin bankın gizli məlumatların ələ keçirməsi nəticəsində həmin banka böyük ziyan vurulmuşdur. Adi bir hadisə Şotlandiya Dövlət bankında olmuşdur. Bu bankda VBA vəzifəsində işləyən şəxs müştərilərin email ünvanlarını reklamla məşğul olan şirkətə satmışdır. Bu gün banklarımızda bu və ya buna oxşar hadisələrin baş verməsinin qarşısına alan təhlükəsizlik sistemi yoxdur və VBA vəzifəsində işləyən biri bankın müştərilərin siyahısını çox asanlıqla götürüb başqa rəqib banklara sata bilər.

VBA və sistem administratorları bankın gizli məlumatlarını nəinki iş saatlarında o cümlədən kənarda qoşulma ilə istənilən vaxt görə bilirlər və heç nə edilməsəs belə

kənardan qoşulmanın özü təhlükəsizlik qaydasını pozur. Bundan başqa kənardan qoşulanda məlumatlar nəinki qoşulan şəxsə, şəbəkəyə qanunsuz müdaxilə edən pis niyyətli istifadəçilərə də açıq olur. Buna görə də bazaya qoşulmanın iş saatlarına, bazaya qoşuyan komputerlərin İP adressinə görə də nizamlamaq lazımdır.

Banklarda İT departamentinə işə götürülən işçilərin keçmişi araşdırılmır və banklar öz işçilərinə etibar edərək gizli məlumatlarını onların görməsinə icazə verir. Hər bir bankın bir işə götürülmə qaydası olmalıdır və işçi işə götürərkən xüsusilə də VBA vəzifəsinə işçi götürərkən bu qaydaya uyğun olmalıdır.

Hal hazırda əksər banklarda oracle-ın bütün istiqamətləri üzrə təhlükəsizlik işlərinə ən çoxu üç nəfər nəzarət edir. Təhlükəsizlik kimi bazanın yerləşdiyi serverın yəni sistemin şifrəsini qoruyurlar və şifrəni yalnız bazaya nəzarət edən sistem administratorları bilir. Təhlükəsizlik yənə də səlahiyyətli şəxslərdən asılı olur. Balaca banklarımızda isə OVB-nın təhlükəsizliyə heç kim nəzarət etmir və profile, səlahiyyət təhlükəsizliyi yalnız application səviyyəsində həyata keçirilir.

Bank sahibkarları daha çox öz qazanclarını düşünərək gizli məlumatların təhlükəsizliyini unudurlar və problem olanda artıq hər şey çox gec olur. Təhlükə olanda isə bank həm müştəri itkisi ilə həm də maddi itki ilə qarşılaşır.

Oracle VB-sı öz VBA-sını izləyən, lazım olarsa VBA-nın səlahiyyətlərini azalda bilən tək VB-sıdır. Oracle VB-sı Oracle Database Vault texnologiyası vasitəsiylə öz VBA-sının səlahiyyətini azaldır və VBA-dan bütün cədvəllərə, görünüşlərə əməliiay etməsinin qarşısın alır.

Oracle database Vault,VB-yə girişi olan istifadəçilərin gizli məlumatlara girişini nəzarət altında saxlayır, VB-na və gizli məlumatlara kimin, nə vaxt, haradan və necə çata biləcəyinə dair siyasətlər inkişaf etdirən bir təhlükəsizlik texnologiyasıdır.

Oracle Database Vault-un komponentləri- realms, command rules, factors, rule sets, secure application rules - gizli məlumatları günün saatına, İP adresinə, kimlik yoxlama üsullarına görə icazəsiz girişdən təhlükəsiz şəkildə müdafiə edir və vəzifələrin ayrılmasını tələb edir.

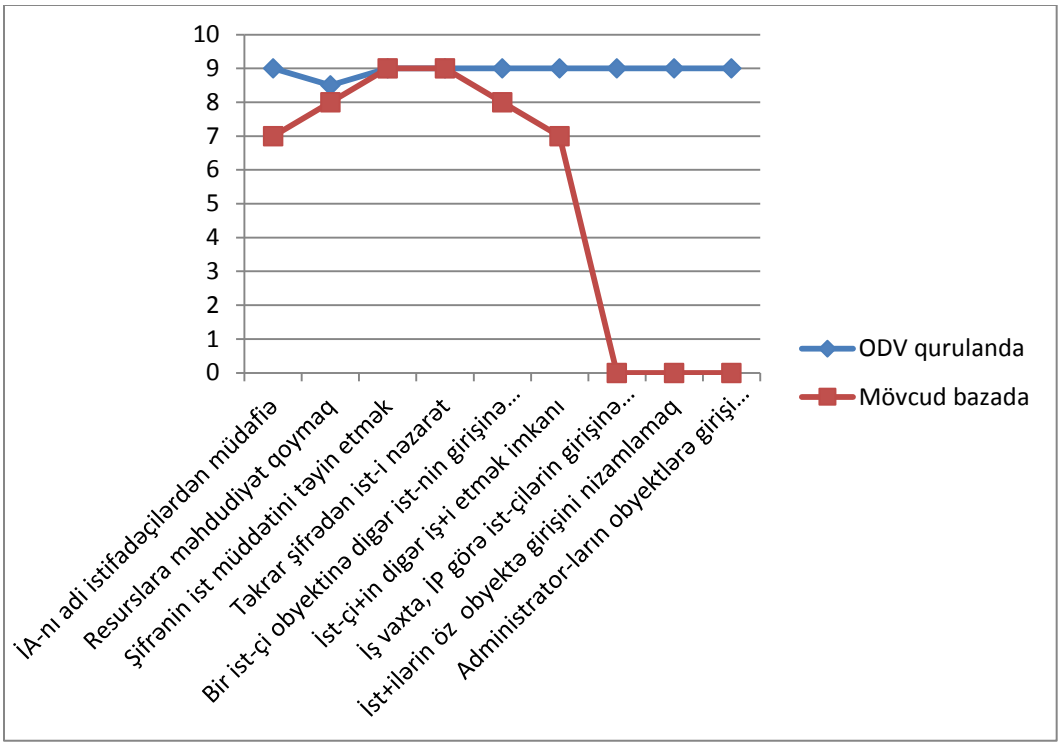
Oracle verilənlər bazası vault mövcud olan bazanın üzərinə quraşdırılır və mövcud təhlükəsizlik üsulları ilə birgə, bazanı saxlayan serverə və application serverə də firewallar qoyulmaqla daha güclü təhlükəsizlik yaratmaq olar.

Bu texnologiyanın Azərbaycan banklarında tətbiq olunmamasının əsas səbəbi istifadəsi üçün çox işçi və çox maddi ehtiyat tələb etməsidir. Ona görə də Azərbaycanda, eləcə də dünyanın bir çox banklarında bu texnologiyadan istifadə edilmir.

3.4 Azərbaycan Banklarında mövcud OVB-sı ilə OVBV qurulan OVB-nın müqayisəsi

Azərbaycanda bank sektorunda cari istifadə olunan bazanın üzərinə Oracle verilənlər bazası vault qurulduğuna görə bu mövcud təhlükəsizliyi gücləndirir. Biz cədvəl 3.1-də mövcud təhlükəsizliyin mənfi və müsbət xüsusiyyəyləri göstərilibdir. Əgər bazanın üzərinə OVBV quraşdırılarsa, bazanın göstərilən mənfi xüsusiyyətlərinin qarşısı alınacaqdır.

ODV-nin tətbiqi administratorun səlahiyyətlərini azaldır. Bu isə bankın təhlükəsizliyini artırmaqla bərabər müştərilərin banka etibarını artırır. Biz bazanın təhlükəsizliyini OVBV qurulandan sonra müqayisə etmək üçün Şəkil 3.3-dəki qrafikə baxaq. Şəkil 3.3-dəki qrafikdən görünür ki, OVBV texnologiyasının qurulması təhlükəsizliyi artırır.



Şəkil 3.3 Mövcud baza ilə ODVqurulandan sonra olan bazanın müqayisəsi

IV Fəsil. Oracle verilənlər bazası vaultun bankda tətbiqi

Oracle Database Vaultun bank sektoruna tətbiqini göstərmək üçün banka aid aparılmış tətbiqi göstəriləcəkdir. Əvvəlcə ODV-un qurulmamışdan görüləcək işlər haqqında məlumat veriləcəkdir. Ondan sonra ODV-nın qurulması göstərilib analiz olunacaqdır.

4.1 OVBV-un qurulmasından əvvəl ediləcək əməliyyatlar

Oracle Database Vault mövcud bazanın üzərinə qurulur və bu məhsul qurulandan sonra bazanın bəzi lazım olan parametrlərinin qiyməti dəyişə bilər. Ona görə də biz OVBVqurulmamışdan əvvəl lazimi cədvəllərdə, verilənlər lüğətində, görünüşdəki məlumatlar yaddaşa verilməlidir. Bu cədvəllərdə, verilənlər lüğətində, görünüşdəki məlumatı görmək üçün sqlplus-a sysdba kimi qoşuluruq və aşağıdakı əməliyyatları edirik.

SQL> select * from dba_network_acls;

Dba_Network_Acls cədvəlində girişi idarə etmək üçün şəbəkənin host və portları saxlanılır və cədvəlin sütunları Cədvəl 4.1-də göstərilmişdir.

Cədvəl 4.1. Dba_Network_Acls sütunları

Column	**Datatype**	**NULL**	**Description**
HOST	VARCHAR2(1000)	NOT NULL	Şəbəkə hostu
LOWER_PORT	NUMBER(5)		Port aralığının aşağı qiyməti
UPPER_PORT	NUMBER(5)		Port aralığının yuxarı qiyməti
ACL	VARCHAR2(4000)		Girişə nəzarət siyahısının yolu
ACLID	RAW(16)	NOT NULL	Girişə nəzarət siyahısının Object ID-si

SQL> select * from dba_network_acl_privileges;

dba_network_acl_privileges cədvəlində indiki şəbəkə hostu üçün bütün girişə icazəsi olan şəbəkə səlahiyyətləri təsvir edilir və cədvəlin sütunları Cədvəl 4.2-də göstərilmişdir.

Cədvəl 4.2 Dba_network_acl_privileges sütunları

Column	Datatype	NULL	Description
Acl	Varchar2(4000)		Girişə nəzarət siyahısının yolu
Aclid	Raw(16)	NOT NULL	Girişə nəzarət siyahısının Object ID-si
Principal	Varchar2(4000)		Principal (database user or role) imtiyaz verilmiş və ya qadağa qoyulmuş
Privilege	Varchar2(7)		Şəbəkə imtiyazı
Is_Grant	Varchar2(5)		True qiyməti ilə imtiyazın veildiyini, false qiyməti il qadağa edildiyini göstərir
Invert	Varchar2(5)		Giriş nəzarət siyahısına qoymalıdır (true) yoxsa yox (false)
Start_Date	Timestamp(9) With Time Zone		Giriş nəzarət siyahısının başlama vaxtı
End_Date	Timestamp(9) With Time Zone		Giriş nəzarət siyahısının son vaxtı

SQL> select inst_id,name,value from gv$parameter where upper(name) in ('audit_sys_operations','os_roles','recyclebin','remote_login_passwordfile','sql92_security');

sql> select * from dba_tab_privs where table_name ='utl_file';

sql> select grantee, privilege from dba_sys_privs where privilege in ('create job', 'create any job') order by privilege;

sql> create table invalid_objects_before_dv as select owner,object_name,object_type from dba_objects where status='invalid' and object_type <> 'synonym' ;

SQL> select * from dba_registry where comp_id in ('OLS','DV');

sql> select p.name, p.value memory, sp.value spfile from v$parameter p, v$spparameter sp where p.name = sp.name and upper (p.name) in ('audit_sys_operations', 'os_roles', 'recyclebin', 'remote_login_passwordfile', 'sql92_security');

SQL> select * from dba_priv_audit_opts;

SQL>select * from DBA_STMT_AUDIT_OPTS order by audit_option;

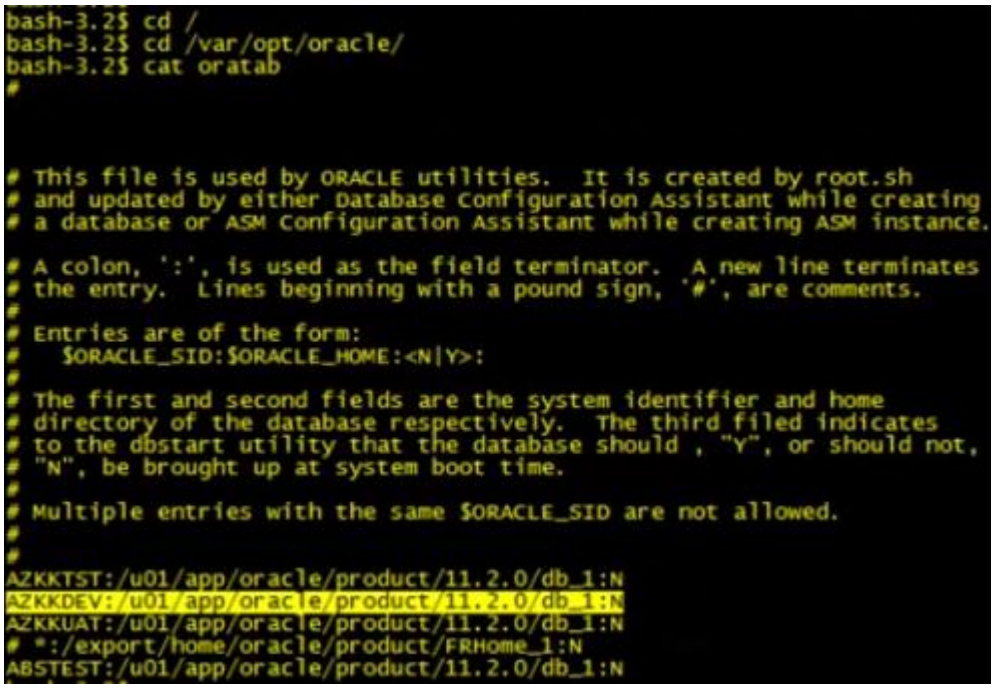
SQL>select * from dba_obj_audit_opts;

Göstəriləcək bütün əməliyyatlar yaddaşa verilib saxlanılır. ODB qurulandan sonra yuxarıdakı əməliyyat təkrar aparılır və cədvəllərdə, verilənlər lüğətində, görünüşdəki məlumatlar əvvəlcə yaddaşa verilmiş məlumatlarla müqayisə olunmalıdır. Əgər dəyişilik varsa onda obyektlərdəki məlumatlar əvvəlki kimi düzəldilir.

4.2 OVBV-un qurulması

Biz sqlplus-a sys kimi qoşuluruq və Oracle Database Vaultu qurmamışdan əvvəl aşağıdakı əməliyyatı edirik.

1) Şəkil 4.1-də kimi /var/opt/oracle/oratab altındakı əlaqəli sətiri düzgün $ORACLE_HOME olmalıdır.



Şəkil 4.1 $ORACLE_HOME parametin yoxlanması

Əks halda dbca çalışdırılanda Configure Database Option buttonu passiv olacaqdır.

2) Şəkil 4.2-də kimi Default profildəki PASSWORD_VERIFY_FUNCTION parametrinin qiyməti NULL olmalıdır. Əks halda ORA-29504: Naməlum yaxud buraxılmış sxema adı səhvi ekrana çıxar.

```
SQL> select * from dba_profiles where PROFILE='DEFAULT';

PROFILE                        RESOURCE_NAME                    RESOURCE LIMIT
------------------------------ -------------------------------- -------- ----------
DEFAULT                        COMPOSITE_LIMIT                  KERNEL   UNLIMITED
DEFAULT                        SESSIONS_PER_USER                KERNEL   UNLIMITED
DEFAULT                        CPU_PER_SESSION                  KERNEL   UNLIMITED
DEFAULT                        CPU_PER_CALL                     KERNEL   UNLIMITED
DEFAULT                        LOGICAL_READS_PER_SESSION        KERNEL   UNLIMITED
DEFAULT                        LOGICAL_READS_PER_CALL           KERNEL   UNLIMITED
DEFAULT                        IDLE_TIME                        KERNEL   UNLIMITED
DEFAULT                        CONNECT_TIME                     KERNEL   UNLIMITED
DEFAULT                        PRIVATE_SGA                      KERNEL   UNLIMITED
DEFAULT                        FAILED_LOGIN_ATTEMPTS            PASSWORD UNLIMITED
DEFAULT                        PASSWORD_LIFE_TIME               PASSWORD UNLIMITED
DEFAULT                        PASSWORD_REUSE_TIME              PASSWORD UNLIMITED
DEFAULT                        PASSWORD_REUSE_MAX               PASSWORD UNLIMITED
DEFAULT                        PASSWORD_VERIFY_FUNCTION         PASSWORD NULL
DEFAULT                        PASSWORD_LOCK_TIME               PASSWORD 1
DEFAULT                        PASSWORD_GRACE_TIME              PASSWORD 7

16 rows selected.
```

Şəkil 4.2.Default Profilin parametriləri

3)Db Vault Option-ın Oracle Binary üçün nəzarət edilməlidir və passivdirsə, aktiv etmək lazımdır.

Nəzarət etmək üçün sqlplus-a sys kimi girik. Girərkən Şəkil 4.4.-də kimi bu yazı ilə qarşılaşırıq.

"Connected to: Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production with the Partitioning, OLAP, Data Mining and Real Application Testing options."

```
SQL*Plus: Release 11.2.0.3.0 Production on Mon Mar 3 15:25:02 2014

Copyright (c) 1982, 2011, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
```

Şəkil 4.3 ODV-nın qurulu olmadığı göstərilir.

Bu yazıda Vault ilə əlaqəli yazının gəlmədiyini görürük.Əgər qurulu olsaydı əlavə olaraq " With the Oracle Label Security, Oracle Database Vault options" yazısı görəcəkdik.

Bundan əlavə Şəkil 4.4-də kimi V$option görünüşünə baxa bilərik.

Şəkil 4.4 V$option görünüşü ODV-nın qurulu olmadığı göstərilir.

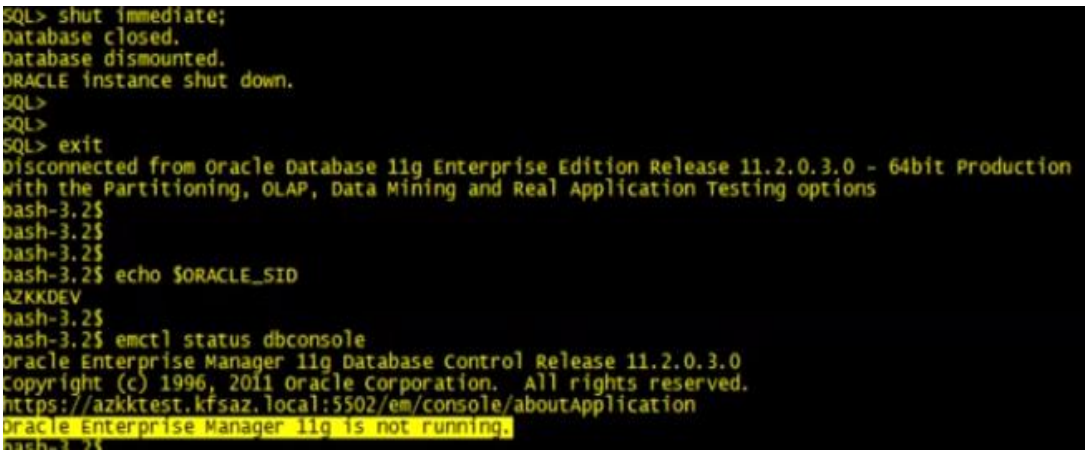
Db Vault Option-ın Oracle Binary-nin aktiv edilməsi edilməsi üçün aşağıdakı addımlarla əməliyyatlar edilir.

addım 1-əlaqəli VB-sı bağlanır

SQL> SHUTDOWN IMMEDIATE

addım 2-Dbconsole (Enterprise Manager) varsa bağlanır

SQL> $ emctl stop dbconsole



Şəkil 4.5 VB-sının və Enterprise Manager bağlanması

addım 3- əlaqəli Listener bağlanır

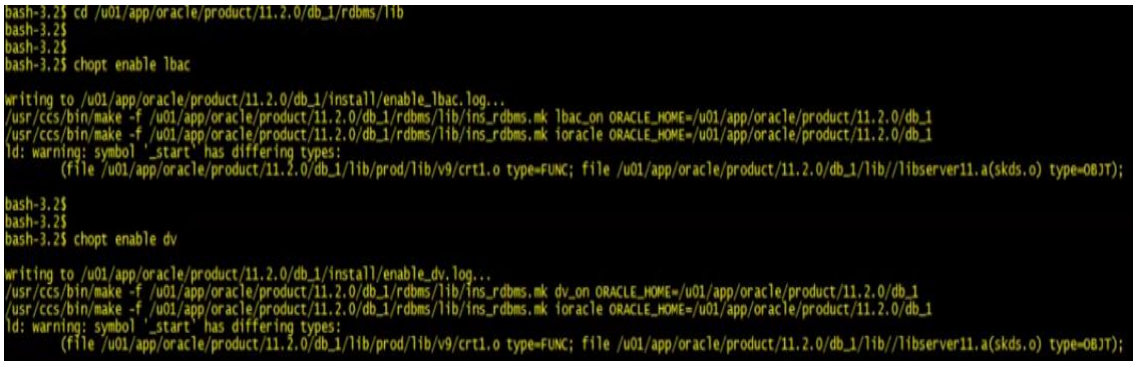
SQL> lsnrctl stop listener

addım 4 - DB Vault Option Oracle Binary üçün enable edilir

cd $ORACLE_HOME/rdbms/lib

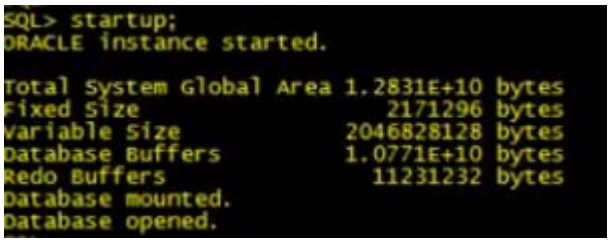
make -f ins_rdbms.mk dv_on lbac_on ioracle

Oracle binary də option enable edərkən Make –f yerinə chopt əmri də istifadə edilə bilər. İstifadə qaydası aşağıdakı kimidir.

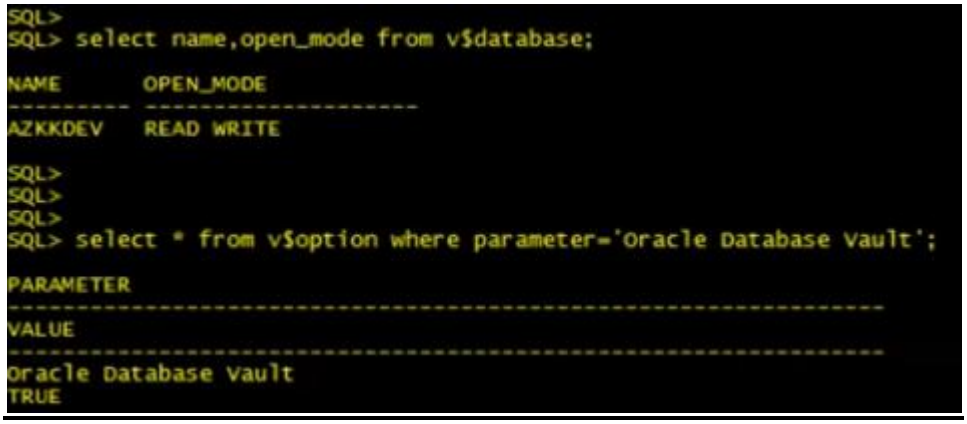


Şəkil 4.6 Chopt əmrinin istifadəsi

Addım 5-Database ve Listener açılaraq DB Vault-un enable olub olmadığı yoxlanılır.



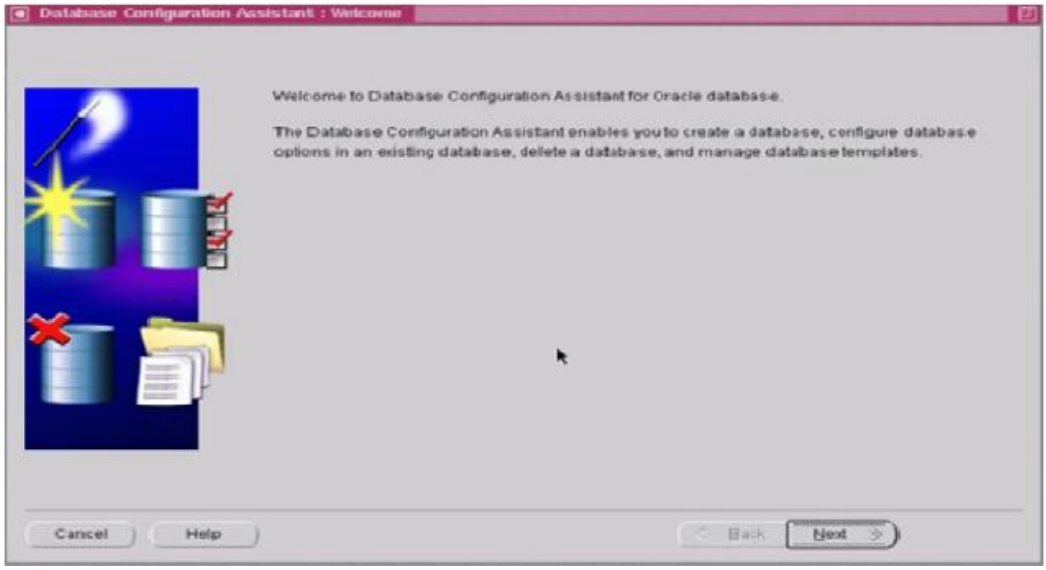
Şəkil 4.7 Bazanın və listenerin başlanması



Şəkil 4.8 ODV-nın aktiv olduğunu yoxlamaq əmri

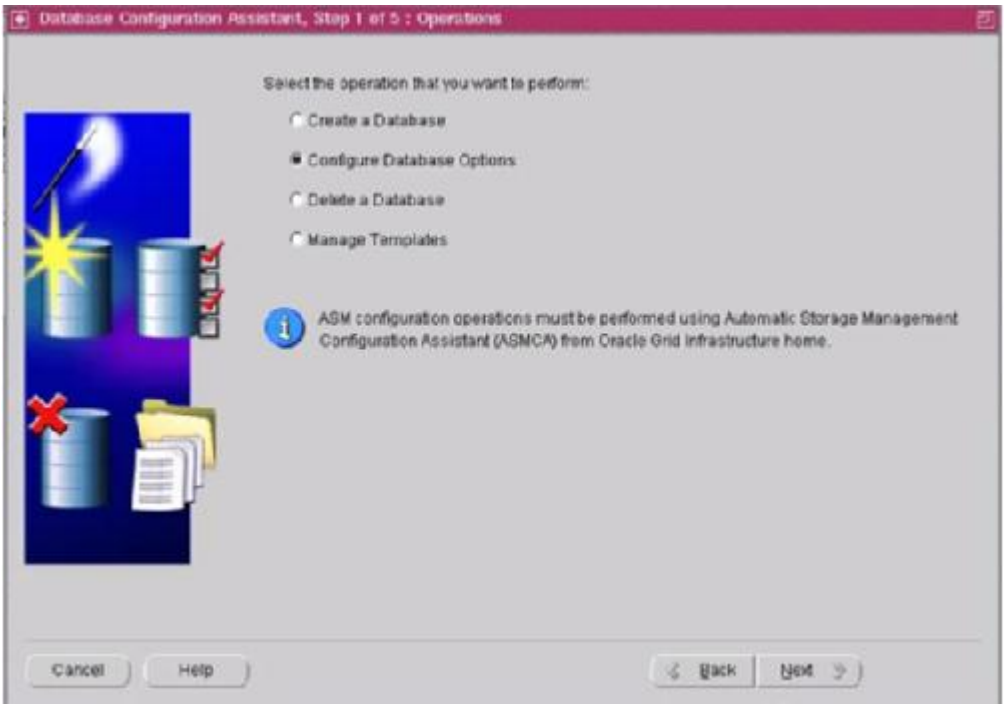
Oracle Database Vault VB-sında seçimli olaraq olur. Database vault, Oracle qurularkən seçilə biləcəyi kimi, Oracle instance qurulduqdan sonra da aktiv hala gətirilə bilər. Oracle instance qurulduqdan sonra aktiv hala gəlməsi üçün dbca əmri ilə Database Configuration Assistant çalışdırmaq lazımdır.

1) Database Configuration Assistant açılır və biz Next düyməsin basırıq.



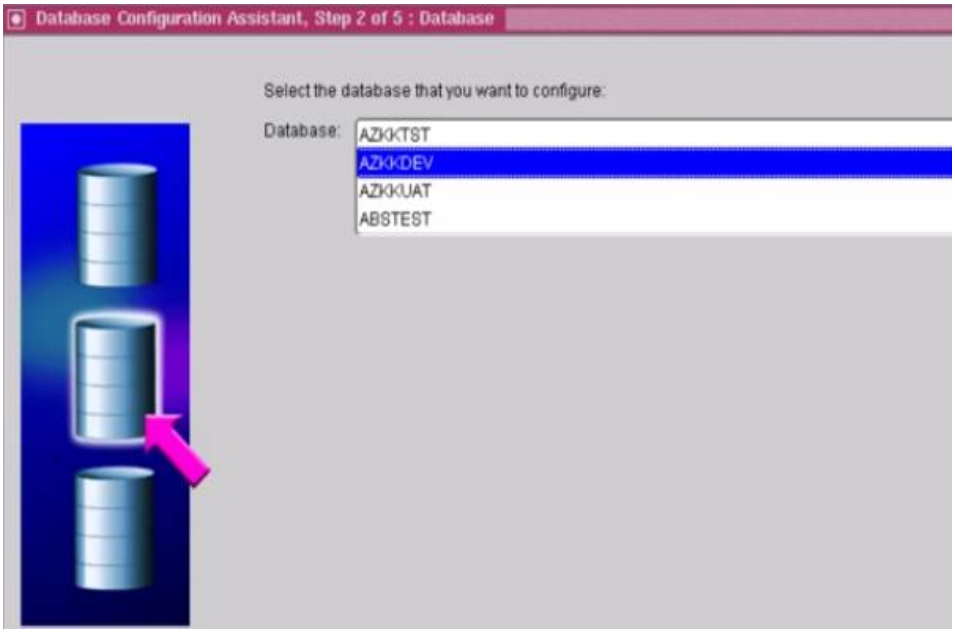
Şəkil 4.9 Database Configuration Assistant açılması

2) Sonra Şəkil 4.10-da göstərildiyi kimi açılmış pəncərədə Configure Database Option seçilir.



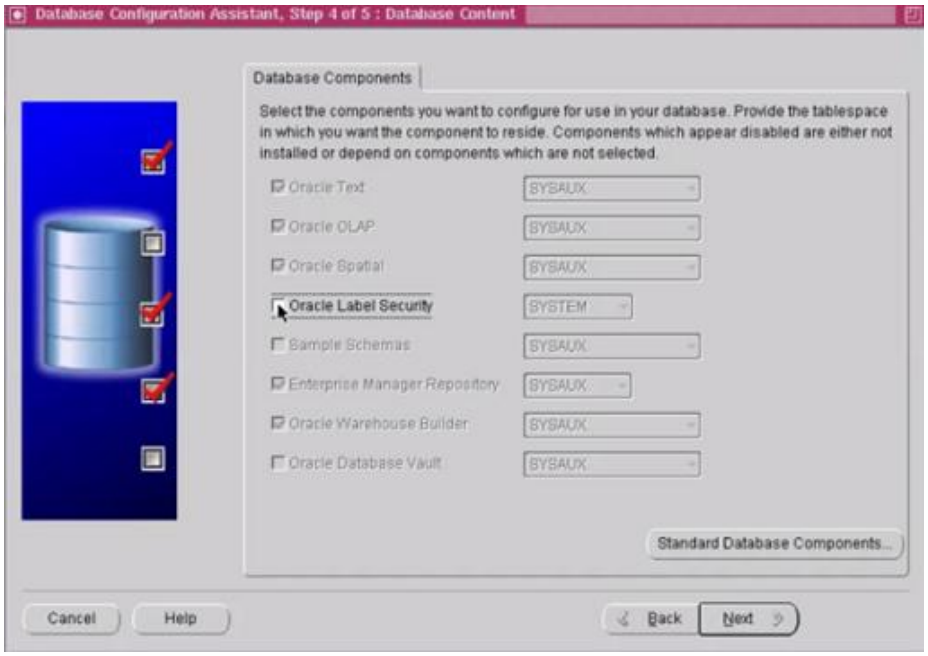
Şəkil 4.10 Configure Database Options parametrinin seçilməsi

3) Açılmış yeni pəncərədə Şəkil 4.11-da göstərildiyi kimi AZKKDEV seçib Next düyməsin basırıq.



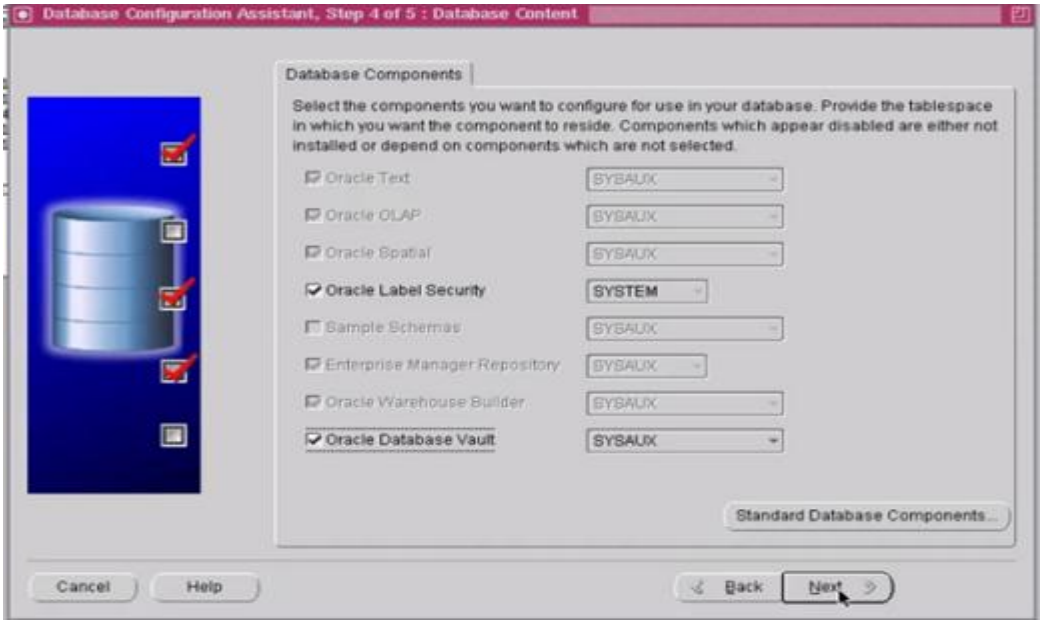
Şəkil 4.11 AZKKDEV bazasının seçilməsi

4) Açılmış pəncərədə Next basırıq. Onda Şəkil 4.12 kimi pəncərə açılır.



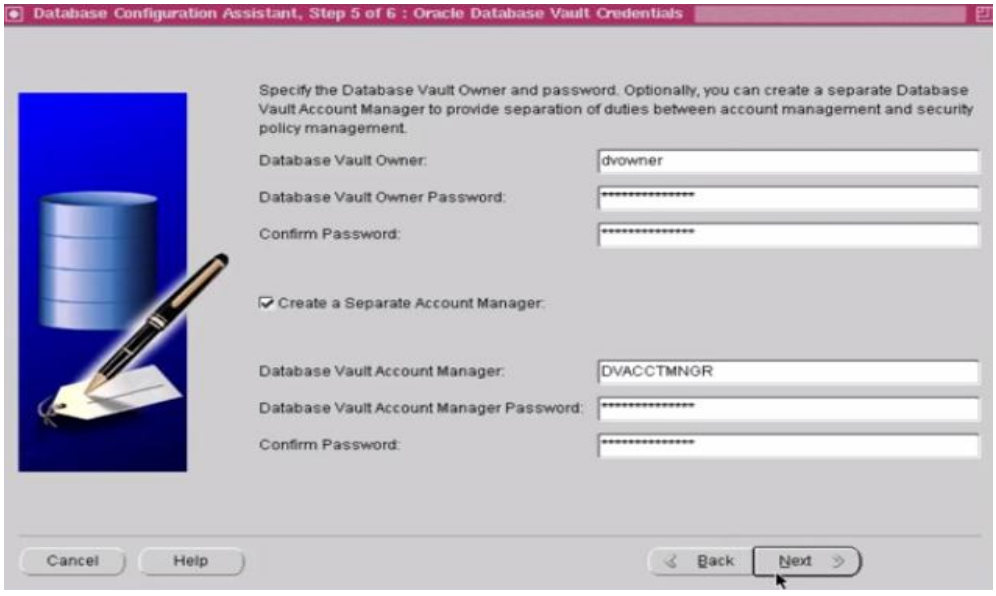
Şəkil 4.12 Oracle Label security-ni seçilməsi

Açılmış pəncərədə Oracle Label security-ni seçirik. Onda Oracle Database Vault checkbox aktiv olur və onu seçirik.



Şəkil 4.13 Oracle Database Vault-un seçilməsi

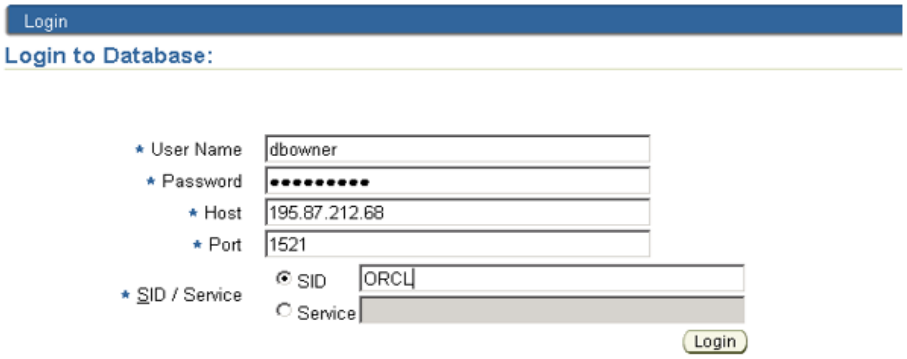
5) Next basırıq və açılmış pəncərədə ODV-nın Owner və account Manager istifadəçisinin adını və şifrəsin yazırıq.



Şəkil 4.14 Oracle Database Vault-un istifadəçi adlarının daxil edilməsi

Sonra açılmış pəncərədə Finish basırıq və Oracle Database Vaultun qurulur. Qurulub qurtarandan sonra baza yenidən başlanır.

Qurulma bitdikdən sonra, https://hostname(veya host ip):port number/dva hər hansı bir brouzerə yazıb Oracle Database Vault ekranına giririk.



Şəkil 4.15 ODV-nın ara üzü

Bu ara üzündən OVBV-nin administratoru səlahiyyətləri idarə edir.

4.3 OVBV-un qurulandan sonra yaranan analizi və test olunması

Qurulan Oracle Database Vault-un test edək. Bunun üçün əvvəlcə realm komponenti yaradaq.Realm yaratmaq üçün DV Administrator adı ilə daxil olub aşağıdakı addımla yaratmaq lazımdır.

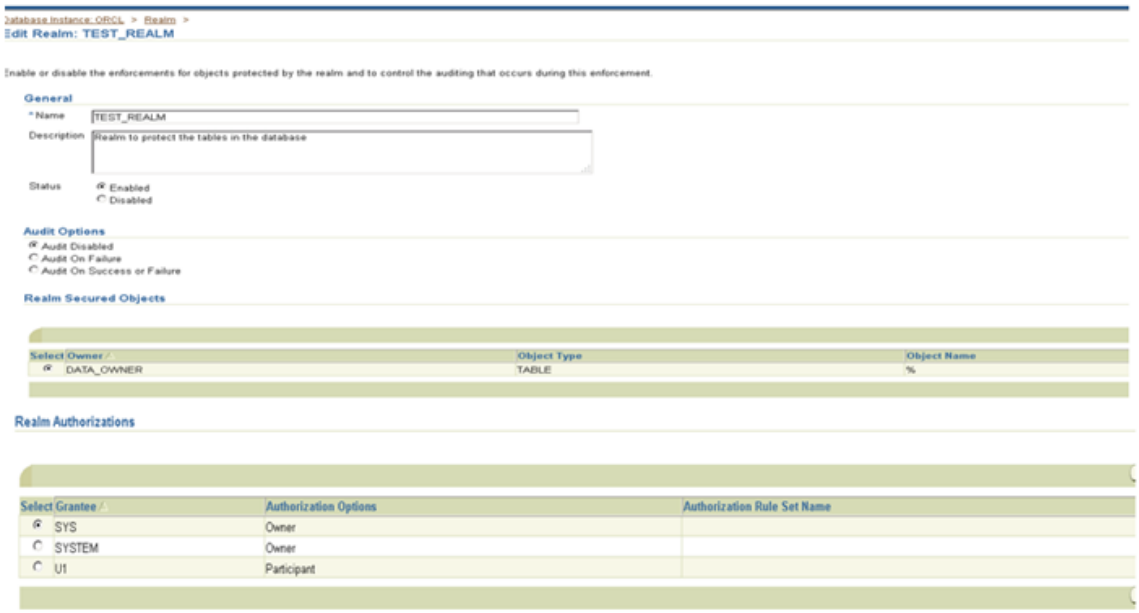
1) Aministrator tabına klik edib realm linkinə giririk;

Şəkil 4.16 OVBV-da MACSYS istifadəçinin Administrator Tabı

2) Ekranın yuxarısında sağ tərəfdə Create düyməsin basırıq;

3) Name hissəsinə Scott_Name , description hissəsinə “Bu realm Vba keçidi mühafizə edir.” yazırıq. Leave Status hissəsində Enable, Audit Option hissəsində isə Audit

Disabled seçirik. Sonra select Owner hissəsində Data_Owner və Select Grantee hissəsində sys seçib Ok düyməsin basırıq. Bununla realm yaradılacaqdı.



Şəkil 4.17 ODV-da Realm komponentinin yaradılması

İndi test edək.

sqlplus sys/*******

SQL> select * from data_owner.t1;

select * from data_owner.t1

*

ERROR at line 1:

ORA-01031: insufficient privileges

[oracle@ksoracletest1 ~]$ sqlplus u1/u1

SQL*Plus: Release 11.2.0.2.0 Production on Tue Jul 10 16:24:18 2012

Copyright (c) 1982, 2010, Oracle. All rights reserved.

Connected to:

Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - 64bit Production

With the Partitioning, Oracle Label Security, OLAP, Data Mining,

Oracle Database Vault and Real Application Testing options

SQL> select * from data_owner.emp;

ID Name

---------- ----------

1 Əli

2 Orxan

3 Məlik

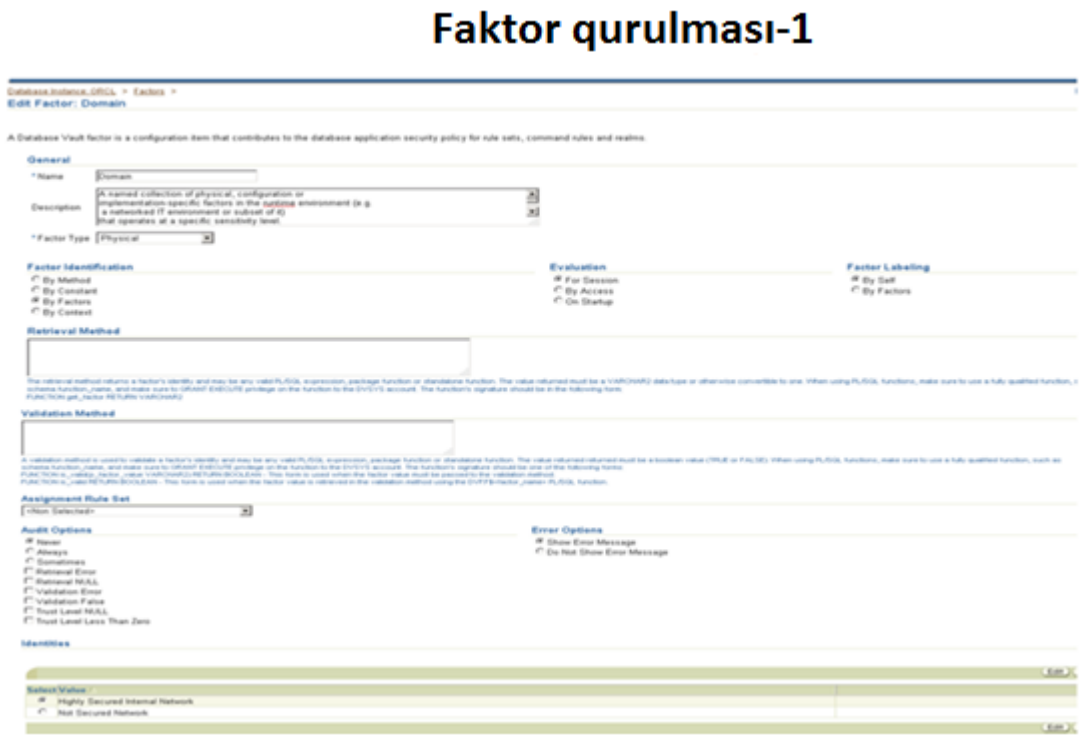
Növbəti misalda, Rule sets, Factors ve Command Rules bərabər istifadə edək. 195.87.212.68 ip adresindən ‘Highly Secured Internal Network’ domain’dən bağlanan DBSMAPS istifadəçisi hafta içi hərgün saat 09:00 – 19:00 arasından DBSMAPS sxeemasından table truncate ede bilsin. Bu qaydadan kənar istifadəçilər truncate edə bilməsinlər.

Görüləcək işlər.

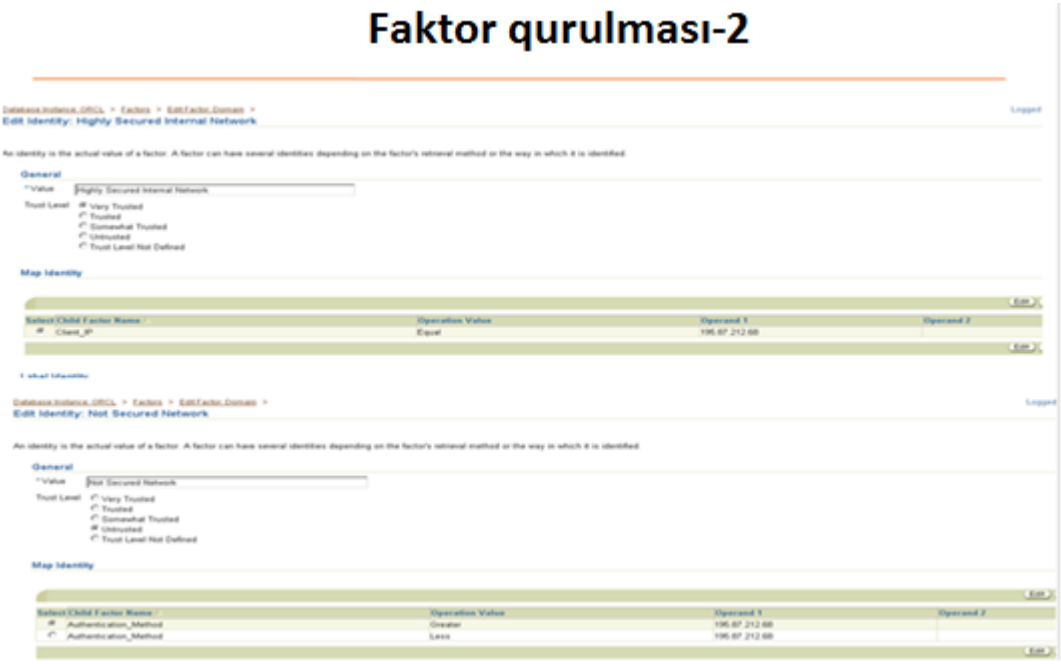
1. İstifadəçi üçünbir factor yaradaq. Factor yaradılanda bağlanılacak session’in ip adresi ve domain adı verilir.
2. Bir rule set yaradaq. Evaluation Option all true seçənəyini işarə edək.
3. Həftə içi günləri, istifadəçi adı ve həftə içi iş saatları üçün rule yaradıb, rule set-ə əlavə edək.
4. Command Rule ilə truncate table əmri, bu misal üçün yaradılan rule set ilə əlaqələndirilir.

Not:SELECT OBJECT_NAME, OBJECT_TYPE FROM DBA_OBJECTS WHERE

OWNER='DVF' AND OBJECT_NAME LIKE 'F$%'

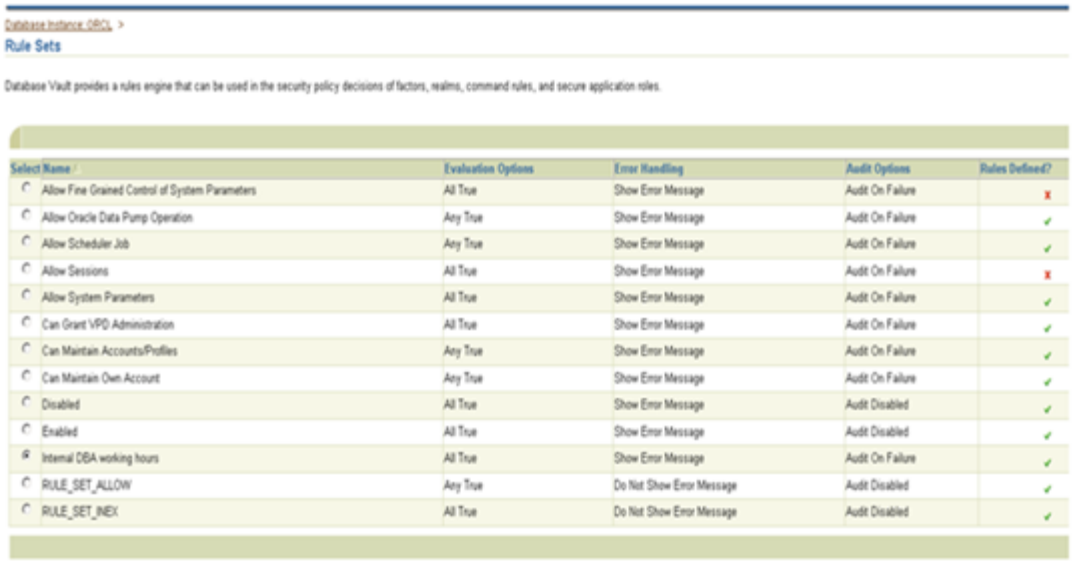


Şəkil 4.18 Faktor-un qurulması-1



Şəkil 4.19 Faktor-un qurulması-2

Qaydaları yaradıb rule set-ə əlavə etmək



Database Instance: ORCL >

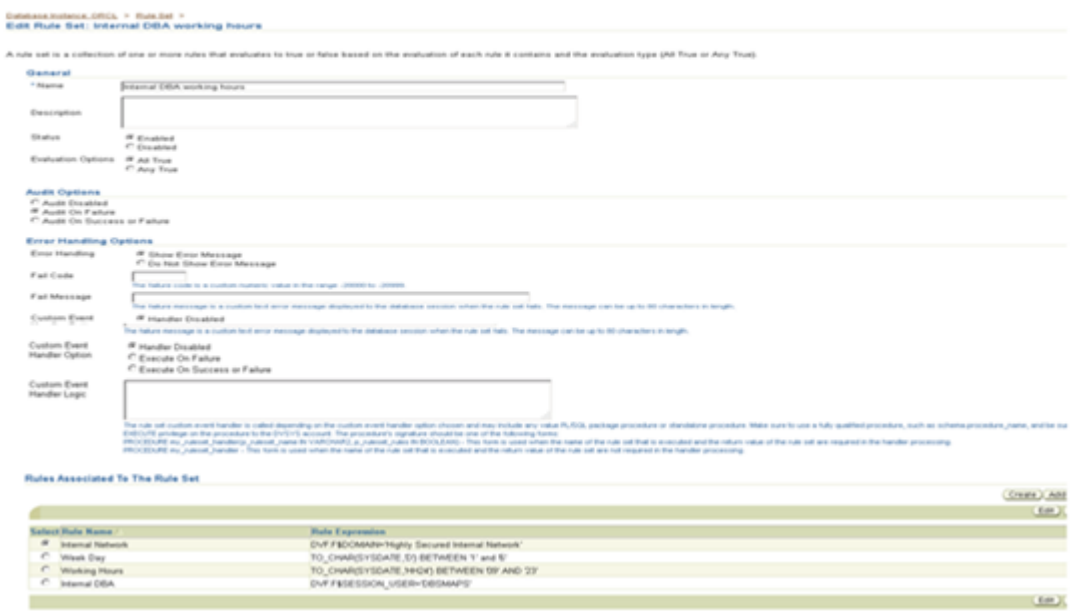
Rule Sets

Database Vault provides a rules engine that can be used in the security policy decisions of factors, realms, command rules, and secure application roles.

Select	Name	Evaluation Options	Error Handling	Audit Options	Rules Defined?
○	Allow Fine Grained Control of System Parameters	All True	Show Error Message	Audit On Failure	x
○	Allow Oracle Data Pump Operation	Any True	Show Error Message	Audit On Failure	✓
○	Allow Scheduler Job	Any True	Show Error Message	Audit On Failure	✓
○	Allow Sessions	All True	Show Error Message	Audit On Failure	x
○	Allow System Parameters	All True	Show Error Message	Audit On Failure	✓
○	Can Grant VPD Administration	All True	Show Error Message	Audit On Failure	✓
○	Can Maintain Accounts/Profiles	Any True	Show Error Message	Audit On Failure	✓
○	Can Maintain Own Account	Any True	Show Error Message	Audit On Failure	✓
○	Disabled	All True	Show Error Message	Audit Disabled	✓
○	Enabled	All True	Show Error Message	Audit Disabled	✓
◉	Internal DBA working hours	All True	Show Error Message	Audit On Failure	✓
○	RULE_SET_ALLOW	Any True	Do Not Show Error Message	Audit Disabled	✓
○	RULE_SET_INEX	All True	Do Not Show Error Message	Audit Disabled	✓

Şəkil 4.20. Rule set-in qurulması-1

Qayda yaradıb rule set-ə əlavə etmək -2



Edit Rule Set: Internal DBA working hours

A rule set is a collection of one or more rules that evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True).

General

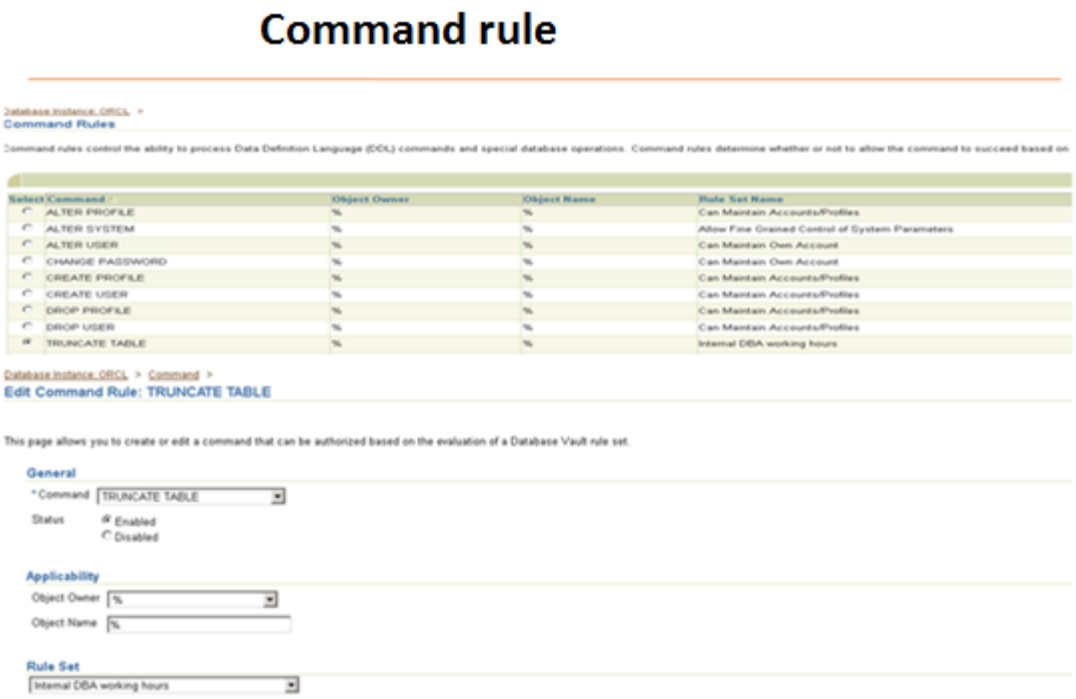
Audit Options

Error Handling Options

Rules Associated To The Rule Set

Select	Rule Name	Rule Expression
◉	Internal Network	DVF.F$COMMON='Highly Secured Internal Network'
○	Week Day	TO_CHAR(SYSDATE,'D') BETWEEN '1' and '6'
○	Working Hours	TO_CHAR(SYSDATE,'HH24') BETWEEN '09' AND '23'
○	Internal DBA	DVF.F$SESSION_USER='DBSMAPS'

Şəkil 4.21 Rule set-in qurulması-2



Şəkil 4.22 Command rule-un qurulması

sqlplus dbsmaps/dbsmaps

SQL> create table test (aaa char(1));

Table created.

SQL> truncate table test;

truncate table test

*

ERROR at line 1:

ORA-47400: Command Rule violation for TRUNCATE TABLE on DBSMAPS.TEST

SQL> select DVF.F$CLIENT_IP from dual;

F$CLIENT_IP

SQL> select DVF.F$DOMAIN from dual;

F$DOMAIN

Not Secured Network

SQL> exit

```
oracle@ksoracletest1 ~]$ sqlplus dbsmaps/dbsmaps@ORCL
SQL> truncate table test;
Table truncated.
SQL> select DVF.F$CLIENT_IP from dual;
F$CLIENT_IP
--------------------------------------------------------------------------------
195.87.212.68
SQL> select DVF.F$DOMAIN from dual;
F$DOMAIN
--------------------------------------------------------------------------------
Highly Secured Internal Network
SQL>
sqlplus ANARDB/ksxxxx11@ORCL
SQL> select DVF.F$CLIENT_IP from dual;
F$CLIENT_IP
--------------------------------------------------------------------------------
195.87.212.68
SQL> select DVF.F$DOMAIN from dual;
F$DOMAIN
--------------------------------------------------------------------------------
Highly Secured Internal Network
SQL> truncate table test;
truncate table test
*
ERROR at line 1:
ORA-47400: Command Rule violation for TRUNCATE TABLE on ANARDB.TEST
```

Nəticə

Bütün bu araşdırmalarımızın nəticəsi olaraq göstərmək olar ki, Oracle verilənlər bazası çox güclü qorunma və təhlükəsizlik texnologiyalarına malikdir. İstifadəçilərin verilənlər bazasına nə zaman, hansı komputerdən, gündə neçə dəfə qoşulduğunu, nə zaman xətalı qoşulduğunu və s. haqqında dərin məlumat almaq, istifadəçilərin hansı cədvələ hansı əməliyyatları etmək lazım olduğunu, həftənin günlərinə, iş saatlarına, İP ünvana görə qoşulmanı nizamlamaq olar.

Bu magistr dissertasiya işində Oracle Verilənlər bazası Vault araşdırıldı və onun digər istifadəçi texnologiyalarından üstün cəhətləri qeyd edildi. Həmçinin Azərbaycan banklarında Oracle VB-sının istifadəçi təhlükəsizliyinin müasir vəziyyəti və problemləri haqqında məlumat verilib, mövcud bazanın təhlükəsizliyi ilə Oracle verilənlər bazası vault qurulandan sonra yaranan bazanın təhlükəsizliyi müqayisə edildi.

Son olaraq, Oracle verilənlər bazası vaultun bank sistemində tətqiqi göstərildi.

Onu da qeyd edək ki, bu göstərilən üsullar Oracle-in yeni verisyası 12c-yə də uyğundu və biz Oracle verilənlər bazası vaultun 12c-də çıxan Privilege Analysis komponenti haqqında məlumat verildi.

Ədəbiyyat siyahısı

[1]. *Ault, Mike; Liu, Daniel; Tumma,* MadhuDon *Burleson, ed. "Oracle Database 10g New Features: Oracle 10g Reference for Advanced Tuning & Administration"*,2003

[2]. William Heney,Marlene Theriault,"Oracle Database 10g New Features; Oracle 10g Advanced Tuning & Adminstartion",2007

[3]. Ron Ben Natan, Elseiver Digital Press, 2013 "How to Secure and Audit Oracle 10g and 11g"

[4].Bureau Of Labor Statistics. "Database Administrators". 11/04/2015.November 2015.

[5]. David Knox,McGraw-Hill/Osborne"Managing Users and Resources". February 2004

[6]. http://www.dba-oracle.com/articles.htm

[7].Dan Norris,"Confirung System priviliges and Role authorization"," GoogleTechTalks, London, TUCS,2012.

[8].T.Kristense,T.R.Jesup,May,2011.[Online].Available:http://www.techonthenet.com/oracle/functions/user.php [Accessed 22 April 2015].

[9]. "Oracle Secure Global Desktop Enhances Application in the Enterprise". Press release (Oracle). April 30, 2013. Retrieved October 13, 2013.

[10].Ashdown.Lance, Kyte.Tom,"Oracle 10g Advance security techniques",2014.

[11]. Kreines, David C. ,"*Oracle DBA Pocket* Guide",2005.

[12]. Pete Finnigan, Insight Consulting, "How to secure oracle in 20 minutes", 2012.

[13]. Esteban Martinez Fayo,"Hacking and protecting Oracle Database Vault" Argentina, 2011.

[14]. https://docs.oracle.com/cd/E11882_01/server.112/e23090/toc.htm