جزوه درس امنیت بانک اطلاعاتی

نام استاد: جناب آقای مهندس قربانیان

در طراحی امنیت بانک دو موضوع مورد بررسی است:

۱-امنیت در طراحی بانک اطلاعاتی

۲- بکارگیری ابزارهای امنیتی بانک اطلاعاتی

که به دستور العمل های طراحی بانک نیز این ابزارها قابل پیاده سازی هستند.

نکته مهم : این است که همه بانک های اطلاعاتی دارای Back door می باشد. Back door به مدیر بانک مجوز می دهد تا از امکانات امنیتی بانک استفاده کند. ولی اگر دست کاربر و یا شخص مزاحم بیفتد بانک منحدم می کند مثل User یا SA در SQL Server .

در بعضی از بانک های اطلاعاتی مانند ORACLE چندین User و Admin داریم هر یک از آن ها دامنه فعالیت دسترسی خاص خود را دارد مثل User SYS, User sys Admin, User system که با هم فرق می کنند. این User ها دامنه ای از فعالیت های مختلفی از کاربران را تعریف می کند و به کمک آن ها می توان User های متعددی را تعریف کرد.

تذکر مهم : با وجود این تعاریف امنیت در طراحی بانک اطلاعاتی یعنی امنیت در هنگام پیاده سازی بانک بسیار مهم است.

در طراحی هنگام پیاده سازی موارد زیر را دقت کنید:

۱- تعیین درست جداول و صفات مشخصه، کلیدها
۲- نرمال سازی داده ها و ارتباط بین جداول و مرجع ها Reference
۳- تعریف حوزه مقادیر داده ها و استفاده از حوزه های اختصاصی مقدار برای آن (Buffer را کنترل می کند)

پس از انتخاب ساختار داده برای طراحی نوع نگرش طراح برای امکانات زیر روی Data Base تعریف می شود.

۱- تعیین موجودیت ها

۲- تعیین صفات خاصه

۳- تعیین مقادیر صفات خاصه

۴- تعیین Reference یا ارجاعات

با توجه به این موارد انتخاب نوع ساختار می تواند براساس سلسله مراتب یا درختی یا پدر و فرزندی باشد. در این ها طراحان Data Base به صورت سلسله مراتبی با رابطه ی ارث و میراث ، چند ریختی ، Deligation ، Polymorphism می باشد.

با توجه به نشست Data به صورت گراف یا در عوض هم می توانیم طراحی Data Base را به صورت شبکه ای انجام دهیم که برای نشست Data ، مدیریت آن و بازیابی آن از روش های درخت پوشا ، پیمایش عمقی و پیمایش گرافی استفاده کنیم . اما طراحی Data Base به صورت مجموعه ای که منجر به Data Base های رابطه ای می باشد.

بانک اطلاعاتی رابطه ای RBDBMS

در این بانک اطلاعاتی مجموعه یا set یکی از ارکان طراحی است که به کمک آن طبق تئوری رابطه می توانیم همه‌ی داده های خود را مثبت نمائیم. در این بانک های اطلاعاتی مجموعه و تعاریف مرتبط با آن مهمترین عامل اند.

M : مجموعه مرجع

A : مجموعه صفات خاصه

B : مجموعه مقادیر صفات خاصه

C : رکوردها

D : مجموعه موجودیت ها (رابطه)

$A = \{ A_1, A_2, A_3, \ldots\ldots\ldots\ldots \}$

$B = \{ B_1, B_2, B_3, \ldots\ldots\ldots\ldots \}$

$C = \{ C_1, C_2, C_3, \ldots\ldots\ldots\ldots \}$

$D = \{ D_1, D_2, D_3, \ldots\ldots\ldots\ldots \}$

$A \subset M$ $B \subset M$ $C \subset M$ $D \subset M$

$C \subset B$ $B \subset C$ $A \subset D$

درس(موجودیت) = { واحد، ساعت، کد درسی، نام درس }

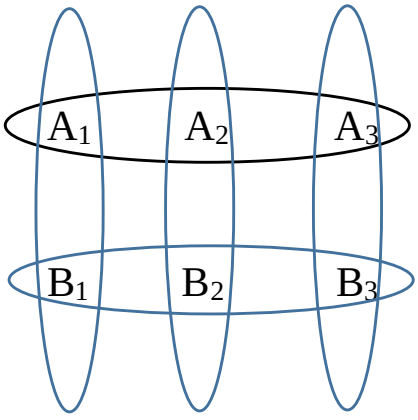
$D_1 \in D = \{ A_1, A_2, A_3, A_4 \} \in A$

$C_1 = \{$ ریاضی ,۴۸۰۱۲۰ ,۳ ,۳$\} \in C$

B_1

تک تک مقادیر می شود B

با توجه به شکل تعریفی مجموعه ها ، وقتی مجموعه ای موجودیت را تعریف می کنیم. یعنی رابطه را تعریف می کنیم که آن ها در تبادل انجام یک عمل روی هم تاثیر می گذارد و در آن صورت منجر به ارتباط Relation Ship می شود. وقتی ارتباط روی مجموعه ها تعریف شود برای پیاده سازی آن از شکل ماتریس داده استفاده می کنیم که به آن Table گویند.



از آنجایی که Relation طبق تعریف مجموعه شکل می گیرد همه ی قوانین مجموعه ها روی آن تعریف می شود و ماتریس ایجاد شده از قابلیت جبر رابطه ای استفاده می کند.

این ماتریس قابلیت اجتماع ، اشتراک ، تفریق ، ضرب ، جمع ، تقسیم و متمم گیری را خواهد داشت.

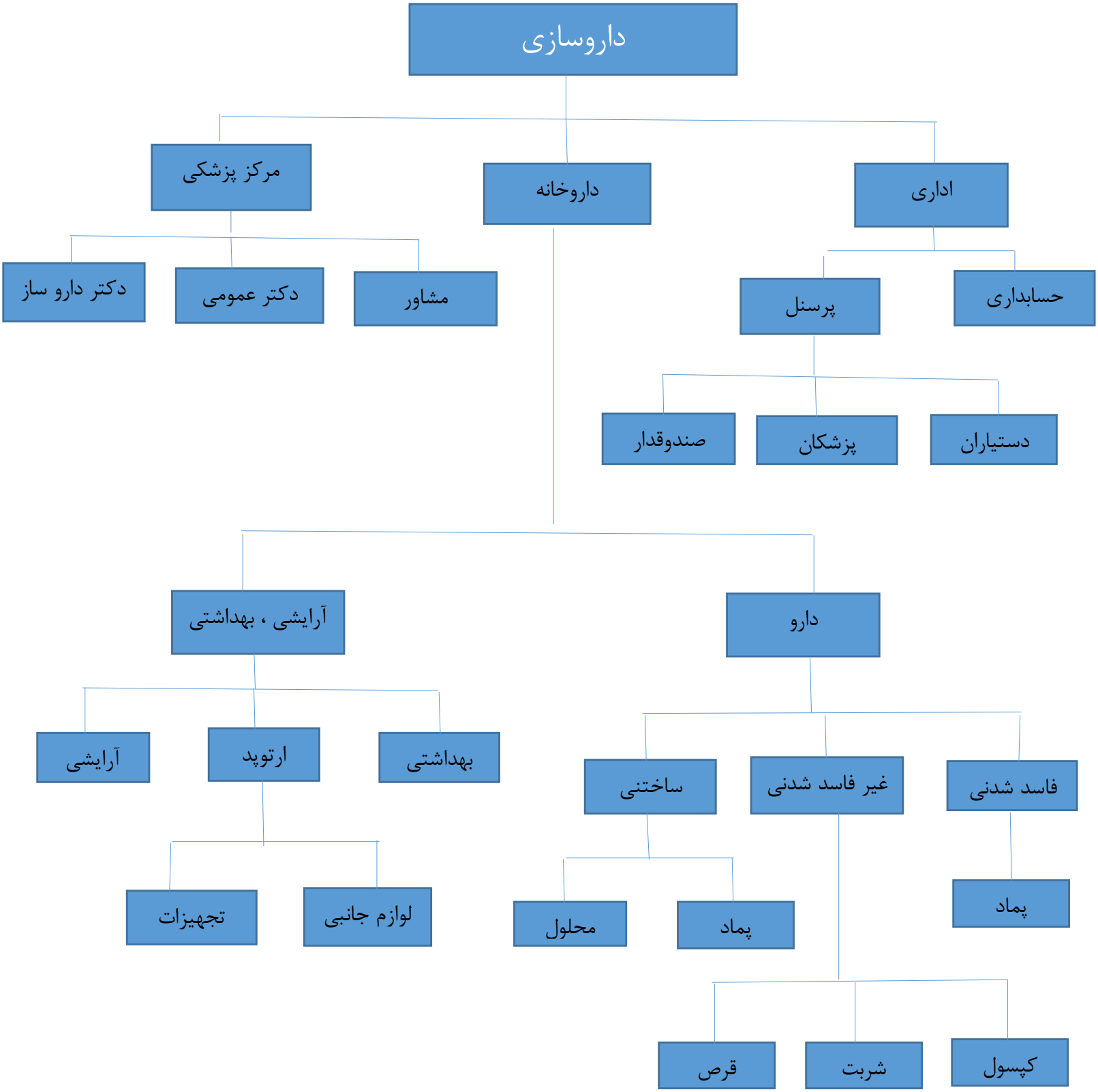
از آنجایی که عملیات ارتباط شامل حالت های مختلف پیوند روی جداولی است و از ضرب مجموعه ها استفاده می کند منجر به ضرب ماتریسی خواهد داشت که شامل عملیات نیم پیوند چپ، نیم پیوند راست، تمام پیوند و شبه پیوند می باشد.

Left Joined Right Joined Same Joined

این پیوندها منجر به تولید حجم زیادی خواهد شد. اگر هر طرف این پیوندها Data || Null وجود داشته باشد در آن صورت بر اساس نوع نرم افزار Data Base و همچنین بر اساس نوع طراحی منجر به تولید هیچ مقدار مضاعف می کند. که در آن صورت ماتریس اسپارس بوجود می آید و ضرب ماتریس ماتریس اسپارس باید کنترل و نرمالیزه شود.

یکی از راه های کنترل صفات مشخصه ها وارد کردن صفت مشخصه هایی که همیشه مقدار بگیرد. راه دیگر کنترل مقادیر وارد شده در Data Base می باشد که حوزه ی مقادیر صفات مشخصه را تعریف می کند. که هر صفت مشخصه مقدار خود را از آن حوزه خواهد گرفت و این مقدار کنترل روی کمیت و واحدهای استاندارد و اندازه گیری خواهد گذاشت.

تمرین: بانک اطلاعاتی برای دارو سازی ایجاد کنید توسط روش Hierarchy پیاده سازی کنید؟



Domain چگونه ایجاد می شود؟

Domain با دستور Create Domain ساخته می شود بعد از آن می توان Create Table صفت مشخصه مورد نظر را در Table ایجاد می کنیم

```
Create Domain
Create Table                    stable
(
Sname    Domain    mname
Or
Sname    nvarchar(20) , Not Null, Domain mname,
..
.
.
);
```

کاربرد Domain :

کاربرد Domain در این است که داده های مهم و واحدهای مرتبط با آن ها در ثبت بانک اطلاعاتی در جداول شکل بگیرد.

داده های مهم چه هستند؟

داده های مهم در بانک اطلاعاتی شامل : (کارت های اعتباری) Account , credit card حقوق و درآمد، مالیات، رکورد ها، گواهینامه ها، اعتبار نامه ها می باشد.

دزدی اطلاعات از Data Base شامل چه موارد هستند؟

بیشتر Account ، کارت های اعتباری و گواهینامه ها است.

نگرانی های دزدی از Data Base در چه بخشی هایی بیشتر است؟

۱- حمله به بانک اطلاعاتی SQL

۲- حملات Registry در تثبیت بانک اطلاعاتی درون سیستم عامل (حمله به ثبت وقایع SQL Server در Registry و ویندوز)

۳- حملات مربوط به تزریق کد

سطوح امنیت بانک شامل چه مواردی است؟

۱-سطح امنیتی انسانی :

سطح امنیتی انسانی که در این سطح کاربران و استفاده کنندگان Data Base مطرح می شود که شامل end user , programming user , Admin user می باشد.

۲- سطح امنیتی شبکه و user interface :

در این سطح packet ها واسط کاربر، محتویات داده ای آن ها که در شبکه در جریان است مورد تهدیدات امنیتی قرار می گیرند.

۳-برنامه کاربردی AP :

Application Program این است که در این قسمت شامل متدهایی است که داده های بانک و با تکنولوژی های برنامه نویسی جابه جا می کند.

۴-بانک اطلاعاتی Data Base System :

اصل جداول و داده های بانک و Query ها در این قسمت قرار دارند.

تذکر : در قسمت Data Base هنگام تولید جداول وinterface بحث نرمال سازی جزء موارد مهم امنیت است.

۵-سیستم عامل Operation System(os) :

سطح امنیتی عمل نشست Data Base و Registry یا ثبت وقایع آن و نحوه استفاده منابع Data Base مثل Intrupt ها،memory Range

۶-امنیت لایه فیزیکی :

در این قسمت ابزار و محل ذخیره سازی و محل های ارتباطی و همچنین سخت افزار ذخیره سازی و Media و همچنین سیستم های SAN نصب و سوار می شود و می توان دادهای آنها در هنگام نشست ، درون این سیستم ها رمزگذاری و رمزگشایی کرد.

امنیت در بانک اطلاعاتی Data Base Security چه مفاهیمی دنبال می شود؟

۱-در دسترس بودن دادها:

اولا Data : برای همه مواقع در دسترس باشد.

دوما Data : بدست کاربر خواهان مورد نیازش برسد.

۲- تایید پذیر بودن و تصدیق پذیر بودن: Authenticity

۱- منشاء Data کیست و آیا مطمئن است یا خیر

۲- نیاز به تایید دست یابی های کاربر و اینکه کاربر مورد نظر همان است یا خیر داشته باشد.

۳- تایید همه گزارشات درخواست شده از جانب کاربر تایید شده داشته باشد.

۴- Data خارج شده آیا به گیرنده اصلی آن رسیده یا خیر

۳-یکپارچگی یا جامعیت : Integrality

۱- تایید اینکه Data با فرمت اولیه به مقصد رسیده باشد.

۲- تایید اینکه همه داده های دریافت شده و وارد شده قابل تایید باشد.

۳- لازم به دانستن این است که گزارش همه تغییرات بر روی Data برمبنای گواهینامه و قوانین امنیتی استاندارد و محرز باشد.

۴-قابل استفاده بودن در صورت تخریب:

۱- اطمینان پیدا کنیم که داده موجود منحصر به فرد و اصل است.

۲- داده های درونی Data Base از جانب فرد گیرنده قابل اعتماد است.

۳- نیاز به جهت مهیا کردن گزارشاتی است که دسترس به Data بانک اطلاعاتی و چگونگی آن را مشخص کرده باشد و بگوید که چه کسی حق دسترسی دارد و چه کسی ندارد.

عمده اختلافات و ناامنی ها و اختلال در بانک شامل موارد زیر است:

۱-گم شدن ناگهانی داده ها در بانک (اشکال نرمال سازی)

۲-حملات بیرونی به بانک (تزریق کد SQL Server و حملات Fishing)

۳-مشکلات یا ضعف های امنیتی Storage ها و یا مشکلات مکانیکی آن ها

۴-دسترسی غیر مجاز مدیریتی یا بی سوادی مدیران بانک

نکته: در تعیین امنیت بانک ابزاری به نام میان افزار Middle Wave وجود دارد که ارتباط کاربر و داده را وسط می شود مثل لایه Business که بین لایه های Application و Data Logic در برنامه نویسی ASP.Net مورد استفاده قرار می گیرد.

نکته مهم : در تعیین ریزه کاریی های امنیتی درون Data Base ها از ابزاری به نام 3 rd party استفاده می شود.

که این ابزار برای بالا بردن Data Base و مانیتورینگ Data Base و پردازش کردن Data Base استفاده می شود این ابزار معمولی از تولیدکنندگان دیگر به کمک تولیدکننده Data Base می رسد. این ابزار می تواند به اجرای رمزگذاری Data Base کمک کند. عملیات پوشش گذاری ، همچنین بهم زدن scrambling را نیز انجام دهد.

نرمالیزه کردن

۱-موجودیت ها را جدا کنید (برای هر موجودیت به صورت مستقل صفات مشخصه تعریف شود)

۲- عنصر اصلی هر جدول که یونیک باشد.

۳-بین موجودیت های پیدا شد ارتباط تعریف می کنید.

۴-تکرار واصل قبل (از شماره ۱) تا زمانیکه همه ارتباطات تعریف شده باشد و دیگر جدولی قابل تجزیه نباشد.

۵-Reference تعریف کنید. کلید خارجی

یک جدول کلی برای یک لباس فروشی که تهیه کنیم ایرادهای پیش آمده ۱- تکرار داده ها و افزونگی ۲- پیچیدگی

آدرس	خریدار	تخفیف	زمان	تحویل	جنسیت	رنگ	سایز	جنس	فروشنده	نوع لباس	لباس

جدول ها را می شکنیم

جدول خریدار

کد	آدرس

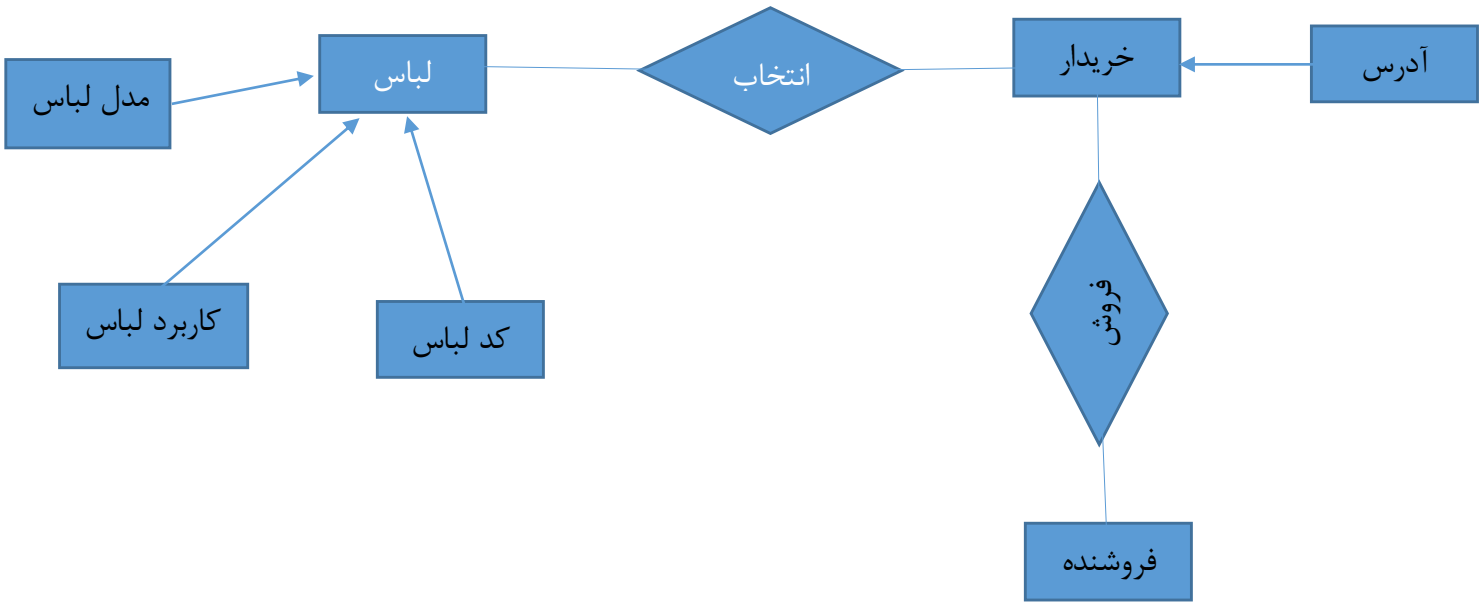
جدول نوع لباس

کد

جدول لباس

کد

پس از مراحل نرمال سازی Data Base با تمام جداولش طراحی می شود.



تمرین : یک Data Base در نظر گرفته و مانند SQL Server یا ... بخش های امنیتی آن را برشمارید؟

SQLDict

این ابزار که در سطر فرمان تمامی ویندوزها قابل اجرا است، تدارک یک حمله دیکشنری علیه SQL Server را می دهد. جهت بکارگیری آن باید IP ماشین هدف، شناسه‌ی کاربری که می‌خواهید رمز او را به دست آورید و فایلی که حاوی رمزهای عبور برای چک کردن می باشد را مشخص کنید.

CPMdeamon

این برنامه که در محیط لینوکس نوشته شده است، یک کد CGI را اجرا می‌کند و اجازه¬ی عوض کردن رمز عبور را از راه دور می دهد.

SQLScanner.exe

این ابزار که در سطر فرمان ویندوز اجرا می شود، یک محدوده آدرسIP از نوع کلاس B(XXX.XXX) و نام یک فایل خروجی را به عنوان پارامتر می گیرد، و سپس محدوده را جستجو کرده و IP¬هایی را که دارای Sql Server هستند مشخص می نماید و در فایل خروجی لیست می کند. این ابزار قادر به شناسایی Server SQLهایی که از درگاه استاندارد ۱۴۳۳ استفاده نمی کنند نیز می باشد.

SqlPing.exe

این برنامه ی سطر فرمان ویندوز، اطلاعات مفیدی (نظیر نام سِرور، شماره ی نسخه ، شماره ی درگاه و ....) در مورد یک SQL Server نصب شده بر روی یک IP خاص ارائه می دهد.

NGSSQLCrack

NGSSQLCrack ابزاری است که جهت شکستن رمز عبور در SQL Server۷ و ۲۰۰۰ بکار گرفته می شود.

بانک اطلاعاتی سلسله مراتبی

در بانک اطلاعاتی سلسله مراتبی طبق نمونه فوق (مثال دارو سازی) چون رابطه پدر و فرزندی برقرار است بنابراین نرمال سازی بانک دارای ضریبی از ارث بری در بانک و همچنین پیمایش های Thread در بانک می باشد.(پیمایش معکوس درختی از فرزند به پدر و پیمایش رشته ای درخت‌ها)

در این نمونه بانک برای دستیابی به Object ها بصورت سلسله مراتبی از هم ارث می برند.

عملیات نرمالیزاسیون در این بانک به کمک روابط Deligation واگذاری انجام خواهد شد.

خطرات محیطی بانک اطلاعاتی شامل چه مواردی خواهد بود؟

۱-بکارگیری ابزار واسط روی داده های ذخیره شده که به کمک Query انجام می شود.

Query روی چند جدول متصل بهم انجام می شود و دچار Reference to Reference شدن Data می شویم و تشکیل یک Loop می دهند. Query باعث می شود جدول حاصله چندین برابر جواب مورد نیاز حجم بگیرد که دارای افزونگی و تکرار است.

۲- حملات مستقیم Data Base که باعث تغییر در صفات ، نتیجه Query ها و همچنین پیوندهای جداول انجام می شود.

پیاده سازی SQL Injection با کمک

Drop Table
اسم جدول

Alter Table
اسم جدول

در واقع تزریق کد به بسته ها

۳-حملات مربوط به ردیابی یا Tracing داده که به عملیات Track یا دزدی بسته ها مربوط می شود و باعث می شود تا Data Base داده هایش با داده های دیگر جایگزین شود.

هم SQL Injection داریم هم دزدی رمز بسته ها داریم .

برای جلوگیری از این سه عمل بالا

۱-از داده های رمز شده استفاده می کنیم .

۲- از بانک اطلاعاتی شی گرا استفاده کنیم.

۳-از قوانین استفاده کنیم.

نکته : در حملات مربوط به Data Base عموما یا بصورت متداول برهم ریزی امنیت روی محتویات Data انجام می شود اما اگر از رمزگذاری BLP روی آن ها استفاده شود در این صورت جلوی حملات گرفته خواهد شد و در حال حاضر BLP یکی از پر کاربرد ترین رمزگذاری ها روی محتوای Data Base است.

برای تامین امنیت بانک اطلاعاتی چه مواردی را باید در نظر بگیرید؟

۱-حساس کردن داده ها نسبت به متغییر مانند تغییرات بروز رسانی Trigger ها یا قوانین حفاظتی تعریف کنیم.

۲-کنترل دستیابی ها به سطوح مختلف بانک و Data که باعث بوجود آمدن تغییرات در بانک خواهد شد.

این کنترل ها برای تعیین هویت و کنترل XML ها استفاده می شود چون رابطه های XML با خود محتویات را رد و بدل می کنند که امکان تغییر در بانک در آن ها محتمل است با کمک این رابطه ها دست یابی مجوز بانک و دست یابی به سرور زیاد است و امکان ورود داده هایی غیر مجاز به بانک زیاد است.

۳-بعضی از بانک ها از نوع بانک اطلاعاتی شی گرایی هست OODBMS . این بانک ها برای دستیابی به داده هایشان از یک سری رابطه های معنایی بر اساس مدل شی گرا استفاده می کنند. این مدل بانک را قادر می سازد تا به محتویات اصلی با مجوزهای طراحی شی گرا دسترسی داشته باشد. در سیستم های OODBMS اصولا طراحی بصورت سلسله مراتبی است.

بانک اطلاعاتی قبل از سال ۲۰۰۰ چه ابزارهای امنیتی داشتند؟

این بانک ها عمده ترین مسئله امنیتی که داشتند استفاده از رمز عبور و دسترسی های ساده به Data بود اما در هنگام توزیع شدن Data دچار حملات پخشی Data می شوند و چون داده های آن ها بصورت باز و ساده در سطح مسیریاب های شبکه حرکت می کرد از نظر امنیتی راحت در اختیار این حملات قرار می گرفت تا زمانیکه SQL Server 2000 اقدام به تعیین سطح امنیتی روی Data Base کرد که به دو صورت سیستم عاملی و امنیت Data Base معروف است و در Data Base ، SQL Server 2003 مشکلات توزیع پذیری Distribution برطرف شد و در SQL Server 2005 رده های امنیتی توزیع پذیری بصورت لایه هایی از معماری امنیت Data Base طراحی شد.

نیازمندی های امنیتی بانک اطلاعاتی

۱-لایه امنیتی فیزیکی و سیستم عاملی :

در این لایه پایین ترین سطح امنیتی تعریف می شود. حق دسترسی های سیستم عامل به دستیابی فایل ها از یک حالت سنتی به یک حالت طبقه بندی شده تبدیل می شود. خطاهای مدیریتی با Administrator در این بخش کنترل می شود. حفاظت در برابر ویروس ها و همچنین حملات ویروسی در این سیستم ها تعریف می شود و مقابله با آن ها برای مدیران ، سیستم عامل بصورت دستورالعمل های خاص ارائه می شود در جامعیت فیزیکی ممکن است خطر های آتش سوزی، خربکاری دیسک یا اشکالات مکانیکی دیسک باعث برهم زدن امنیت فیزیکی بانک های اطلاعاتی شود.

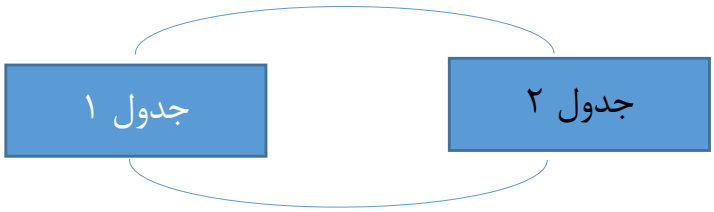
۲-سطح منطقی بانک اطلاعاتی :

در این سطح جامعیت داده ای مورد بحث قرار می گیردو همچنین طراحی منطقی Data Base از لحاظ امنیتی دچار لایه بندی های مختلف می شود.

در این بخش امنیت در کلیدها و Reference ها و همچنین رمزگذاری یا تغییر ماهیت داده در بخش ذخیره سازی و همچنین ترکیب چند Data Base در یک سیستم توزیع پذیری تعریف می شود.

۳-جامعیت مولفه ها ویا المان های Data Base :

در این جامعیت فیلدهای کنترلی (منظور کلیدهای کاندید ، اصلی و کلید خارجی)عامل های اتصال و ارتباط موجودیت ها ، Trigger ها یا دستور العمل های کنترل جهت (تعریف interface برای ارجاع جداول و Schema, User , Data Base) بروز اتفاقات خاص مثل حذف یا بروز رسانی یا همچنین دستور العمل های ذخیره سازی جدول های Temp و همین طور جدول های ناشی از Query ها و مدیریتی دسترسی کاربران به داده های آن جدول ها تعریف می شود.



جدول ها ارتباط داشته باشند و وابسته جدول دیگر باشند که در اثر بروز رسانی و حذف یکی از سه روش (cas coad , nulifield , ristricted) اتفاق می افتد تولید اطلاعات جدید می شود یا داده ها ناخواسته حذف یا تغییر می کند.

تذکر : عملیات Trigger و Store Procedure از جمله عملیات مهم است که لایه بندی نرم افزاری استفاده می شود و باعث تامین امنیت بانک در لایه های نرم افزار شد.

۴-دستیابی یا قابلیت های ممیزی :

در این قسمت مجوز دستیابی به Data Base و ردیابی فیلدهای خاص و همچنین مدیریت Trigger ها و عملیات ثبت وقایع انجام می شود. ثبت وقایع شامل Query هایی است که کاربر روی Data Base می زند.

تذکر: این بخش هر چقدر کامل تر و دقیق تر می شود مقابل SQL Injection دوام می آورد.

۱-Trigger ۲-Shaddow Table (تصویر مجازی از کل Data Base نشان می دهد و با view فرق دارد) ۳- فیلد ثبت وقایع Tracking ۴- ثبت Query

۵-Access Control :

در این قسمت چه کسی به چه چیزی دسترسی پیدا می کند را مشخص می کنیم حق دسترسی ها امکان دسترسی به تک تک جدول ها و تک تک عملیات برای کاربران تعریف می شود مثلا به کاربر اجازه می دهیم که به چه جدولی دسترسی داشته باشد یا بچه عملی در آن جدول انجام دهد. در SQL Server به آن Grant و Revoke می گویند.

این قسمت در Data Base بصورت Role تعریف می شود و حالت های پیش فرض را در Data Base تغییر می دهد.

این بخش یکی از مهم ترین بخش های کنترل Data Base است.

۶-تشخیص User یا هویت کاربر :

تعیین نام برای کاربر(همان تعریف User) ، تعیین پسورد برای آن، مشخص کردن زمان ماندگاری کاربرو زمان ماندگاری پسورد در SQL ، User و SA داریم که دسترسی به همه چیز دارند.

۷- قابلیت دسترس بودن Availability :

۱- Data یا داده ای که نیاز به دسترس در هنگام نیاز در دسترس باشد.
۲- داده های مورد نیاز برای کاربران خاص خودشان باید در دسترس باشند.
۳- داده ای که در دسترس است قابلیت ردیابی داشته باشد که از چه کسی به دست چه کسی رسیده باشد.

طراحی نقشه امنیتی برای بانک های اطلاعاتی

این نقشه کمک می کند تا یک بانک اطلاعاتی با قابلیت های امنیتی مختلف در نظر گرفته می شود معمولا نقشه های امنیتی بانک های اطلاعاتی را با Oracle ترسیم می کند یا با ماکروسافت و شامل این اقلام می باشد.

۱-Platform بانک اطلاعاتی یا سیستم عامل Data Base :

محل اسقرار Data Base را نشان می دهد. در این بخش Platform کمک می کند تا نوع نگاه به اهمیت Data Base تعریف شود چون در Oracle و ماکروسافت دو دید مختلف طراحی وجود دارد (هم User متفاوت کنترل می شود و هم طراحی متفاوت انجام می شود).

۲- نام Data Base یا SID :

این بخش به کمک طراح باعث می شود که یک شناسه یا یک اندیس Index برای دسترسی به Data Base در بین Data Base های موجود تعریف شود.

۳-Function Data Base :

عملکرد Data Base یا Function Data Base یکی از راه های تشخص و تایید امنیتی Data Base است.

۴-Application :

در طرح امنیتی بانک های اطلاعاتی Application کمک می کند که داده های ورود به Data Base و خروج از Data Base بشناسیم.

۵-مالک برنامه کاربردی یا Application Owner :

برنامه کاربردی که به Data Base متصل می شود یک استفاده کننده و یک مدیر دارد در این قسمت باید آن را مشخص می کنیم.

۶-User Name و Password :

در این قسمت دو عامل تعریف می شود که برای دستیابی هاPlan امنیت Data Base بسیار مهم است.

۷-سیستم شناسایی User ها و تمیز قرار دادن User هایی که می توانند Account ایجاد کنند.

۸-انواع سیستم های مجوز دهی و تعریف کاربردی آن ها در Data Base

۹-قالب های پشتیبانی گیری از Data Base

۱۰- تعریف سیستم های Recovery و بازیافت اطلاعات در بانک های اطلاعاتی :

در اینجا هر روشی بتواند بانک اطلاعاتی را بصورت سریع و بدون خطا بازیافت کند و یا مقابل از بین رفتن آن شود تعریف می کنیم.

۱۱- تعریف Role :

در این قسمت هر عمل مختلف انجام می شود:

۱- مجوزهای اجرایی
۲- مجوز های تغییر و حذف
۳- شناسایی Application ها و داده های آن ها و اجازه انجام Recovery و Backup

Privilege چیست؟

این بخش مجوزهایی است که اجازه می دهد یک سری سرویس به کاربر نسبت داده می شود و هر عملیاتی که او می تواند انجام دهد را شامل شود مثلا در هنگام نصب می توان به یک سری از کاربران خاص مجوزهای متفاوت دسترسی به Table ، خاموش و روشن کردن Data Base ، Log گرفتن Data Base و همچنین حذف و برگرداندن جداول و داده ها

تذکر : این بخش در بانک اطلاعاتی Oracle بصورت خاص و با امکانات مختلف برای User های اصلی Oracle تعریف شده است.

چه دستوراتی به Privilege جهت کنترل و دستیابی بانک نوشته می شود؟

1- Grant Privilege On Object To Users
2- Revoke Privilege On Object From Users

تذکر: در دو دستور فوق Privilege ها شامل موارد زیر هستند :

Privilege : Insert , Update , Delete , Referencive , Select , Drop

مثال : می خواهیم به User و A1 اجازه عمل Update را روی جدول T1 بدهیم؟

```
Grant Update On T1 To A1
```

مثال : مجوز درج از جدول Student از کاربر از آموزش ۱ بگیریم ؟

```
Revoke Insert On Student From Amozesh1
```

تذکر : می توانیم فیلد های خاصی از جداول نیز را مورد استفاده مجوز قرار دهیم مثلا در مثال قبل کاربر آموزش ۱ مجوز درج در فیلدهای Name , StdId را نخواهد داشت.

Revoke Insert On Student{ Name , StdId }From Amozesh1

۱- قبل از Privilege تعریف سطوح کاربری است

۲-قانون مند کردن پسورد که شامل موارد زیر است :

۱- طول مشخص داشته باشد

۲- پیچیدگی آن ها تلفیق عدد و کارکتر باشد

۳- تاریخ تولید و انقضا داشته باشد

۴- زمان های تعویض پسورد متغیر باشد

Privilege را بصورت دستی نیز می توان تعریف کرد که همان Grant و Revoke است

Grant Select On employ To User1

مجوز دستور Select را به User از جدول employ

Grant Update On employ { name , family , data } To User1

به User مجوز بروز رسانی نام ، فامیلی و تاریخ را می دهد.

Revoke Drop on employ From User1

اجازه حذف جدول را از User می گیرد.

Multi Level Access :

یکی از مهم ترین نقاط آسیب پذیری Data Base است. اگر درست تعریف نشود بدین منظور بر اساس وظایف کاربران را طبقه بندی می کند و به هر طبقه یک سری کاربر و عملیات آن را نسبت می دهد. در این صورت هر کاربر هر عملی را که بخواهد انجام دهد باید در آن کلاس تعریف شده باشد با همان Grant و Revoke است.

مثلا فرض کنید آموزش در دانشگاه وظایف زیر را دارد:

۱- برنامه ریزی ۲- امتحانات ۳- ثبت نام ۴- دعوت به اساتید ۵- حضور و غیاب اساتید دانشجویان

بخش آموزش به لیست اساسی دانشجویان ، ثبت نام ها ، شهریه های انتخاب واحد دسترسی دارند.
بخش امتحانات به لیست دانشجویان و نمرات دسترسی دارند.

اگر کابران امتحانات را در کلاس B در نظر بگیریم و کاربران ثبت نام را در کلاس D و کاربران برنامه ریزی را در کلاس Fهر یک از این کاربران عضو کلاس مورد نظر می شود و می توان بر اساس آن حق دستیابی چندگانه یا چند منظوره را شکل داد.

Class	User	Table	Field
A	user1	Student	
F	user3	Entekckab	
B			
C			
A	user5	Entekckab	

چه داده هایی بصورت داخلی در امنیت بانک شرکت می کنند:

۱-داده های تعریف در Domain ها

۲-دادهای رمز شده که باید در دیکشنری قرار می گیرند

۳-داده هایی که تازه ایجاد شده اند

۴-آدرس هایی که در درایو داده در آن قرار دارد

۵-بخش هایی از جداول که بصورت Permission و Privilege به User داده می شود

۶-فرم هایی که با Data Base در تبادل هستند

در بانک اطلاعاتی برای کنترل حملات و آمارگیری به چه مواردی باید دقت داشته باشیم؟

۱-کنترل روی Query ها :

کنترل Query بر مبنای اجرا شدن دستورالعمل های غیر مجاز است. مثل SQL Injection

۲-کنترل روی آیتم های امنیتی Data Base :

دسترسی روی User های خاص

۳-کنترل از نظر حجم پرسش و پاسخ ها و فرم های مربوط به آن ها :

این مسئله به نحوه نرمالیزاسیون و Reference ها مرتبط می شود

۴-محدودیت پاسخگویی Data Base :

کنترل در راستای درخواست مجاز و پاسخ مجاز آن درخواست

۵-کنترل روی نقاط جداول نرمال شده :

بعد از نرمال کردن Data Base باید کنترل میزان وابستگی Data Base

۶-تجزیه و تحلیل Query زده شده در طرح آنالیز Data

تعریف نقاط آسیب پذیری در Data Base ها بیشتر روی چه مناطقی از Data Base تاثیر گذار است؟

۱-ورودی های غیر مجاز:

در کارهای ورودی مثل Login , Password , Form ها ممکن است.

۲-دستورالعمل های از قبل تعریف شده :

Store Procedure , Trigger

۳-دستورهای برنامه نویسی از قبل نوشته شده :

Component ها

۴-کتابخانه های غیر قابل دسترسی در Data Base ها :

Framwork (روش های اتصال به Data Base از طریق نرم افزارها و خواندن همه Data Base یا واکشی آدرس Table ها از Data Base)

Multi Three Programming :

در این بخش که مهم ترین قسمت امنیت Data Base است برنامه نویسی لایه ای مطرح می شود. در برنامه نویسی لایه ای می توانیم دست کاربر را بطور کلی از Data Base جدا کنیم به این شرط که از یکی از تکنولوژی ها استفاده کنیم :

1-Hibernate 2-Or Mapping 3- Entity Framwork

این سه نوع تکنولوژی کمک می کند تا نحوه اتصال به Data Base و مدیریت آن را از نظر دستیابی کاربر مشخص شود. در برابر Framwork Entity کاربر کاملا از Data جدا است. Data کاملا

بصورت آدرسی قابل دستیابی است و این آدرس در سطح Business تعریف می شود و کاربر نمی تواند آن را مورد دستیابی یا نفوذ قرار دهد.

دفاع در برابر حملات چگونه شکل می گیرد :

۱-بکارگیری درست برنامه نویسی

۲-تنظیم پسورد و رمزنگاری

۳-تنظیم امنیت رسانه های ذخیره سازی

۴-کنترل محتوا Store Procedure ها و کمتر استفاده کردن از آن ها

۱۰ عنوان امنیتی برتر برای تهدیدات امنیتی بانک های اطلاعاتی :

OWASP یکی از استانداردهایی که خطر ها را روی شبکه کم می کند و این تهدیدات شامل موارد زیر است :

۱- عدم بکارگیری Privilege ها در سطح اجرا
۲- عدم بکارگیری در Privilege ها درسطح تعریفی و منطقی سیستم
۳- حق انتخاب Privilege ها در اجرای شناسایی و تهدیدها مثل قرار دادن IPS در Data Base
۴- نقاط ضعف Plat Form Data Base
۵- حملات تزریق کد SQL Injection در Data Base
۶- سر ممیزی ضعیف از حساب های کارو در حال اجرای و حساب های بلا استفاده
۷- حملات مربوط به سرویس ها و تغییر در Cash و Buffer
۸- نقاط آسیب پذیری در پروتکل های ارتباطی Data Base
۹- تغییر مجوزهای دستیابی و ضعف تعریف مجوزها در Data Base
۱۰- Replication & Backup در Data Base

تصمیم گیری بر مدیریت ریسک ممیزی یا Accounting شامل چه گزینه هایی می شود؟

1- Requlatory – Risk
2- Detterence
3- Detection & Recovery

امنیت در Data Base Oracle :

در Oracle ساختار امنیتی از ورژن ۷ تا ۱۲ به شکل زیراست. در این بخش Network Encryption اولین فاز عملیاتی را تشکیل می دهد.

Authentication در حد محدود به Login , Password بود.

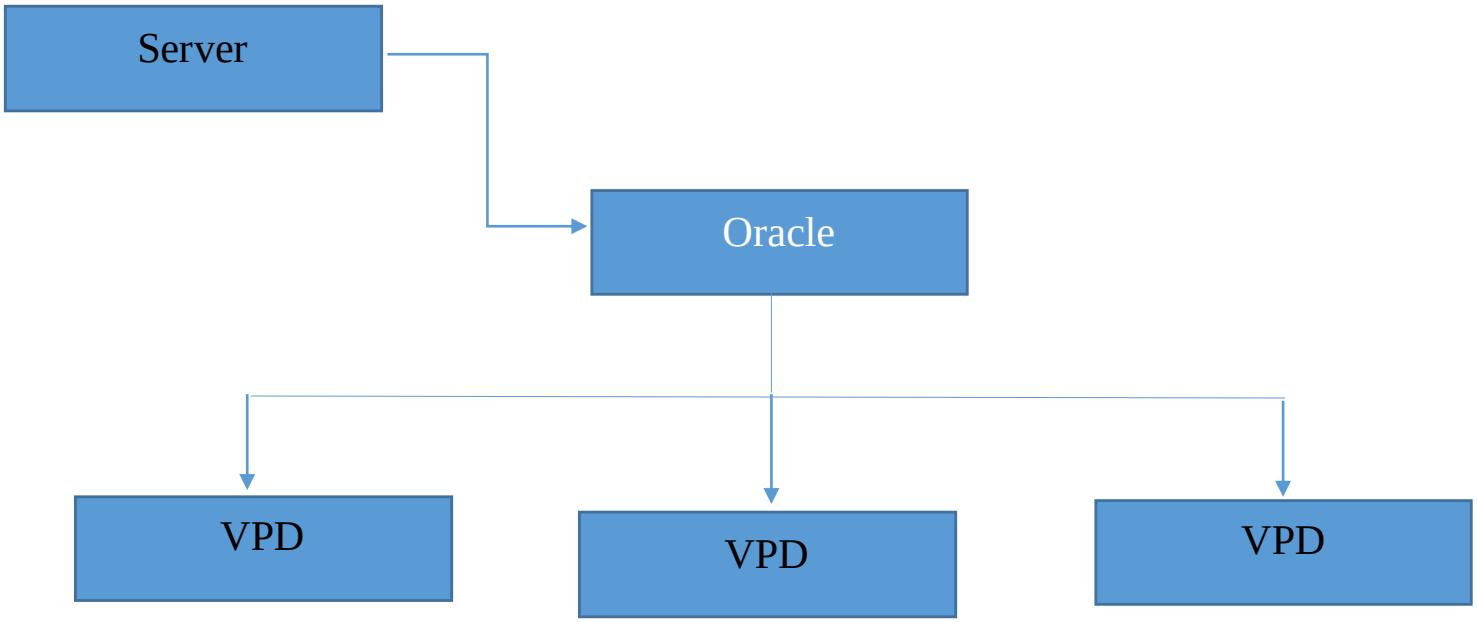
رمزنگاری از نوع PKI می باشد (رمزنگاری نا متقارن) در ورژن ۸ امکانات شبکه گسترده تر و امکان Kerberos نیز تعریف می شود.

امنیت User در سطح Multiuser و Inter pri user در ورژن 8.I تعریف می شود. در این VPD (Virtual Private Data Base) در این ورژن محدوده عملیاتی مشترک بین Data Base تعریف می شود نیمی چند Data Base از رمزگذاری داده مشترک استفاده می کند. ورژن 9.I ، Authentication ممیزی جهت کاربران و کاربران متفاوت با سطح اجرایی متفاوت انجام می شود.

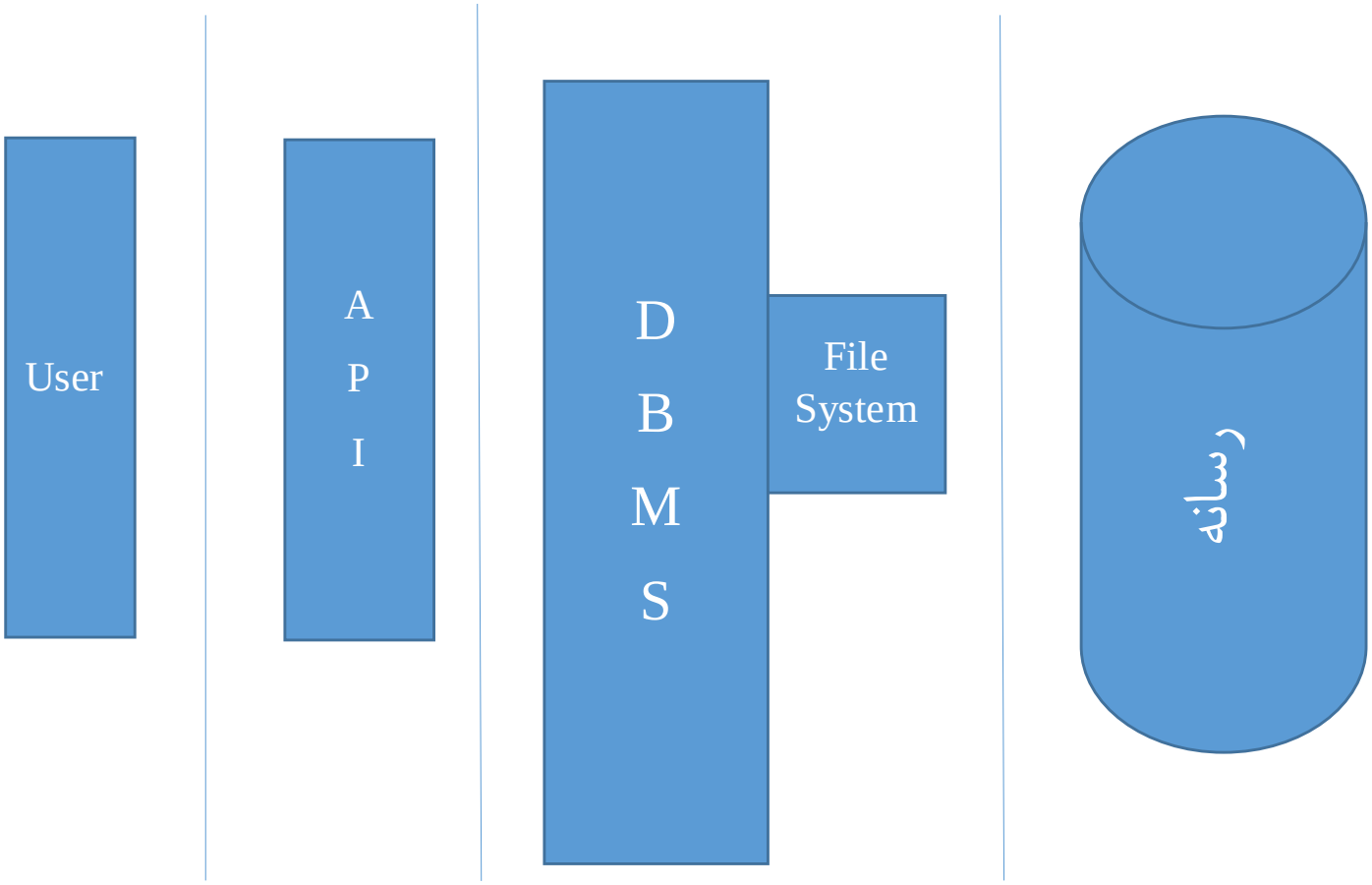
در سال ۲۰۰۱ تا ۲۰۰۳ ورژن 9.I باعث تعریف Policy (قوانین امنیتی) روی VPD شد. در سال ۲۰۰۳ رمزگذاری Transparent (شفاف) تعریف شد.

از Oracle ، 10.g به بعد ممیزی امنیت روی User ها بصورت سیستم عامل Data Base تعریف می شود.

از 10.g به بعد Oracle بانک اطلاعاتی خود را تبدیل به یک file System و سیستم عامل مجزا کرد.



Wave House انباره است در Oracle در سال ۲۰۰۳ بوده در SQL در سال ۲۰۱۴ داریم.



Oracle قدرت رمزنگاری با کمک استاندارد BLP را دارد و رمز آن نسبت به DB2 ۵۰ برابر قوی تر و شکست ناپذیر است. نسبت به SQL ۲۰ برابر قوی تر است. در مجوزهای دستیابی و ممیزی ۵۰ برابر از SQL Server قوی تر و تکنولوژی های Transparent Data Encryption ۳۰ برابر SQL Server قوی تر است.

چرخه Oracle :

۱-هسته مرکزی امنیت یا محل استقرار Platform (تست روی سیستم عامل)

۲-مدیریت User (کاربر) شامل امنیت توسعه یافته و مجوزهای مربوط به کاربران در سیستم عامل و Data Base

۳-کنترل دسترسی :

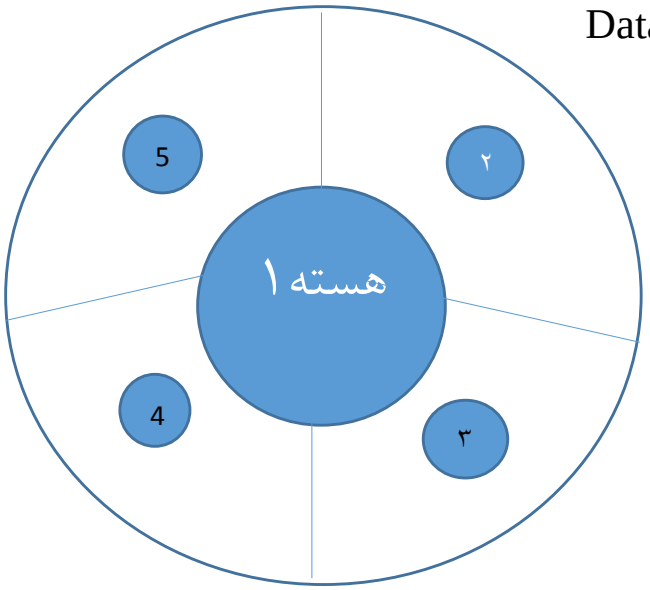
۱-دسترسی VPD

۲-دسترسی به دیکشنری مشخص کردن برپسب های امنیتی

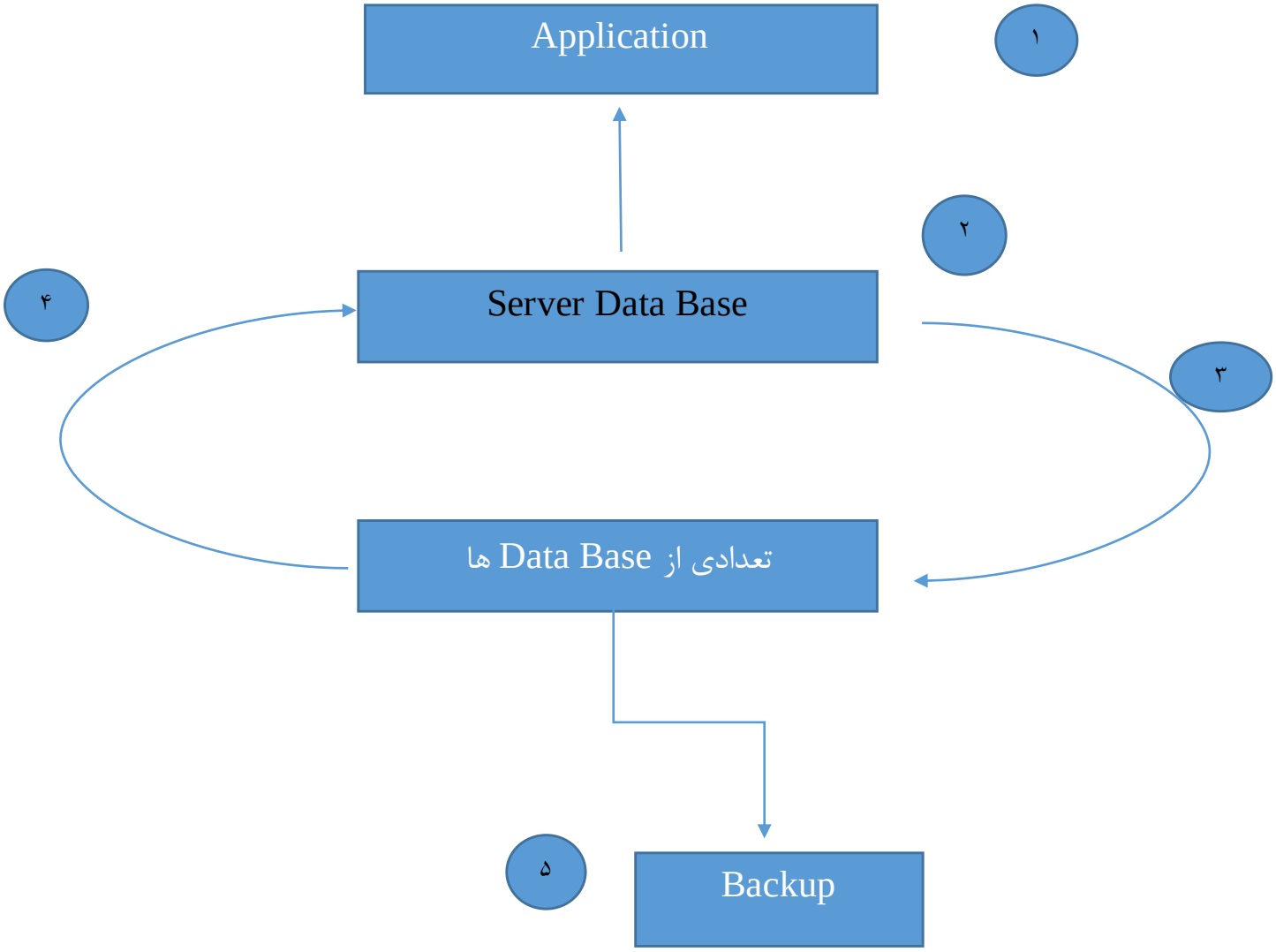
۴-تعریف IPS در Data Base

رمزنگاری سطح بالا و مدیریت امنیتی Backup

۵-نظارت بر مراحل اجرایی و ارتباطی ها Data Base



کاربر ۵ مرحله قبل در نحوه اتصال و استفاده از Data Base



۱-تعریف دسترسی ها با رمز و نام کاربری و همچنین مدیریت شناسایی و تشخیص هویت قوی Access Control که از PKI استفاده می شود.

۲-Network Security فایروال ها ، IPS ها ، IDS ها و رمزنگاری چون بسته ها به سمت Data رمز می شود.

۳-عملیات ذخیره سازی Writing Data با رمز نوشته می شود و رمز آن تغییر نمی کند.

۴-Reading Data + رمزگشایی Decryption می شود.

۵-همان عمل نوشتن با رمز قبلی

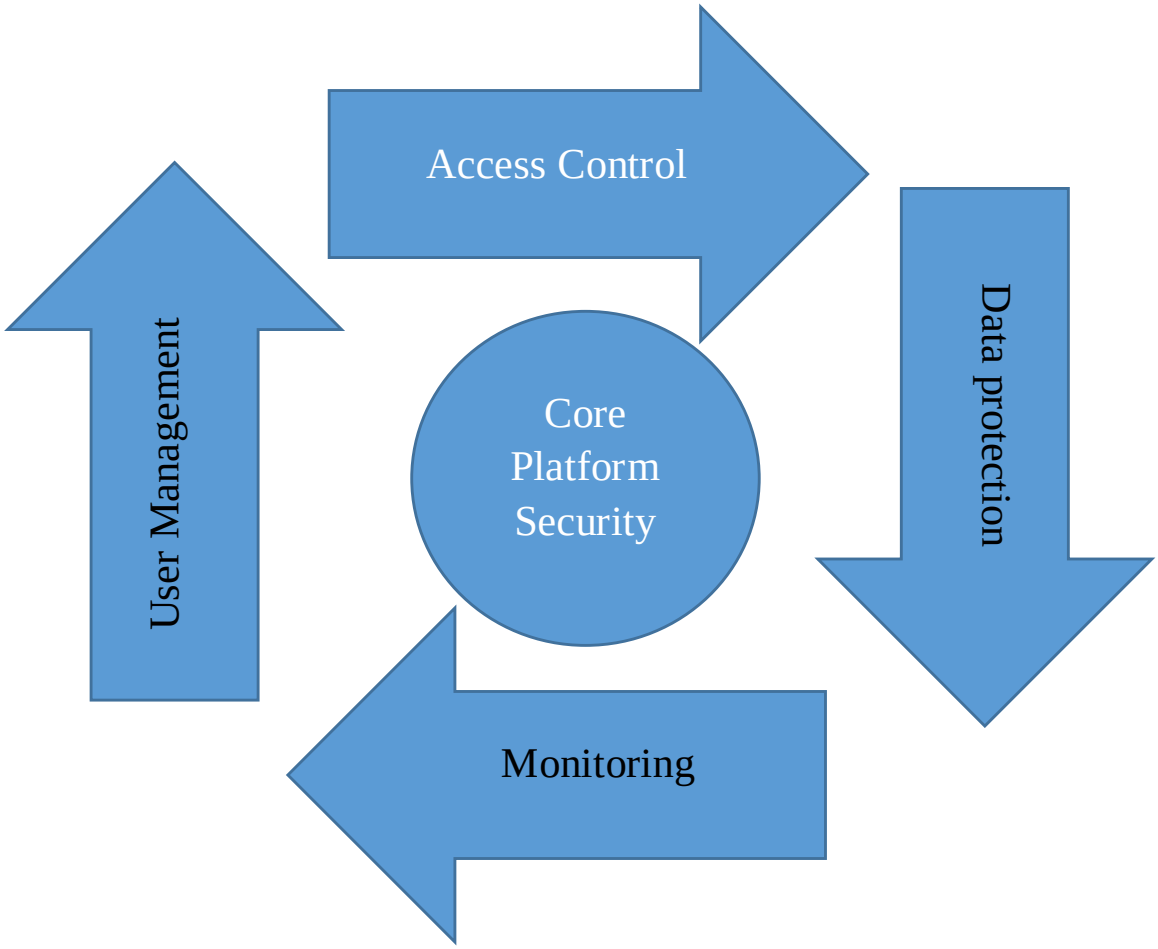
در Oracle خود Data Base خودش رمزگشایی و رمزگذاری می کند و فقط کلید دست کاربر است.

به مرحله ۲ و ۳ و ۴ به آن رمزنگاری پیشرفته می گویند . Advance Security یا Transparent Data Encryption

این پنج مرحله چرخه امنیت Data Base ، Oracle است و رمزنگاری آن از نوع Transparent و مدل استاندارد و رمزنگاری نظامی یا ALP است.

در شکل زیر ۵ مرحله امنیت بصورت یک چرخه اجرایی برای امنیت Data تعریف می شود

Data Security Component



Access Control :

1- Oracle Data Base Vault
2- Oracle Label Security
3- Virtual Private Data Base

User Manager

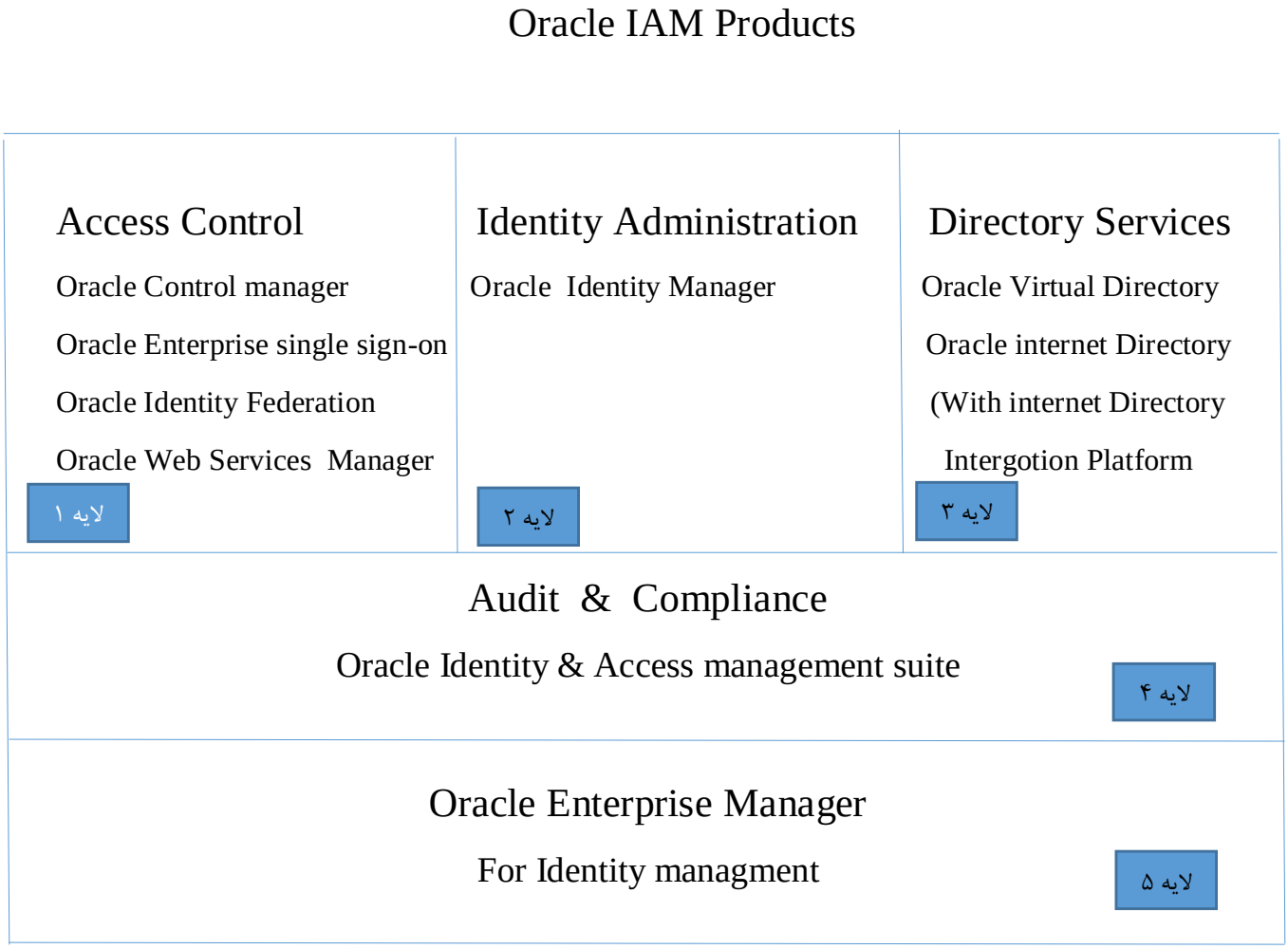
1- Oracle Identity Management
2- Enterprise User Security

Monitoring

1- Oracle Audit Vault
2- EM Configuration Pack

Data protection

1- Oracle Advance Security
2- Oracle Security Backup



در معماری Oracle ، سه قسمت کنترل دستیابی ، مدیریت شناسه ها و همچنین مدیریت خدمات به سرویس ها تعریف می شود در مدیریت خدمات سرویس ها ، مدیریت سرویس ها تعریف می شود. در مدیریت خدمات سرویس ها ، مدیریت سرویس های وب لیست LDAP و همچنین دسترسی وب سرویس ها تعریف می شود. این قسمت ناظر به اجرای سرویس ها و همچنین دستیابی به آن ها می باشد در مدیریت نشانه ها برای دستیابی به فایل و همچنین ذخیره سازی داده به فایل مدیریت هایی در نظر گرفته می شود.

در بخش Audit ممیزی دستیابی ها انجام می شود و ممیزی برای مدیریت نشان ها و فایل ها تعریف می شود.

در رمزنگاری معماری Oracle دو نوع رمزنگاری مطرح می شود؟

1-DBMS-Crypte

2-DBMS-OBFUSCATION-Tool

در این رمزگذاری ها الگوریتم های رمزنگاری شامل DES , 3DES , RC4 , DES-2Key

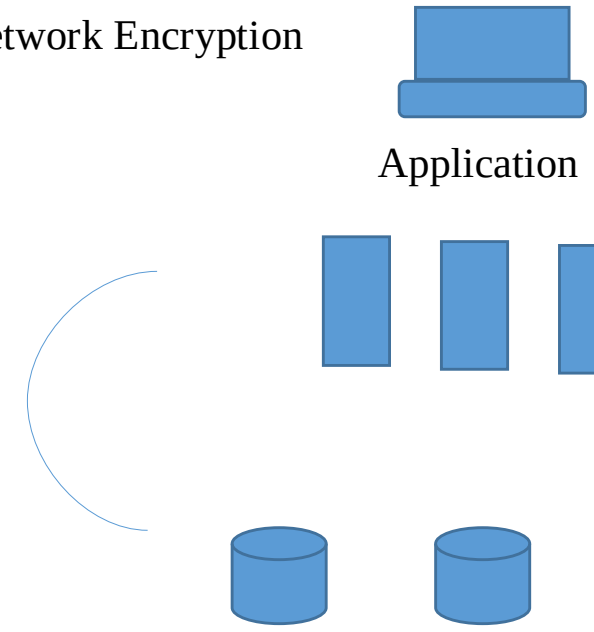
برای رشته ای خواندن Data و Black Sofery از رمزنگاری CBC , CFB , ECB استفاده می کند.در رمزنگاری Hash از رمزهای MD5 و SHA1 استفاده می کند. برای تولید رمز از اعداد تصادفی با رنج بالای Integer استفاده می کند.

تذکر: برای همه ارتباطات با Data Base رمزگذاری RC4 ، ۵۶ و ۲۵۶ بیتی استفاده می شود. و همچنین DES ، ۵۶ بیتی برای مبادله های دو کلید و ۳ کلید هست.

برای مبادلات کلیدها از استاندارد Diffie - Hellman استفاده می کند برای محافظت از جامعیت داده و تشخیص خطا و تصحیح خطا از رمزنگاری MD5 استفاده می کند. برای پیدا کردن Packege ها در شبکه و بازیافت آن ها از رمزگذاری MD5 و SHA1 استفاده می کند.

امکانات رمزگذاری شده در نسخه Oracle 10 :

Oracle Data Base 10g Release Transparent Data Encryption

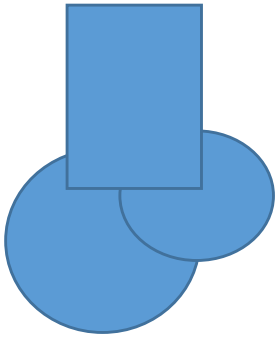


Transparent Encryption

*Includes Key management

*Transparent Application

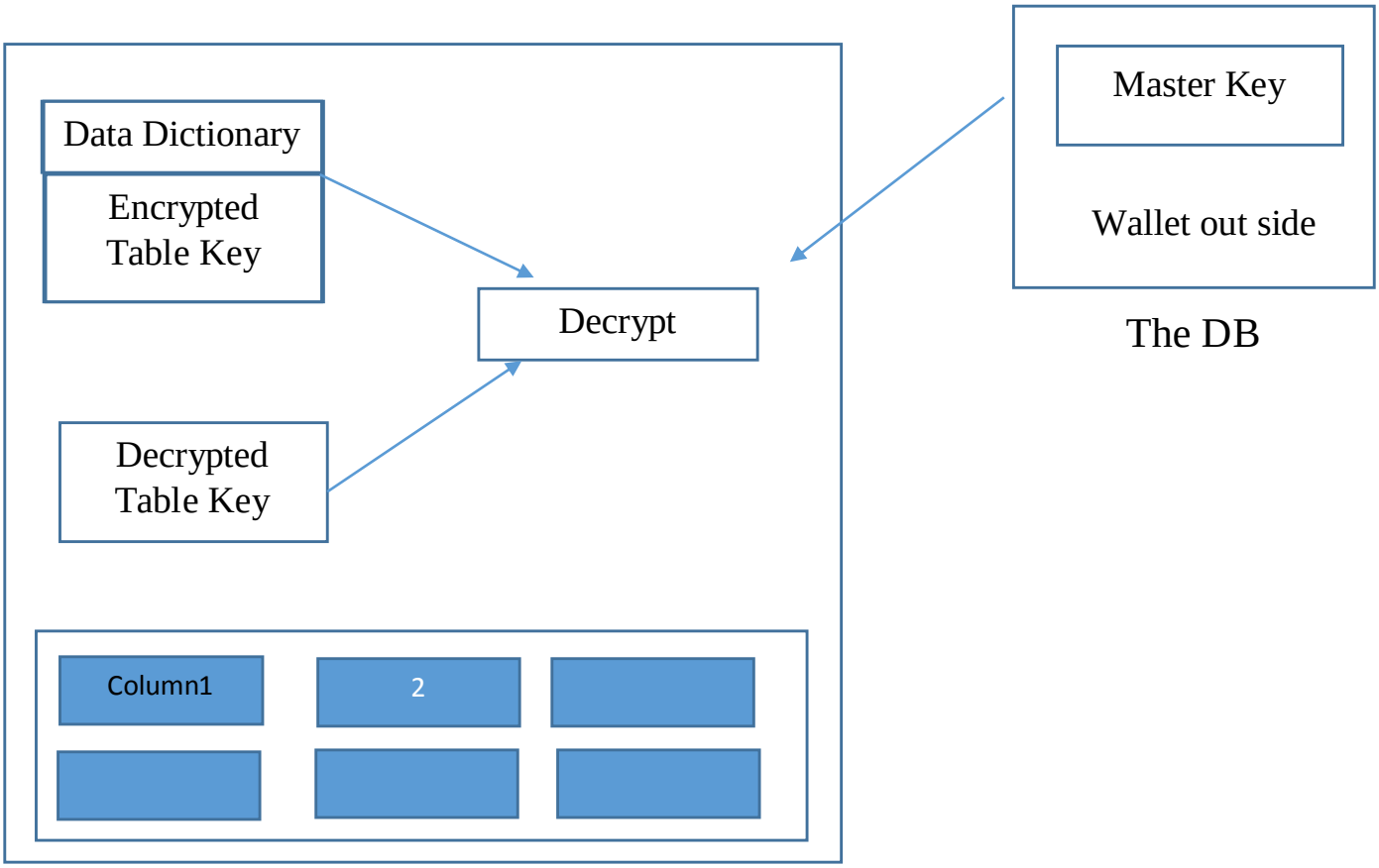
*Helps Address Privacy and Requlatory Compliance



Data Encryption On Backup Files

کلیدها قابلیت مدیریت و بصورت پویا است ، Transparent اضافه شده روی لایه Application ، آدرس محل ذخیره سازی در سمت DBMS است بخاطر همین قابل دسترسی نیست. با توجه به امکانات امنیتی 10g این Data Base در سطح Application نیز رمزگذاری متفاوت Data را داریم همچنین کلیدهای رمزنگاری قابل تغییر و قابل مدیریت هستند و آدرس Data Base و فایل های اصلی آن درون Data Base درون DBMS شخصی سازی و مخفی می گردد.

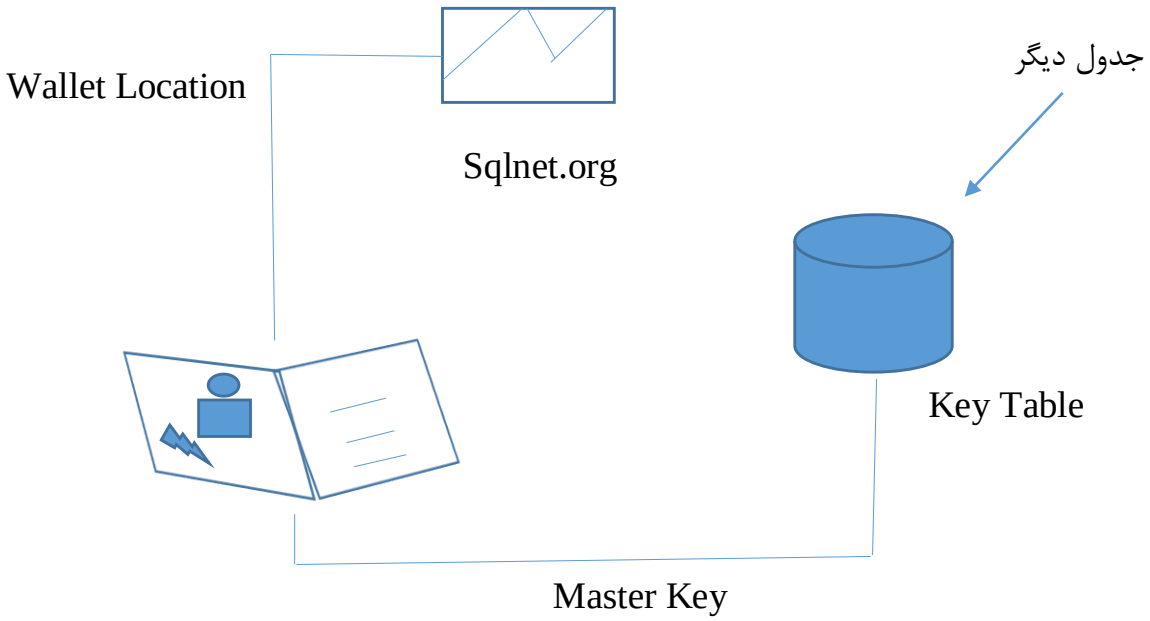
Transparent Data Encryption



در این شکل Master Key خارج از Data Base است برای رمزگشایی Table ها با کلیدی که در دیکشنری وجود دارد می توانید کلید رمزگشایی Table را باز کند و ستون های رمز شده را از رمز درآورد.

این روش Master Key در یک Data Base دیگر یا در یک Table ای در Data Base دیگر نگه داری می کند که به آن کیف یا Wallet گویند. عملکرد Wallet بصورت زیر است.

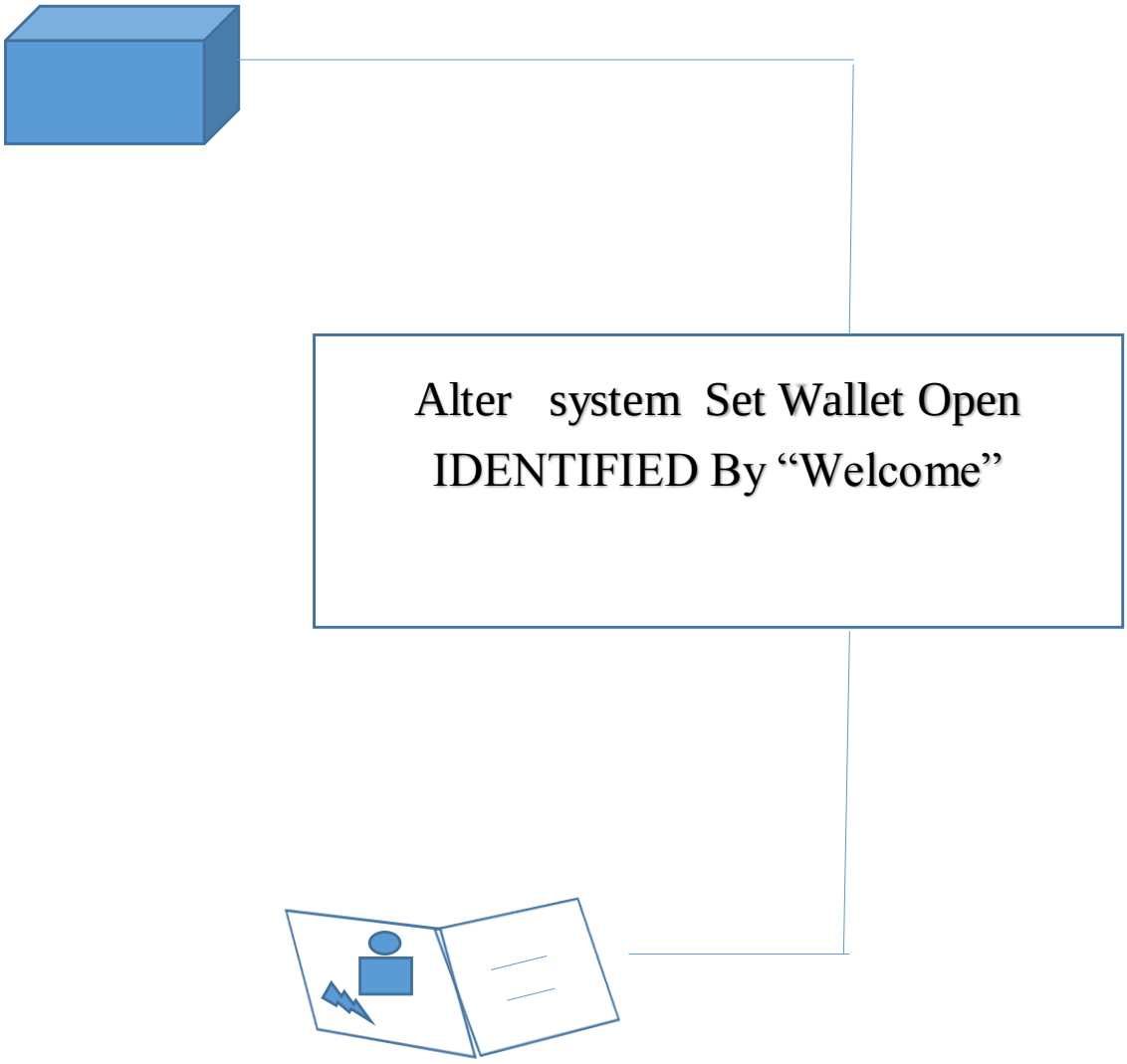
Create the Master Key



در این شکل Master Key درون جدول دیگر است و Wallet آن را می گیرد و در خود ذخیره می کند و امکان تغییر نیز دارد. Wallet خود نیز در جای دیگر می باشد.

طریقه استفاده از Wallet :

Open the Wallet



دستور فوق از دستور های SQL است و برای شناسایی Wallet جهت باز کردن رمز Data Base استفاده می شود.

چگونه می توان ستون های را در Data Base رمزگذاری کرد؟

فرض کنید می خواهیم یک Data Base برای ذخیره سازی اطلاعات مربوط به یک کارت اعتباری ایجاد کنیم. در ساخت جدول زیر شمارCreate Card رمز شده است.

```
Create Table cust-payment-info
( First name varchar2 (11) , Last name varchar2(10) , Order_Number
number(13) , Credit_Card_Number varchar2(30) , Encrypt No SALT);
```

چگونه می توانیم روی جدول هم رمز بگذاریم و هم پسورد؟

```
Create Table cust-payment-info
(……
        Credit_Card_Number varchar2(30)
        Encrypt User ‘AES 256’ IDENTIFIED By Password NO SALT
);
```

در رمزنگاری Oracle ، 10g امکانات زیر در نظر گرفته شده است و ورژن 9.I را کامل تر کرده است :

۱-دسترسی مستقیم به Index ها به ستون های رمز شده غیر ممکن است.

۲-Object های بزرگ مثل کل Data Base یا فیلدهایی که حجم زیادی دارند رمز نمی شوند.

۳-مسیر مستقیم برای دستیابی به بار گذار SQL تعریف شده است.

۴-Object های موجود Schema مربوط به کاربر SyS (Admin اصلی Data Base) رمزگذاری نمی شود.

۵-ابزار Data Base مثل مدیر وب سرورها و مدیر شبکه .... اجازه دستیابی به فایل های می توان داشته باشند.

اما در Oracle ، 10g گزینه های رمزگذاری بهینه تر شده به صورت زیر است؟

الف) کل Table را رمزگذاری می کند و محل استقراری آن ها

Table Pace Encryption

ب) Master Key می تواند در یک Device دیگر مثل USB , Token ، موبایل و غیره ذخیره سازی می شود.

Master Key Stored In HSM Device

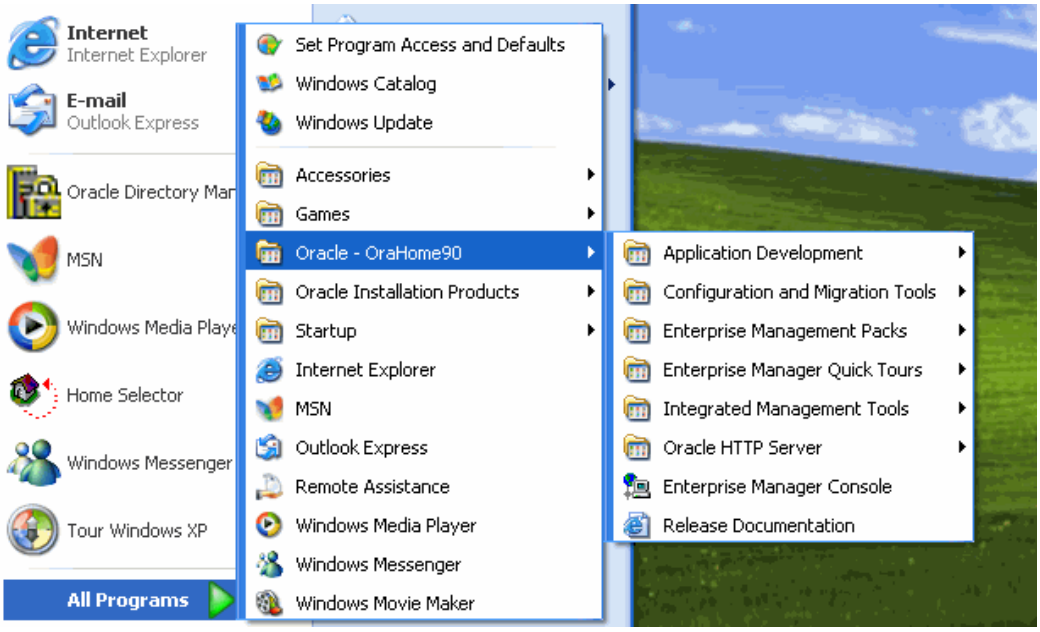
ج) امکان رمز گذاری Object های بزرگ در این ورژن Oracle وجود دارد.

Secure File LOB Encryption

Oracle

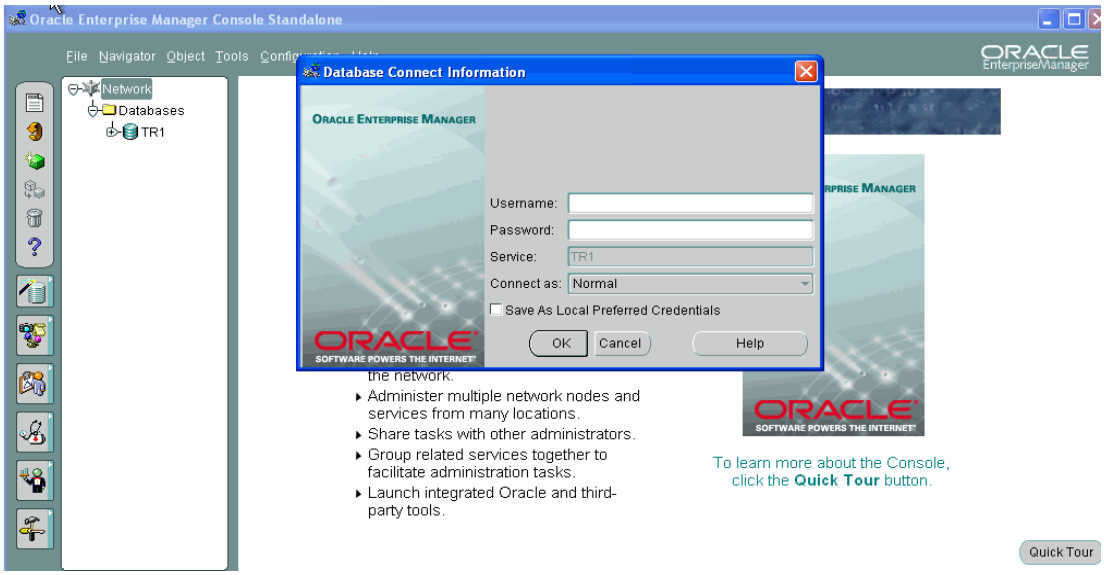
در بانک اطلاعاتی Oracle ما نصب و محل قرارگیری DBMS ، محل قرارگیری فایل اصلی ، تعریف کاربران Oracle ، نام اصلی بانک داریم و بعد از نصب مدیریت پیکربندی Oracle که در دو مرحله conf و running انجام می شود و مدیریت امنیت و برای هر کاربر را داریم مثل کاربر sys , system را داریم و برای هر کاربر یک رمز عبور قرار می دهیم که باید بیشتر از ۱۳ کارکتر باشد.

پس از نصب Oracle در زیر مجموعه Data Base تمام Data Base های ایجاد شده درون Repazitory است.

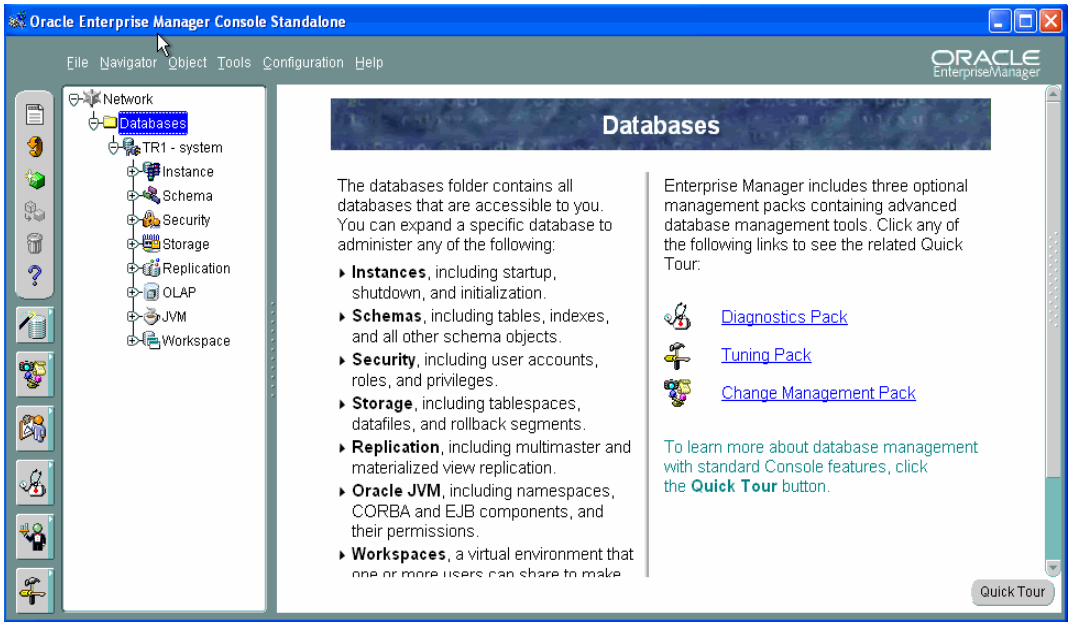


گزینه Enterprise Manager Console را انتخاب می کنیم.

OK را کلیک می کنیم.



وقتی صفحه برنامه باز شد در پنجره سمت چپ Data Base را می توانید می بینید و جدول که در هنگام نصب ساخته شده وجود دارد برای Connect به جدول روی آن کلیک راست کرده و گزینه Connect را زده و پنجره بالا ظاهر می شود که نام کاربری و پسورد را می خواهد که بصورت پیش فرض در هنگام نصب تعریف شد Username: system , Password: manager را وارد می کنیم که صفحه اصلی وارد می شویم.



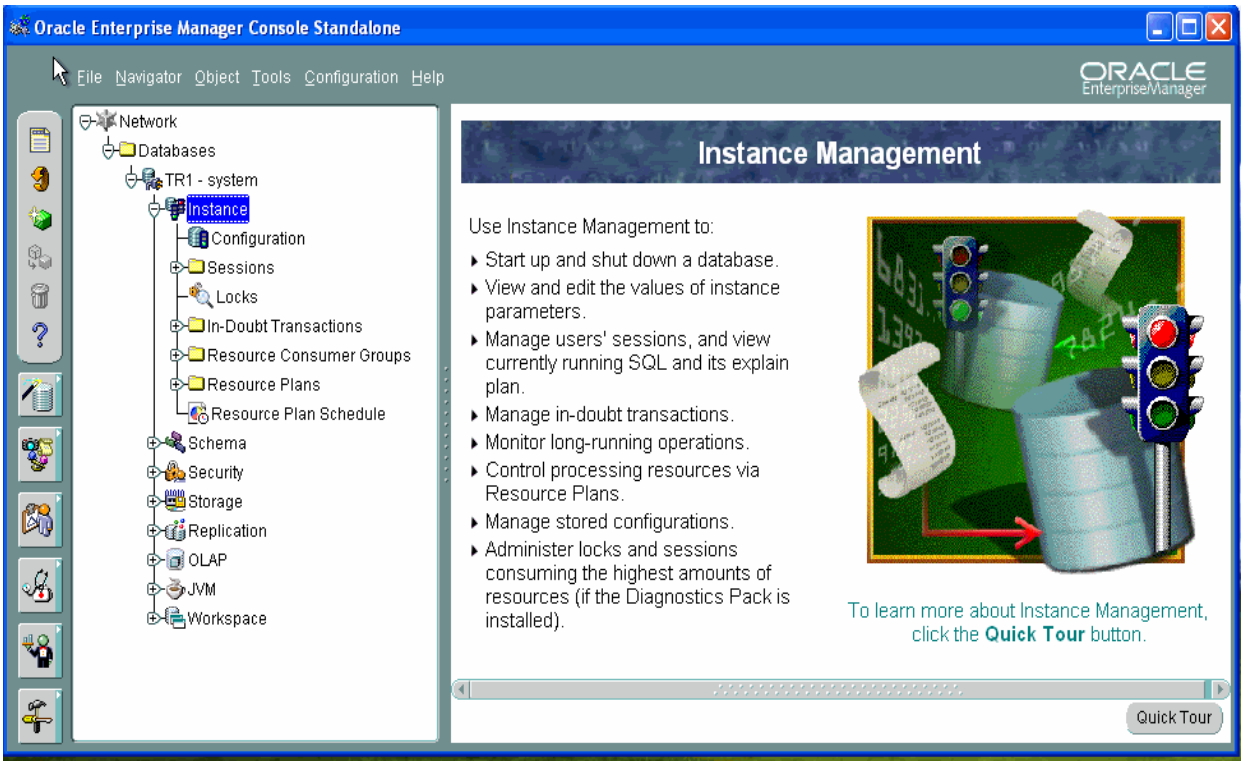
هر Repazitory شامل بخش های زیر است:

۱- Instance
۲- Schema
۳- Security
۴- Storage
۵- Replication
۶- OLAP
۷- JVM(java Virtual Machine)
۸- Workspace

وظایف هر بخش شامل :

1-Instance :

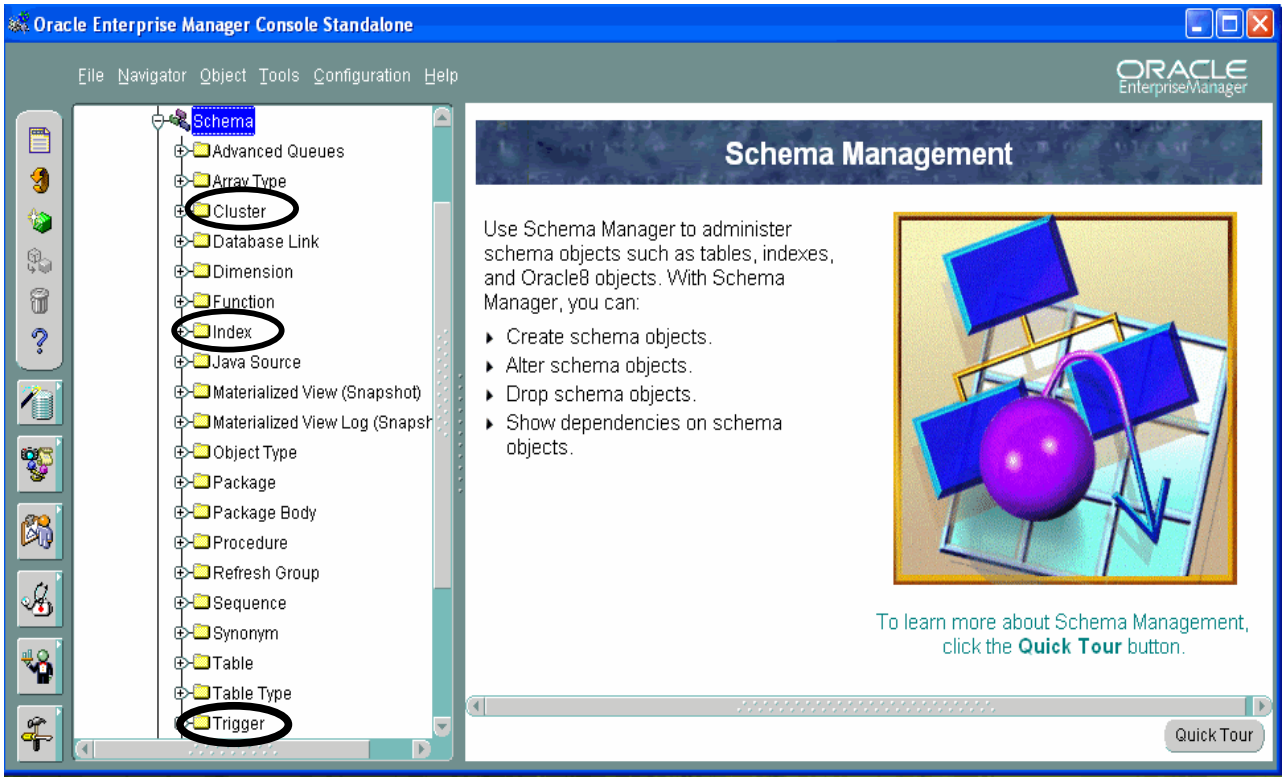
در این قسمت Instance وظایف خاموش و روشن کردن Data Base تعریف View ها و همچنین مدیریت را داریم.



در این بخش مدیریت دید کاربران و همچنین مدیریت تراکنش های در حال اجرا و Monitoring تراکنش ها و همچنین مدیریت پردازشی و همچنین Resource Plan برای منابع پردازشی و همچنین مدیریت Block کردن Session ها انجام می شود.

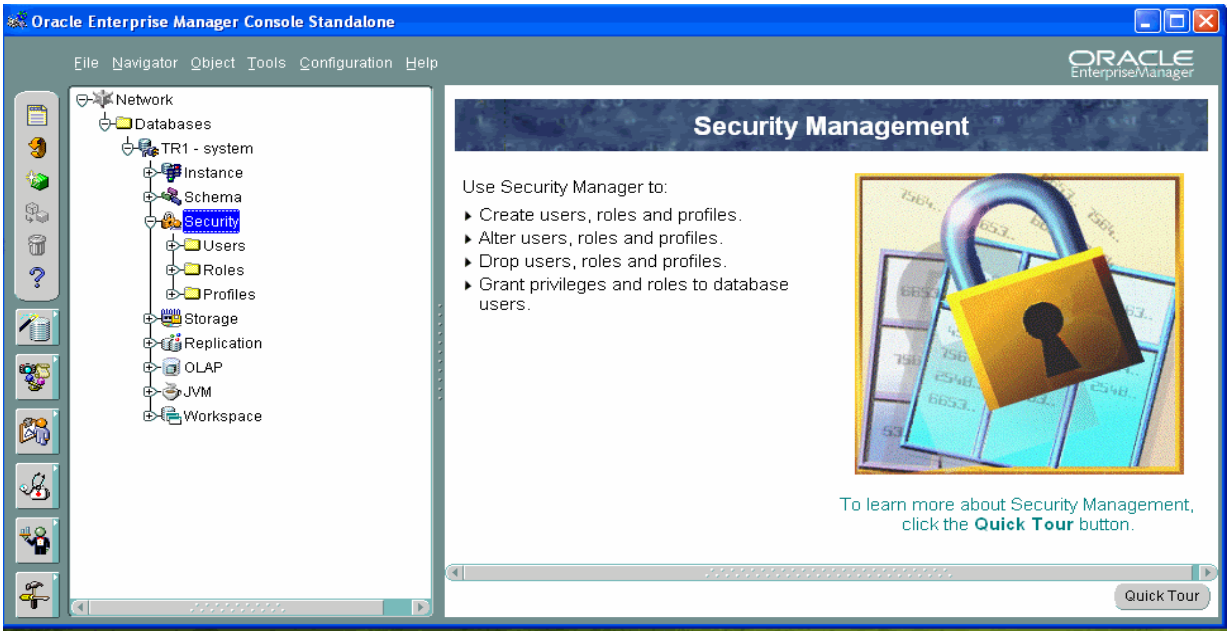
2-Schema:

در این بخش مدیریت object ها مانند جداول ، بخش های Cluster , Index , Trigger ها و همچنین مجوز دستیابی به آن ها و View روی آن ها تعریف می شود.



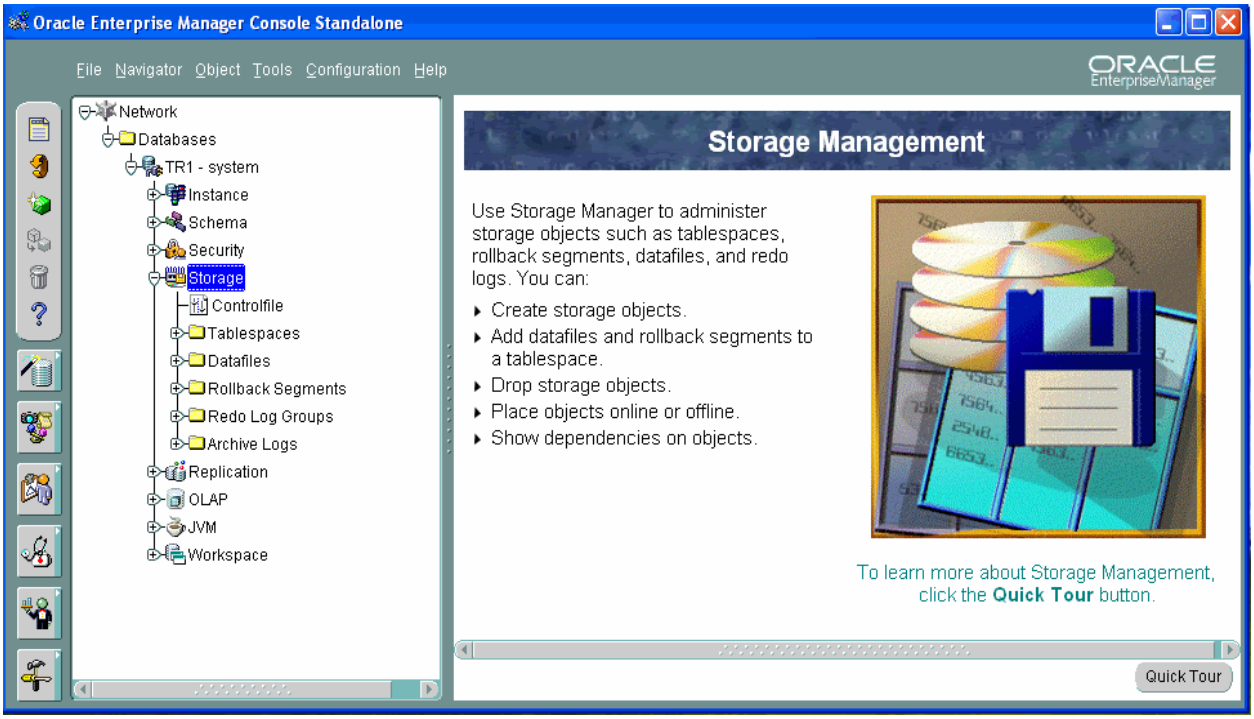
3-Security:

در این بخش سه قسمت برای امنیت تعریف می شود به ازای تک تک User ها Role تعریف می شود و به ازای Role ها ، Profiles تعریف می شود که هر Profiles می تواند به User های خاصی نسبت داده شود.



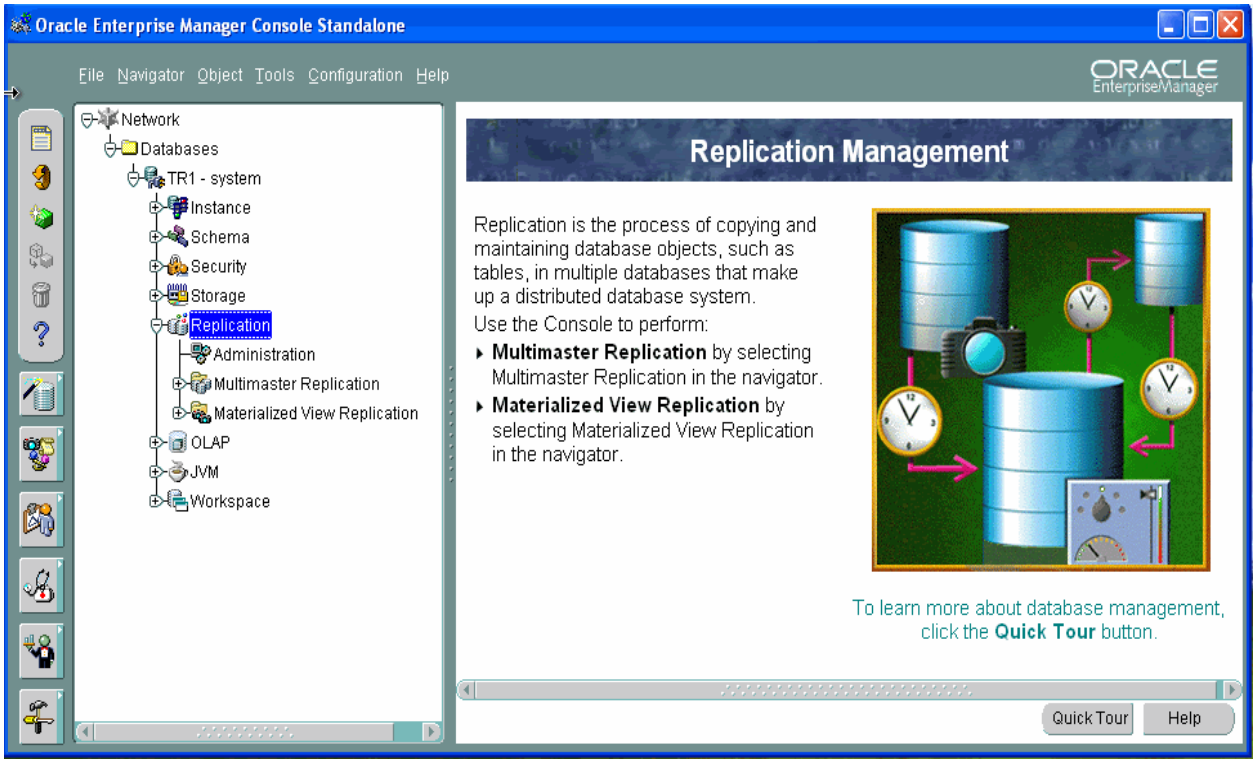
4-Storage:

در بخش Storage ، فایل های Control ذخیره می شود. Tablespaces ها و فضاهای مربوط به آن ها باید تغییر پیدا کند. Rolleback و Recovery در این قسمت تعریف می شود به ازای Control File ها Redo log Group و مدیریت Archive Logs ها انجام می شود.



5-Replication:

یا کپی برداری نام دارد کع عملیات کپی Main Transe نگه داری Data Base را انجام می دهد. توزیع پذیری Data Base و Multi master Replication کپی چندگانه روی سرور در این قسمت انجام شود.



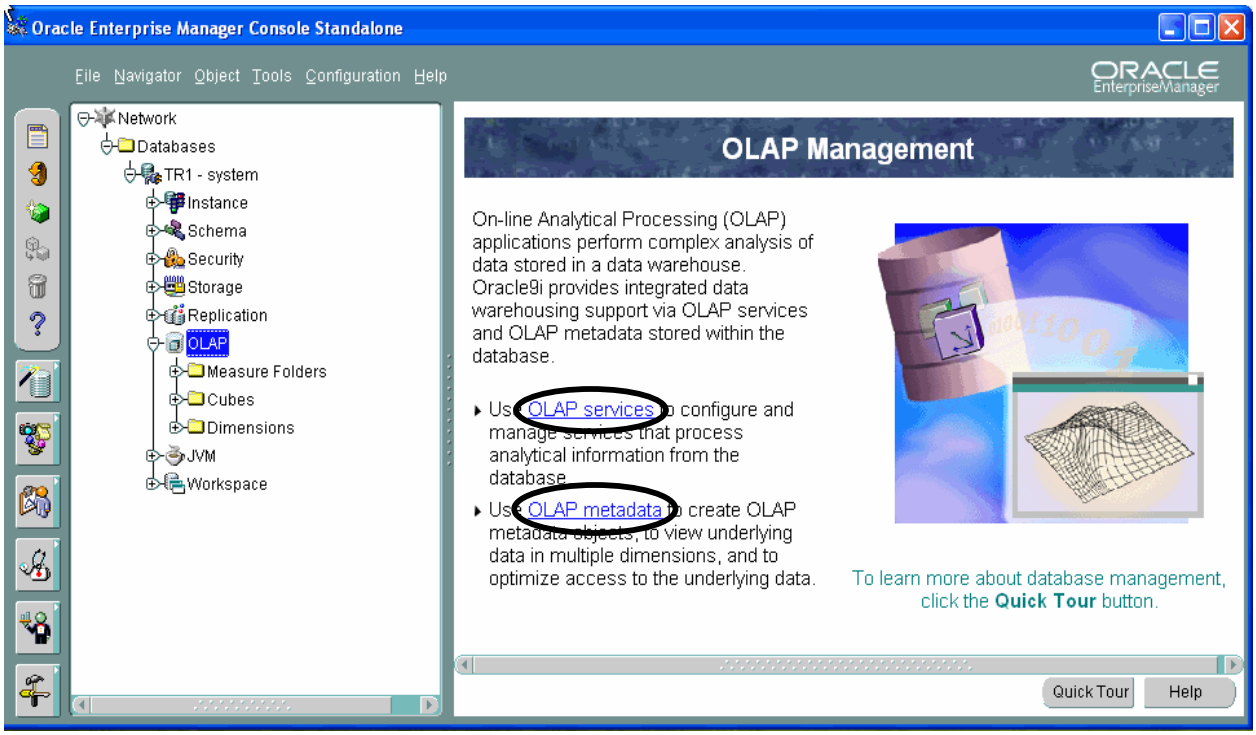
6-OLAP:

در این بخش Data Base را برای آنالیز چند پردازشی و مدیریت Wave house آماده سازی کنیم.

در OLAP به دو قسمت تقسیم می شود:

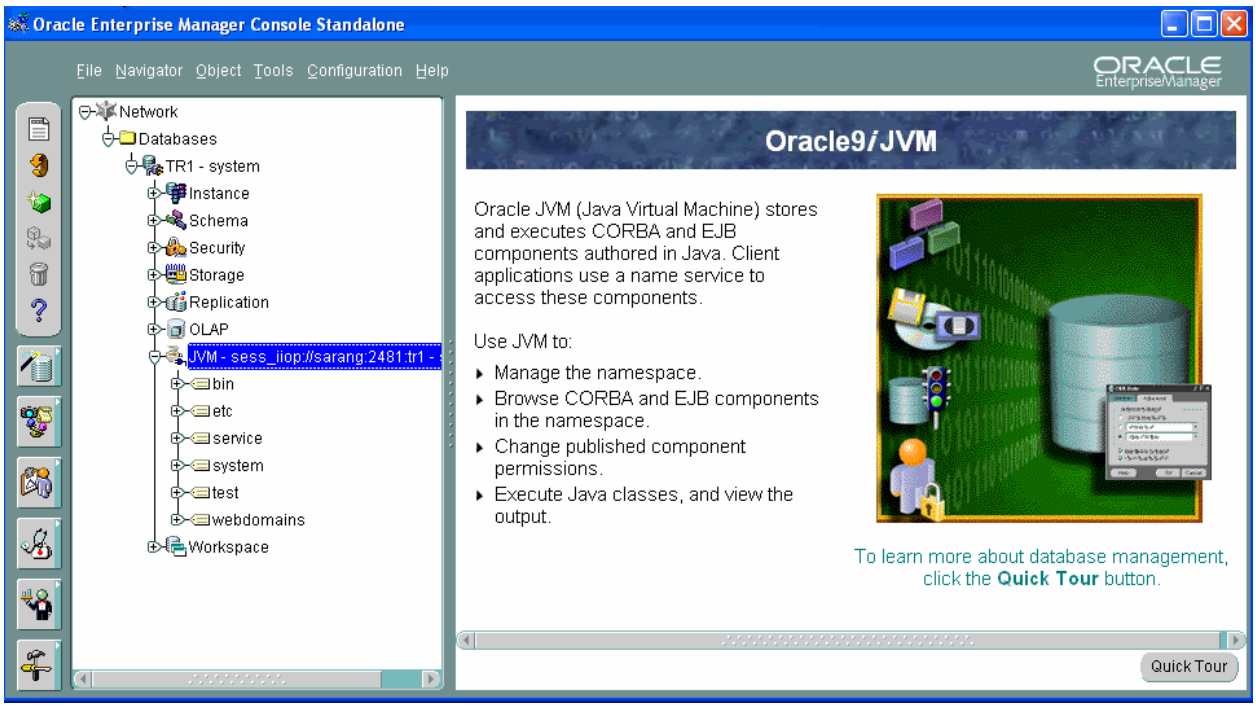
۱-سرویس های مربوط به پردازش

۲-Meta Data



7-JVM:

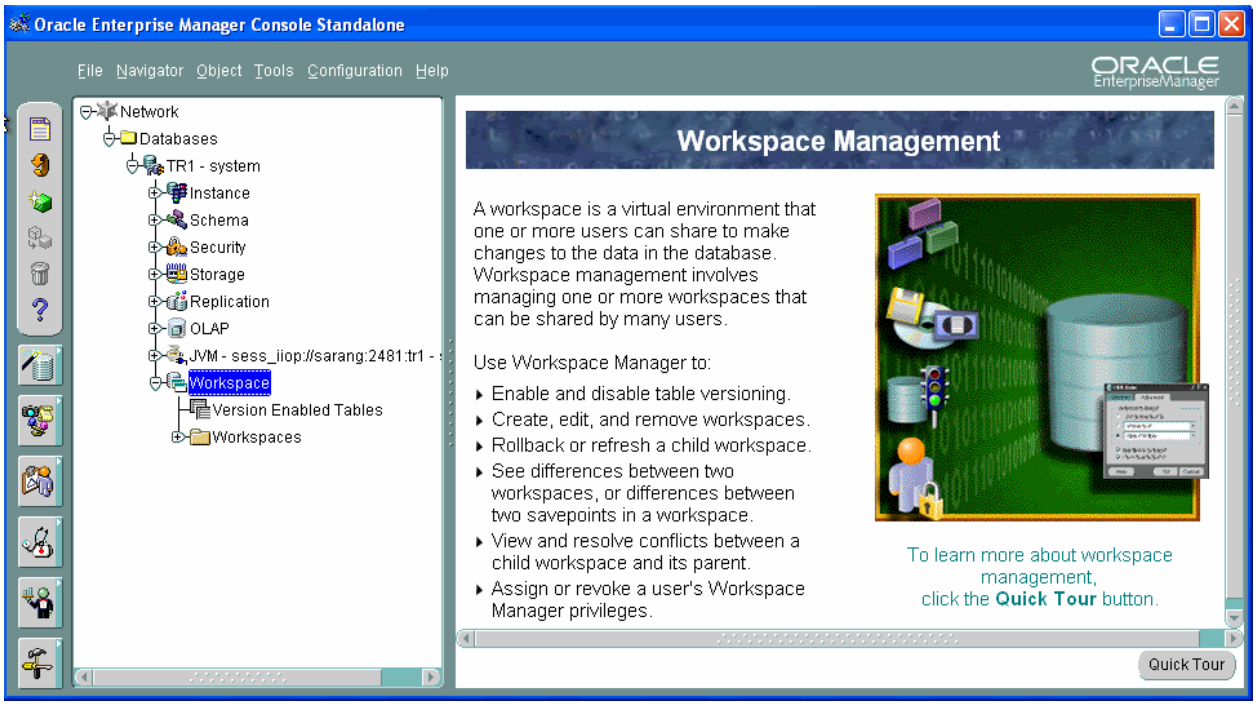
این قسمت به برنامه هایی مثل java و C# کمک می کند تا Component ها و همچنین استانداردهای مثل EJB , JDBC , Spring را مدیریت کند.



8-WorkSpace:

در این قسمت java Virtual Machine تعریف می شود. اجرای Tablespaces روی فضای کاری کاربران در این قسمت تعریف می شود.

Data Base های سلسله مراتبی در این قسمت تعریف می شود و می توانیم به کاربران اجازه دسترسی سلسه مراتبی نیز بدهیم.



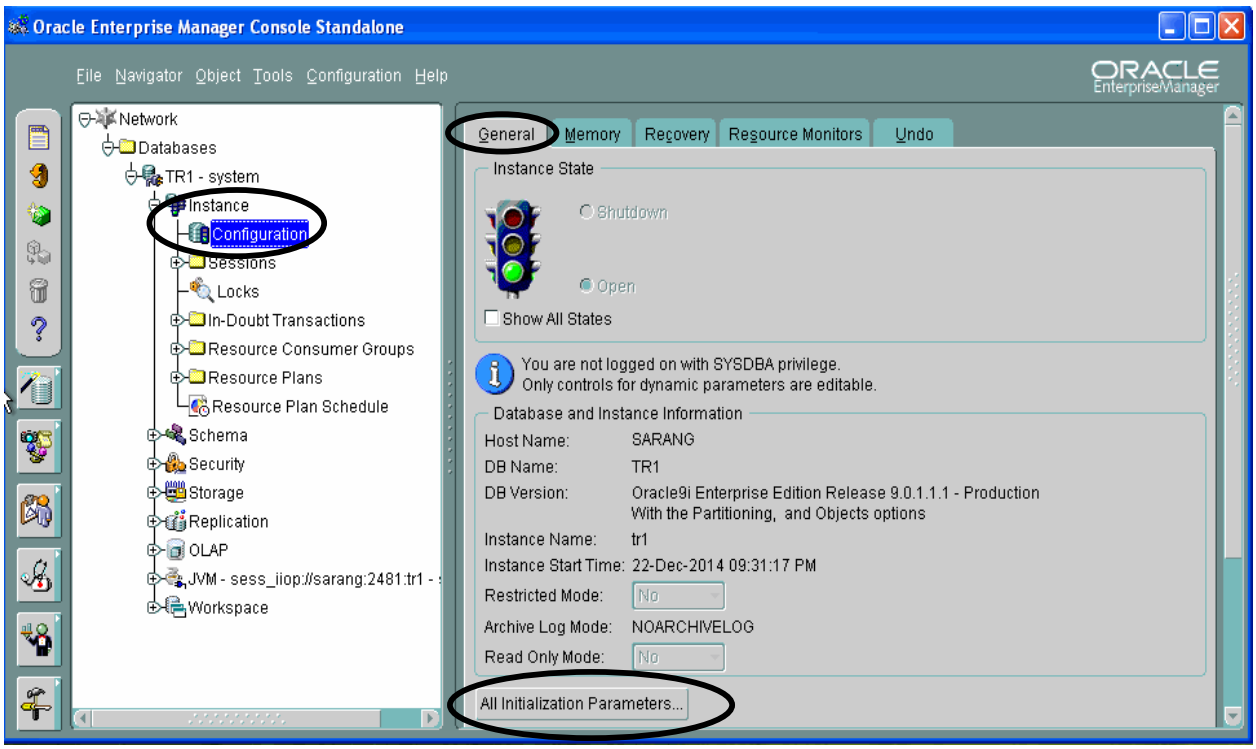
آدرس زیر

Instance ⟶ Configuration

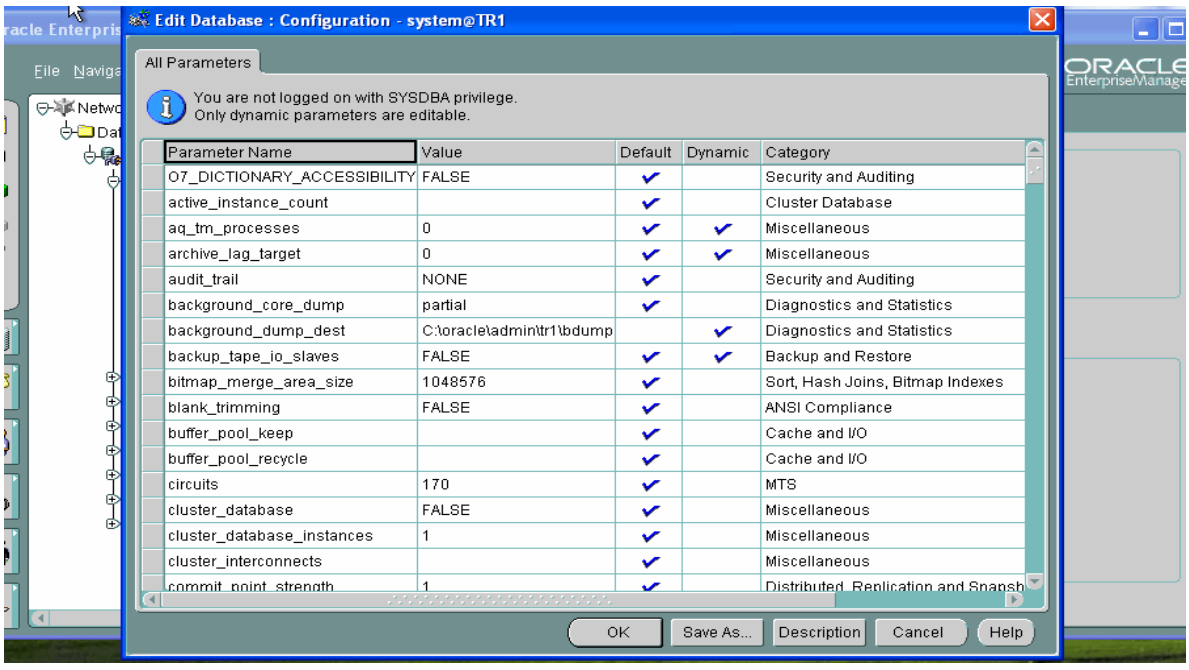
General ⟵ Tab از

دکمه

All Initialization Parameters را کلیک می کنیم .



در پنجره باز شده که در این قسمت نمی گذارد کاربر به Dictionary دسترسی داشته باشد که در حالت پیش فرض False است.



Parameter Name:

1- Dictionary_Accessibilty :

این قسمت کمک می کند تا Privilege یا حق دسترسی user به Data Dictionary تعریف می شود. اگر False باشد user فقط به Object های schema دسترسی دارد.

2-Active_ Instance_Count :

در این قسمت به تعداد Instance ها از Data Base ها در هنگام ایجاد cluster کار دارد و هر چقدر Data Base روی سرورها یا در روی cluster پخش شود در مقابل این قسمت شماره تعداد می خورد.

3-aq_tm_processes :

این بخش مشخص کننده Monitoring است و اگر مقدار آن صفر باشد یعنی صفحه پیامی نداریم و اگر مقدار آن بیشتر از صفر باشد صفحه پیامی برای Monitoring پردازش ها بوجود می آید.

4-Archive_log_target :

در این قسمت می توانیم رشته های پردازشی را مشخص کنیم که در چه زمانی اجرا می شود. مقدار صفر برای این قسمت برای این است که زمان اجرای رشته های پردازش بصورت پیش فرض توسط سیستم عامل تعریف می شود و مقدار ۶۰ تا ۷۲۰۰ میلی ثانیه برای مدیریت Oracle در نظر گرفته شده است.

5-audit_trail :

در این قسمت تعریف می کنیم که آیا SYS AUD قابلیت نوشتن داشته باشد یا خیر که چهار حالت برای آن در نظر گرفته می شود:

1-False 2-True 3-None 4- OS

که در حالت پیش فرض None یعنی ممیزی امنیتی Data Base را بر می دارد.

6-background_core_dump :

7- background_dump_dest :

این گزینه باعث می شود تا از هسته مرکزی Data Base و اطلاعات موجود در آن dump گرفته شود که یا بصورت Full یا Partial است. اگر Data Base در حالت run یا اجرا باشد و در سیستم عامل ویندوز باشیم این عمل بصورت Partial می شود. اگر در سیستم عامل Unix باشیم عمل dump بصورت Full انجام می شود و در حالت های Wave house عمل dump بصورت Full انجام می شود.

محل قرار گیری dump نیز باید تغییر پیدا کند و در آدرس Admin نیامده باشد.

این dump با سرورهای Unix در Cash سرور و درPartion SWP آدرس دهی می شود.

8-backup_tape_io_slaves :

می تواند False یا True باشدعلاوه بر دیسک روی یک Tab دیگر ذخیره را انجام می دهد.

9-bitmap_meger_area_size :

این قسمت یکی از مهم ترین بخش های Index , Cash Index می باشد. برای اینکه بتوانیم عملیات جستجو و مرتب سازی را به کمک Index ترتیبی سرعت بخشیم از این قسمت استفاده می کنیم بصورت پیش فرض 1 MG می باشد.

10-blank_trimming :

در این قسمت مقداری به Data نسبت داده می شود تا طول رشته های پردازشی Data در صورت اضافه شدن event یا رخداد برای آن Data دچار شکست Buffer یا شکست حجمی نشود. مقدار پیش فرض False است.

11-buffer_pool_keep :

در این قسمت حجم Buffer برای Block های Data در نظر گرفته می شود تا یک رشته از Block ها بتواند عملیات I/O را کاهش دهد که این عمل به عنوان Buffer ورودی و خروجی تعریف می شود.

12-buffer_pool_recycle :

این قسمت نیز تعریف Buffer حالت قبل از با این تفاوت که حافظه اصلی سرور را در عملیات I/O کمک می کند. این رشته برای تعریف Rang حافظه RAM می باشد.

دو مورد بالا عملیات cash را انجام می دهند.

13-Global_names :

این قسمت جهت تعریف نام کلی Data Base می باشد. از Distributed برای مدیریت نام Data Base جهت دستیابی به پردازش های CPU موجود در سیستم های توسعه یافته می باشد. مقدار اولیه این پارامتر false است و در حالت Distributed مقدار آن را به True تغییر می دهیم.

14-hash_area_size :

این گزینه برای تعریف مقدار فضای bitmap index جهت جستجوی سریع Data Base در Oracle می باشد. به صورت پیش فرض مقدار آن ۱۰۴۸۵۷۶ می باشد که فضای مرتب سازی را برای الگوریتم Quick sort , merge sort فراهم می کند این فضا برای پیوستن یا join قسمت های ادغام در الگوریتم استفاده می شود و در رمزگذاری داده های موجود در الگوریتم و محیط بانک و شرایط پیوند جداول نیز در نظر گرفته می شود . برای فضای و کنترل نوسانات حافظه آن گزینه hash_join _enabled وجود دارد که با آن می توانیم با گذاشتن گزینه True در مقدار دهی اولیه بانک فضا برای الگوریتم sort آماده کنیم. این دو مقدار برای جلوگیری از حملات Buffer و سرویس استفاده می شود و بنا به کشش CPU و RAM می توانیم مقدار آن ها را تغییر دهیم.

15-hi_shared_memory_address :

این گزینه با مقدار پیش فرض صفر برای حالت اجرا یا run time فضایی را از system_global_area می گیرد و آن را برای عملیات آدرس دهی RAM برای جداول به اشتراک گذاشته شده یا Data Base های به اشتراک گذاشته شده اجرا می کند و مقدار دهی این گزینه با صفر مشخص می شود که هنوز Data Base در حالت shared یا distribution قرار ندارد و در حالت اجرا ۶۴ بیتی بهتر است.

16-hs_autoregister :

این گزینه به حالت Distributed , Replication کمک می کند تا Data Base به کمک تعریف یک سیستم متجانس (همگونی) خود را روی Data Base دیکشنری موجود سوار کند.

مثلا وقتی Data Base کپی برداری می شود یا در یک محل دیگری روی distribution توزیع می شود. باید قابلیت شناخت و همگونی Data distribution مقدار پیش فرض آن در حالت نصب true است چه single باشد چه multi باشد. اگر مقدار false را انتخاب کنیم آنگاه عمل Replication را نمی توان انجام داد.

17-Instance_groups :

این بخش برای تولید Data Base روی بستر clustering است و به کمک آن می توانیم Data Base را روی چنین CPU از کامپیوترهای مختلف بالا بیاوریم و بخشی از فضای CPU آنها را در اختیار CPU سرور جهت کار Data Base قرار می دهیم. و مقدار پیش فرض آن null است.

18-Instance_name :

اسم جدول بصورت پیش فرض درج می شود.

در واقع نام واحدی است برای نام Data Base یا همان SID ، Data Base است در حالت clustering می تواند نام Data Base های cluster نیز باشد.

19-Instance_number :

مقدار پیش فرض آن برابر صفر است. مقداری است که به عنوان واحد یا unic برای تعداد نمونه های Data Base تعریف می شود. که اگر مقدار آن صفر باشد حتما باید دو مقدار قبلی آن نیز برای clustering تعریف شده باشد.

دو تای بالایی جزء زیر مجموعه Instance_groups است.

این سه بخش وقتی تعریف می شوند و clustering اجرا می شود باید نامی را که به عنوان SID می گذارید معمولا پیش فرض نباشد.

20-Java_max_sessionspace_size :

به صورت پیش فرض مقدارش همیشه برابر صفر است این مقدار یکی از مقادیر مهم در تعریف به کارگیری حافظه و ماکزیمم حافظه اختصاصی بر حسب بایت در پردازش Session می باشد و قابل دسترسی به برنامه ها یا Application های javaیی می دهد که روی سرور می خواهند از فضای حافظه تعریف شده استفاده کنند. مقدار پیش فرض این گزینه صفر است ولی اگر بخواهیم روی سرور پردازش های سنگین انجام دهیم و دستیابی به Application ها را تحت وب یا تحت LAN به Data Base سرعت ببخشیم از این گزینه استفاده می کنیم و آنرا مقدار بزرگتر از صفر می دهیم این مقدار بار CPU را زیاد می کند و به کشش CPU بستگی دارد.

21-Java_pool_size :

این قسمت مربوط به Cash JVM , Cash JDBC می شود. مقدار پیش فرض این فضا حدود سه مگ از RAM می شود این فضا را بصورت پیش فرض سیستم عامل مدیریت می کند و مقدار دهی می نماید برای تغییر دادن مقدار آن نیز باید به کشش سیستم عامل CPU و RAM دقت کرد چون روی آن حملات Buffer ی می تواند انجام شود.

22-Java_soft_sessionspace-limit:

این بخش مربوط می شود به پردازش های سیستم و بر حسب بایت برای تعریف Session کاربران حافظه ای اشغال می کند تا برنامه کاربردی بر روی DBM و GDBS می تواند مستقر شود. jbm برای این فضا و نوشتن و خواندن اطلاعات در این فضا فایل LOG یبه نام Trace file ایجاد می کند . مقدار پیش فرض آن صفر است و تا ۴ گیگ می تواند برای آن در نظر گرفت.

23-job_queue_processes :

این قسمت محیطی است برای در نظر گرفتن صف پردازش و جم بندی درخواست های پردازش از هر Instance در هر Data Base که به کمک DBMS job مدیریت می شود. مقدار پیش فرض صفر است و تا 36 job می توان در صف پردازش قرار داد از مواردی که خطرات حمله Buffer و Cash به آن راحت انجام می شود.

24-large_pool_size :

این قسمت کمک می کند به job_queue که فضای Buffer مربوط به آن را مشخص می کند این قسمت فضای shared روی سرورها را مشخص می کند عملیات Backup و RMAN را برای بازگرداندن Data مدیریت می کند. I/O ، Buffer و دیسک را مدیریت و سامان دهی می کند و بین ۶۰۰ کیلو بایت تا دو گیگا بایت می تواند حافظه pool تعریف کند. که بستگی به سیستم عامل سرور دارد که مقدارDBWR_IO_SlAVES تعریف شده باشد و پیکر بندی شده باشد می تواند مقدار ۱۰۴۸۵۷۶ صفر دهیم.

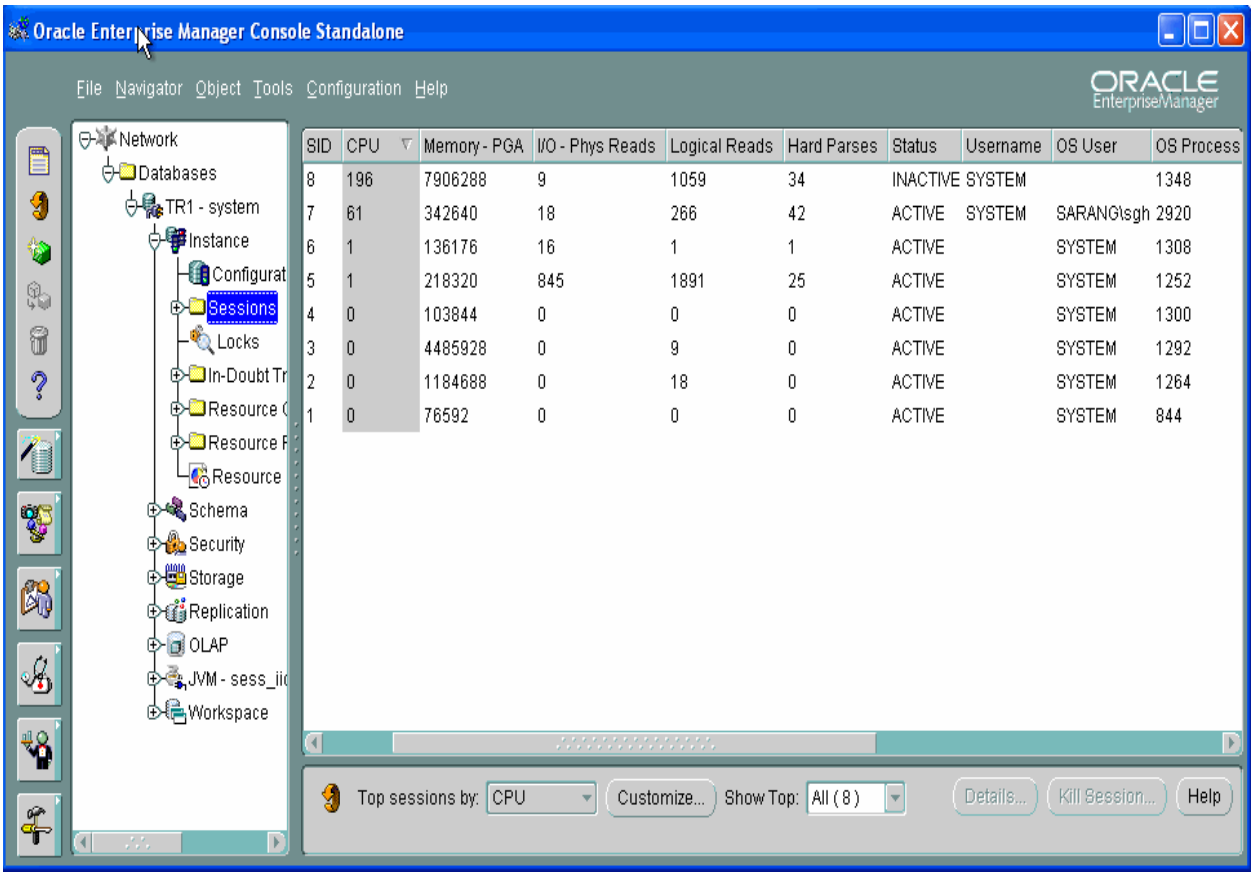
محدودیت های اجرایی :

Instance :

1- Instance_Max_ Session
2- Instance_Max_Users
3- Instance_ Session_warning

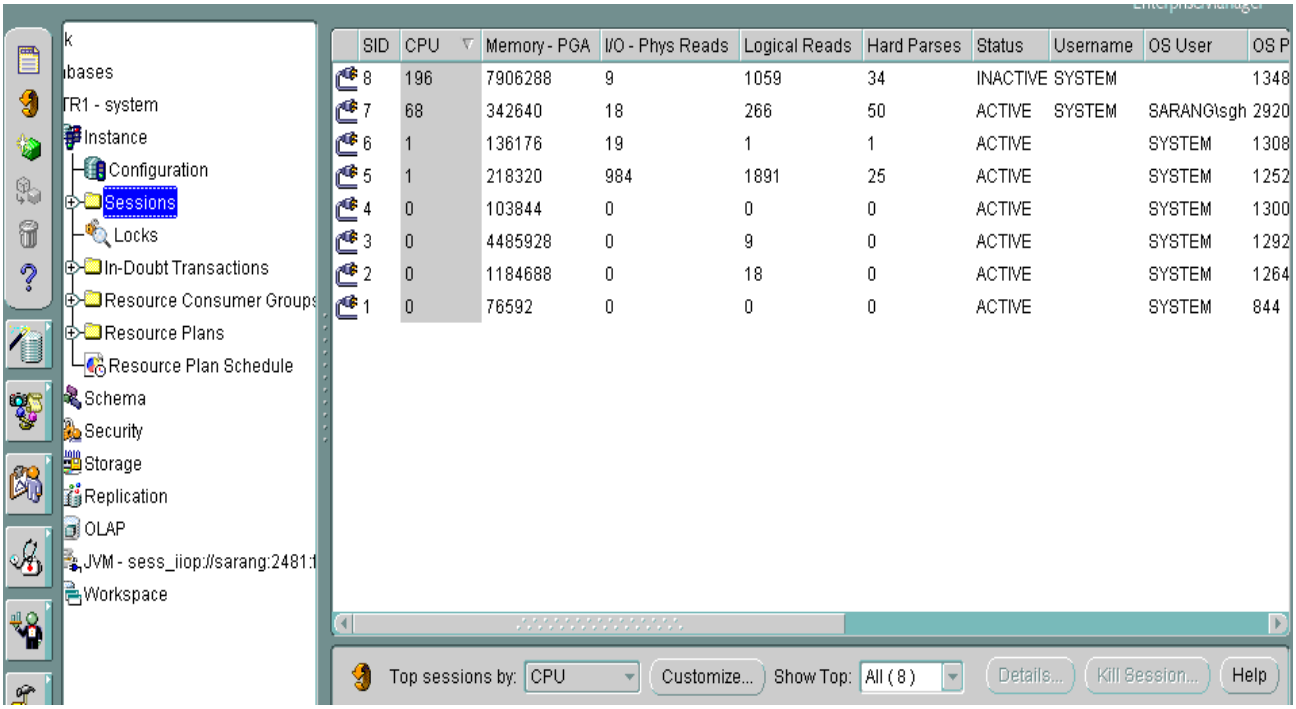
این سه گزینه مربوط به گزینه های محدودیت های License ایی است. اولی تعریف ماکزیمم تعداد کاربران همزمان که به صورت یک زمان و یک دست با هم در حال اجرای درخواست هایی هستند و CPU و سرویس های Data Base به آنها پاسخ می دهد. این قسمت شامل مجوزهای دستیابی و هم چنین اجراهای مختلف کاربران به صورت همزمان روی سطح سرور می شوند. مقدار پیش فرض آن صفر است و بسته به نوع Instance می توان مقدار را افزایش داد. قسمت دوم تعداد کاربران مجاز برای Session های تعریف شده را مشخص می کند مقدار این پارامتر با بالایی یکی باید باشد و پیش فرض آن نیز صفر است. قسمت سوم تعریف اخطار یا خطا برای محدودیت Session های کاربران است.

تعریف Session در سیستم Oracle :



در این سیستم در قسمت Session می توانیم Session های باز یا بخش هایی را که در حال اجرا Oracle هست ببینیم . در این بخش میزان مصرف CPU برای هر Session ، Meory-Rang یا PGA برای هر بخش تعریف می شود.

در این قسمت می توانیم هر Session را مدیریت کنیم و تعداد آدرس های فیزیکی خوانده شده را ببینیم با دابل کلیک روی هر Session اندازه ویژگی ها و همچنین مشخصه های Session نمایش داده می شود. در Session ها تعریف Memory , CPU و IP بصورت Manual دستی نیز تعریف می شود.



Resource Consumer Groups

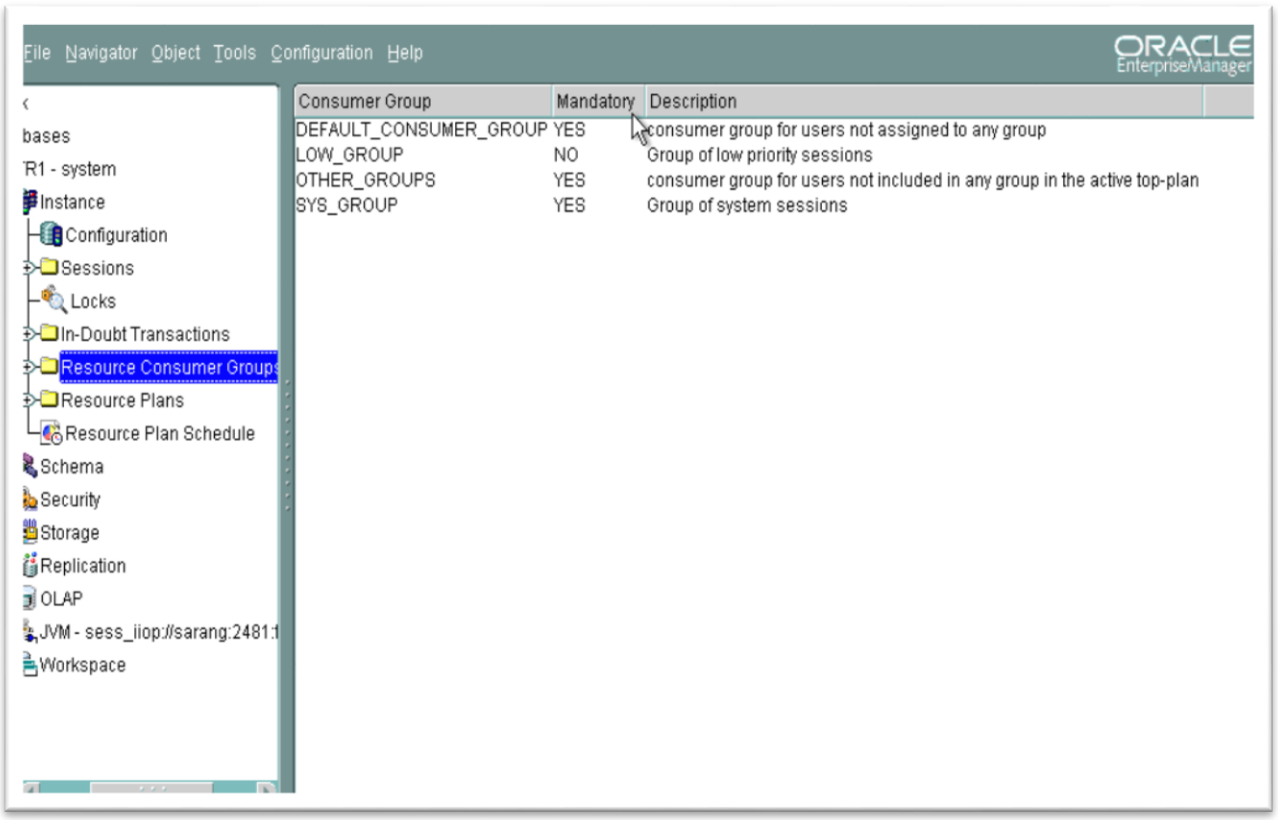
دراین قسمت ۴ دسته تعریف می شود:

1-Default Consumer Groups

2-Low- Groups

3-Other Groups

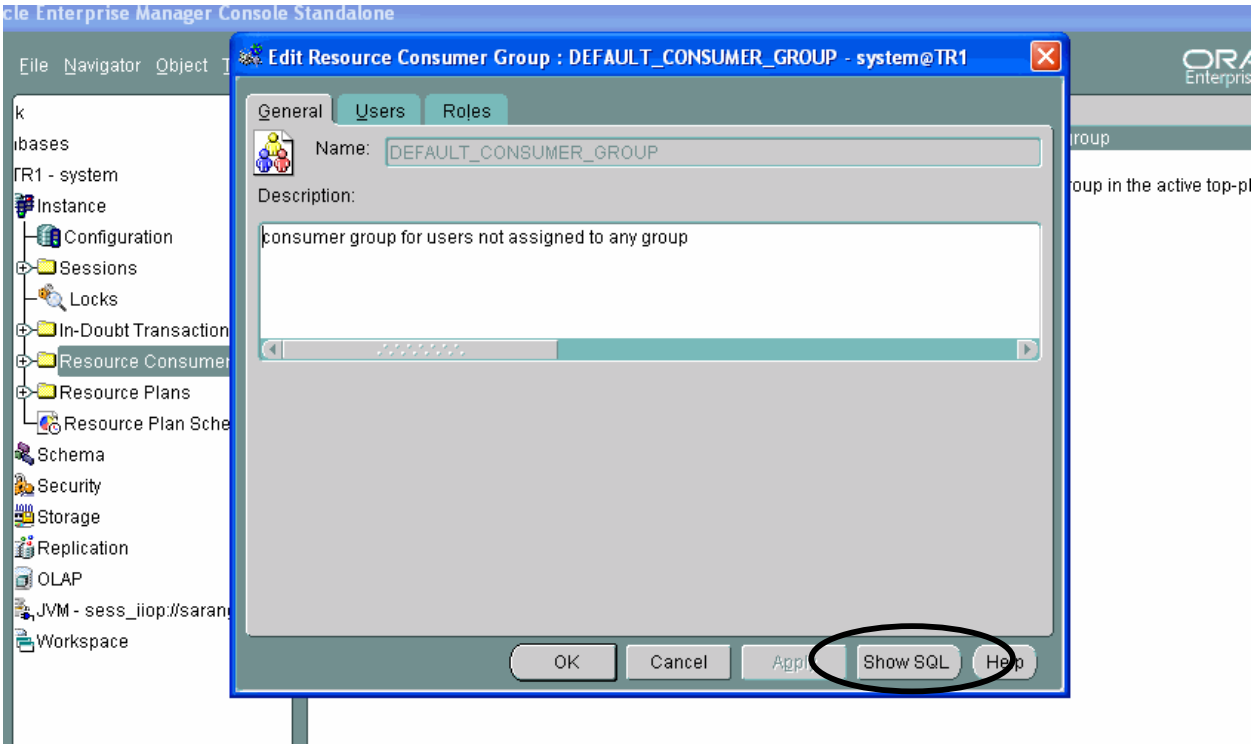
4-SYS Groups



1-Default Consumer Groups :

این گروه ، گروه یا استفاده کننده خاصی را مشخص نمی کند و به کسی نسبت داده نمی شود و دسته استفاده کنندگان آن می تواند شامل همه گروه های تعریف شده در Data Base باشد که در قسمت Users آن را در پنجره ویژگی های آن می بینیم.

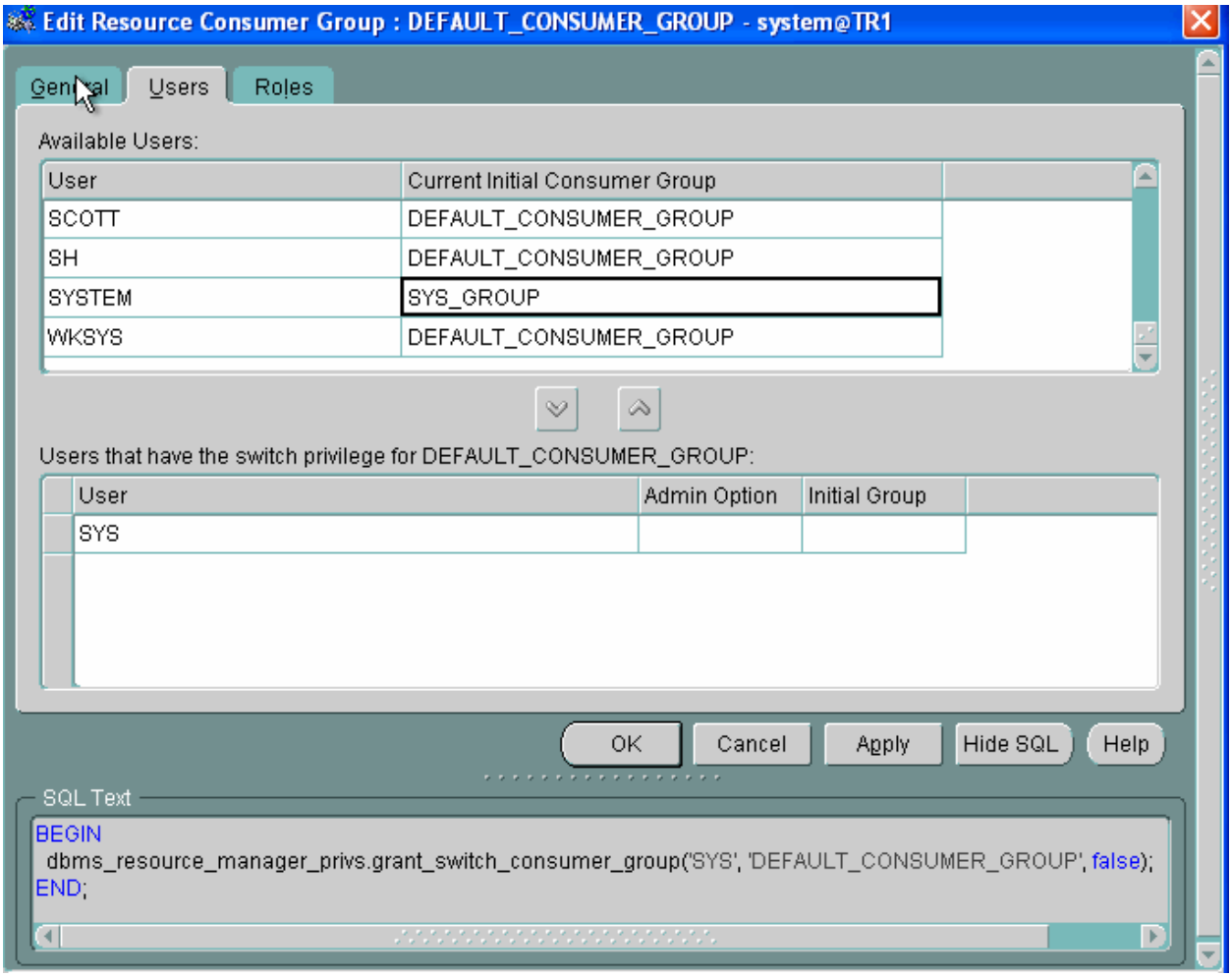
با دابل کلیک روی Default Consumer سه Tab وجود خواهد داشت.



Tab اول آن General که User Description ها است.

Tab دوم لیست User های قابل دسترس برای اضافه کردن موجود است.

Tab سوم انتخاب User های موجود به لیست User های مجوز داده شده Privilege دار در قسمت Default است. همه این کار به کمک دستور SQL انجام می شود و با زدن دکمه Show SQL می توانیم User مربوط به لیست User های Default وارد کنیم.



2-Low- Groups :

مانند قبلی است با این تفاوت که در درجه ای اولویت پایین تر نسبت به کاربران تعریف شده و در گروه های دیگر قرار دارد. اگر کاربری را به لیست Low- Groups وارد کنیم Low- Groups در آن صورت می توانیم Privilege های متفاوتی را در این بخش تعریف کنیم.

3-Other Groups :

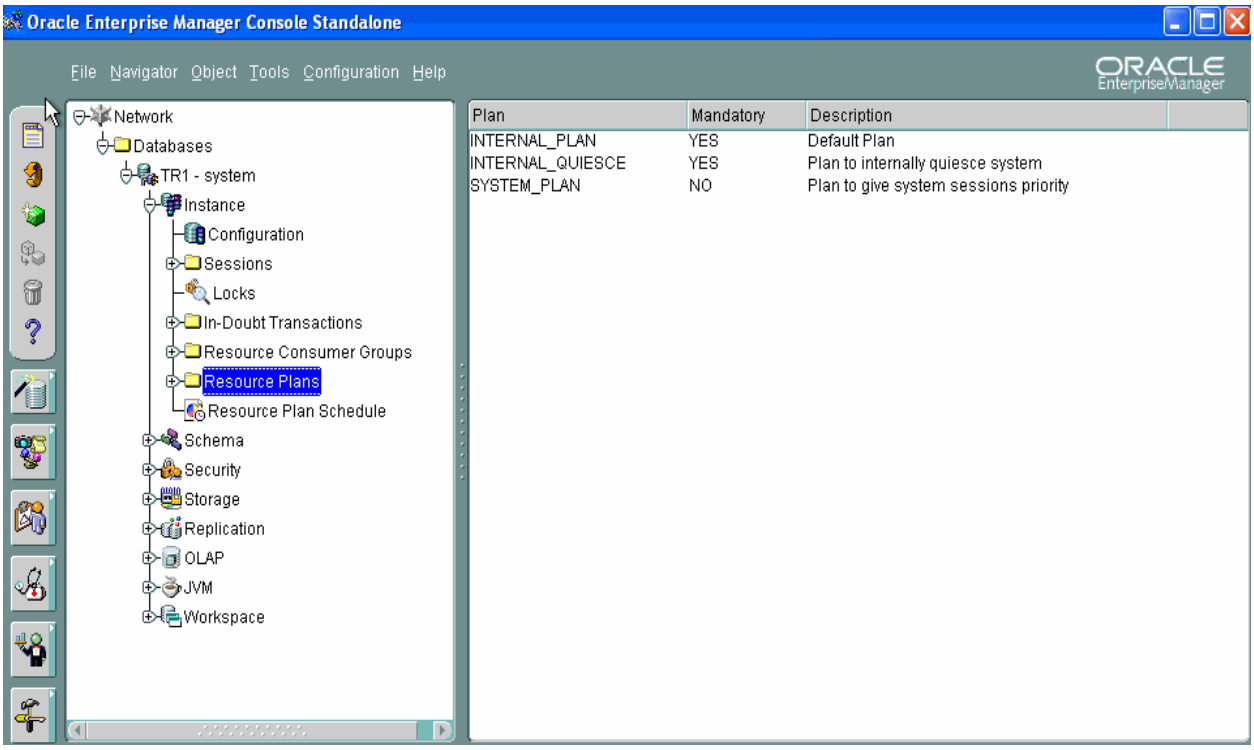
در این قسمت User هایی تعریف می کنیم که در هیچ گروه و دسته ای جهت استفاده از منابع تعریف نشده یا نمی خواهند بشوند.

4-SYS Groups :

یکی از مهم ترین گروه ها است که تمام User های تعریف شده در آن دارای قابل مدیریتی سطح بالا و اولویت بالا در Session خواهد بود.

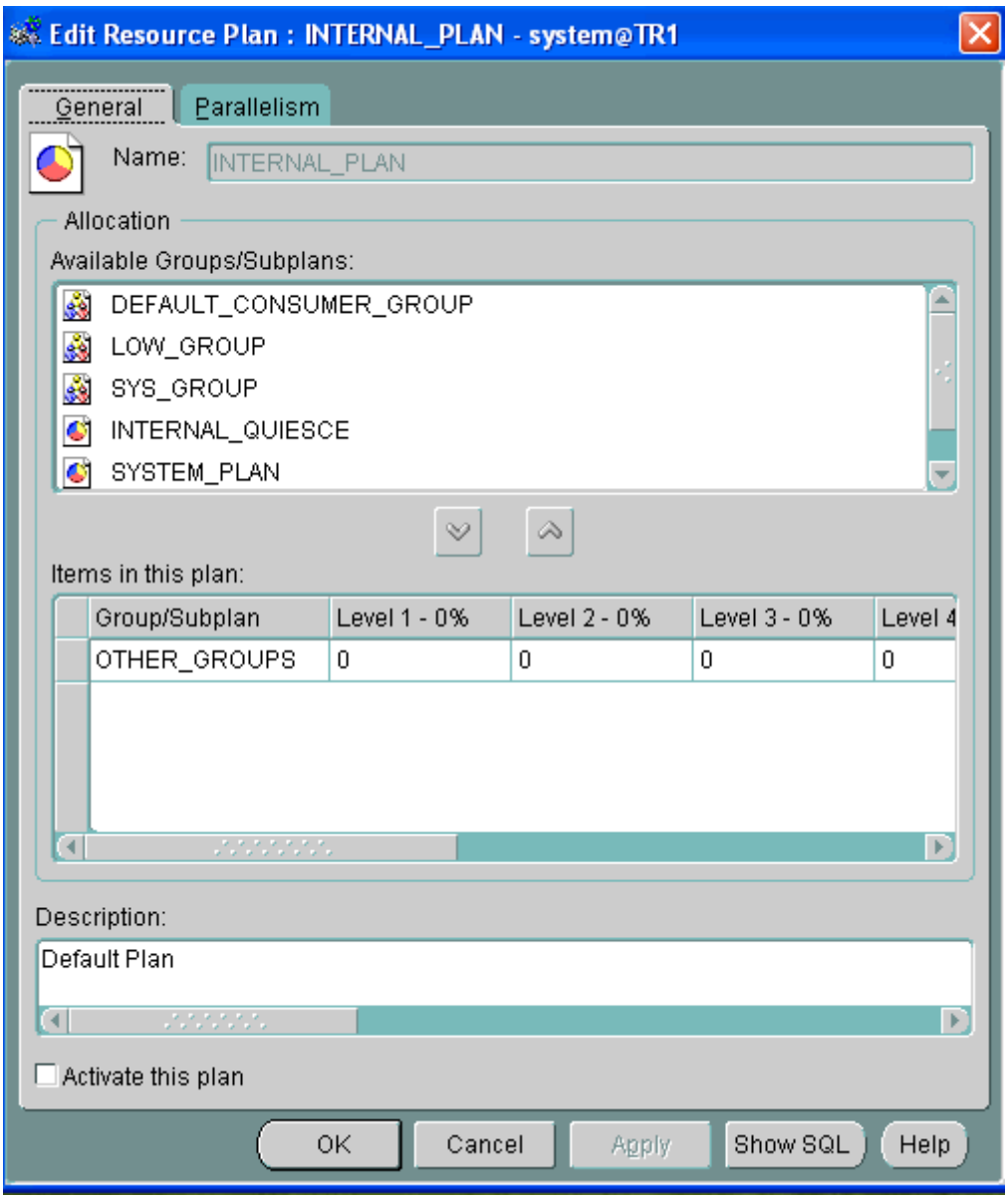
Resource Plan :

بعر از تعریف Resource می توان گزینه های Resource Plan را شکل دهیم. این قسمت به ما کمک می کند تا در سه سطح تعریفی , INTERNAL_PLAN
INTERNAL_QUESCE , SYSTEM_PLAN گروه ها و زیر مجموعه های عملیاتی دسترسی به منابع را تعریف کنیم.



در Resource Plan میزان استفاده از منابع سیستمی به ازای همه گروه های کاری در هشت سطح مقدماتی تعریف می شود و می توان این Plan را بصورت Active تعریف کرد و با دستور عمل های SQL ، Plan را مشخص نمود.

این Plan با دیگر Plan ها موازی شود یا Paralielism و هشت سطح عملیاتی CPU در آن تعریف می شود.



Security:

بخش بعدی امنیت است. در این بخش عملیات مربوط به User انجام می شود. ایجاد User، حذف User، تغییر User و هم چنین دادن مجوز عملکرد به User انجام می شود.

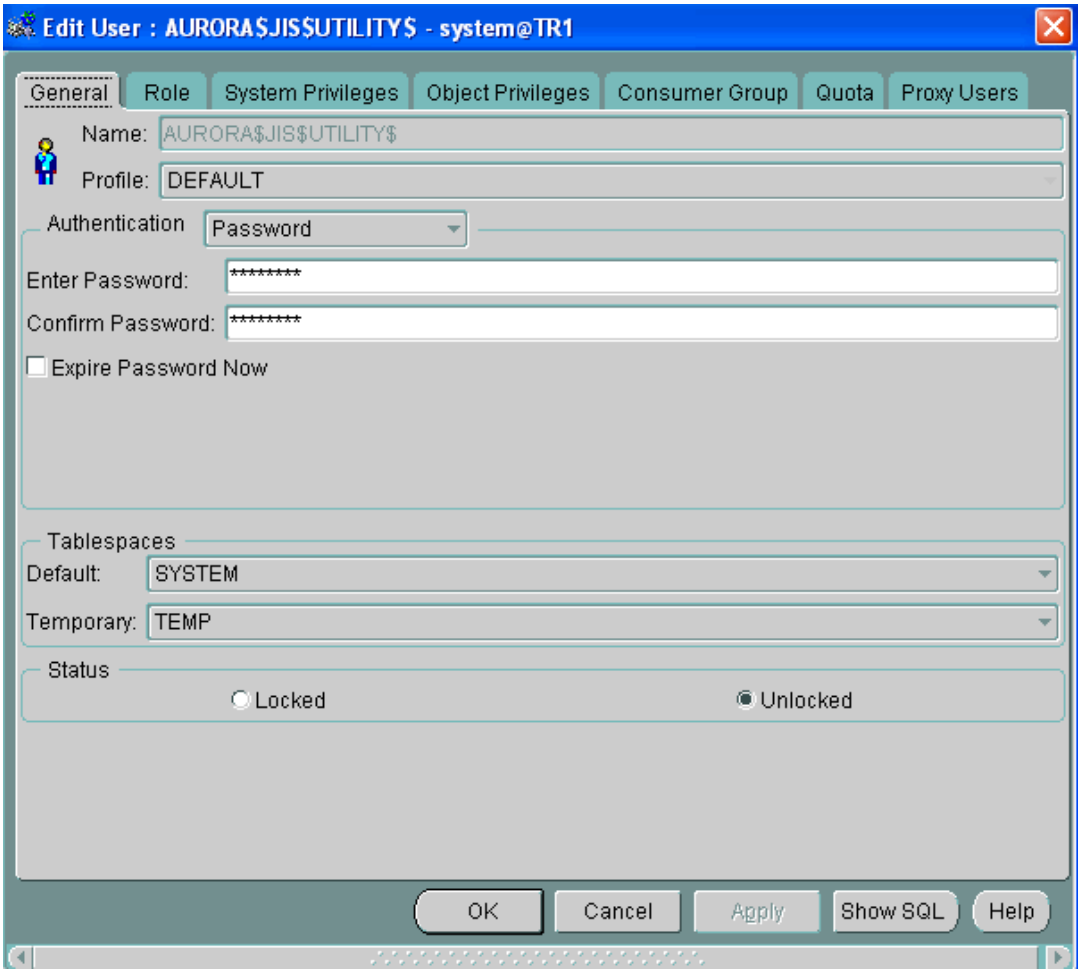
در این قسمت سه بخش داریم: profile، Roles و Users است.

1- Users

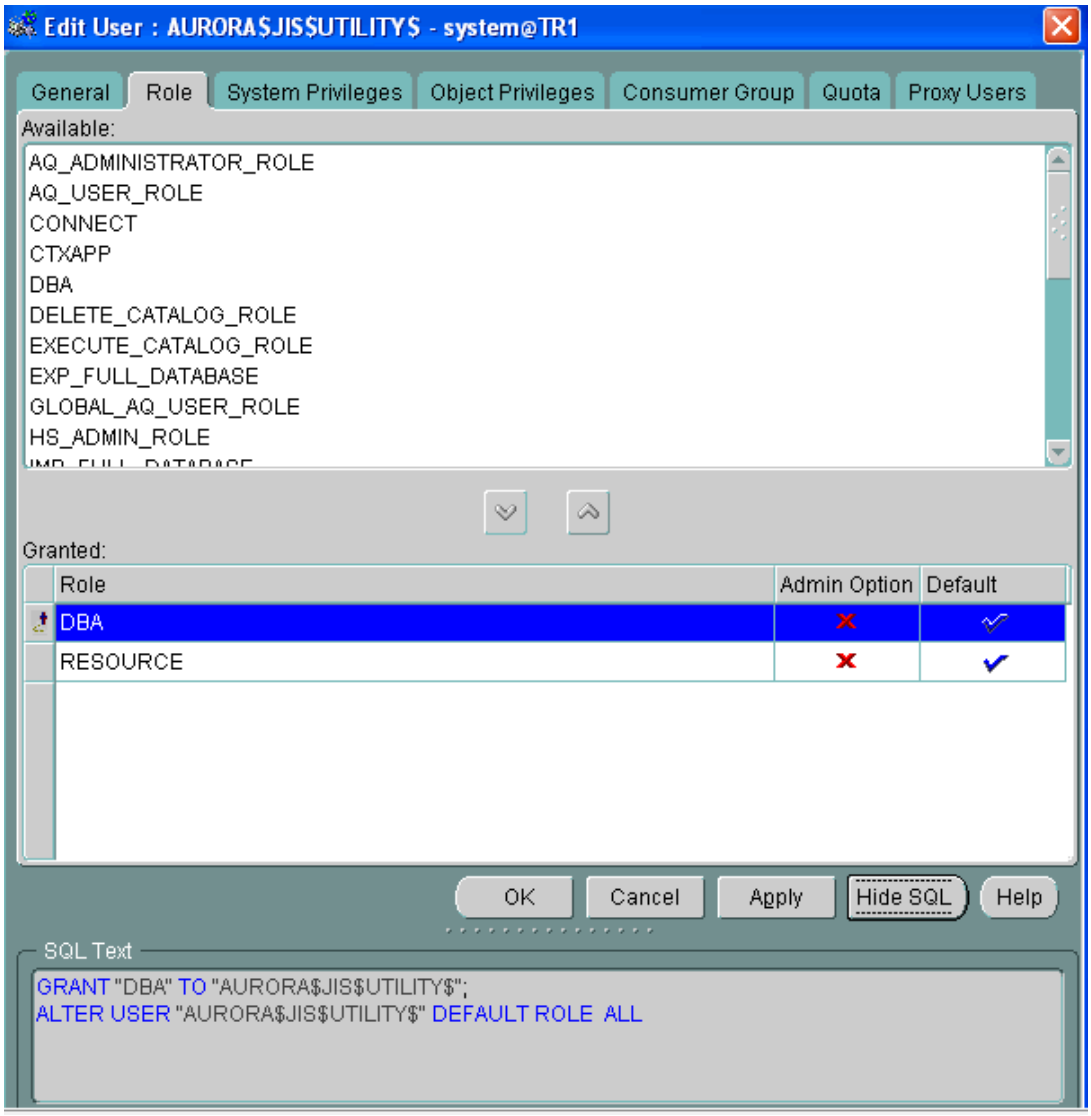
در قسمت User به ازای هر User سیستم موارد زیر را خواهیم داشت: General , Role , System Privilege , Object Privilege , Consumer Group, Quota , Proxy User است.

در قسمت General می توانیم profile کاربر را مشخص کنیم. هم چنین Authentication را روی همه چیز متمرکز کنیم.

و همچنین ۱- پسورد ۲- دسترسی از بیرون ۳- دسترسی عمومی و همچنین پسوردUser ها را مشخص کنیم و برای آن زمان انقضا در نظر بگریم و همچنین برای هر User ، Tablespaces مجزا داشته باشیم.

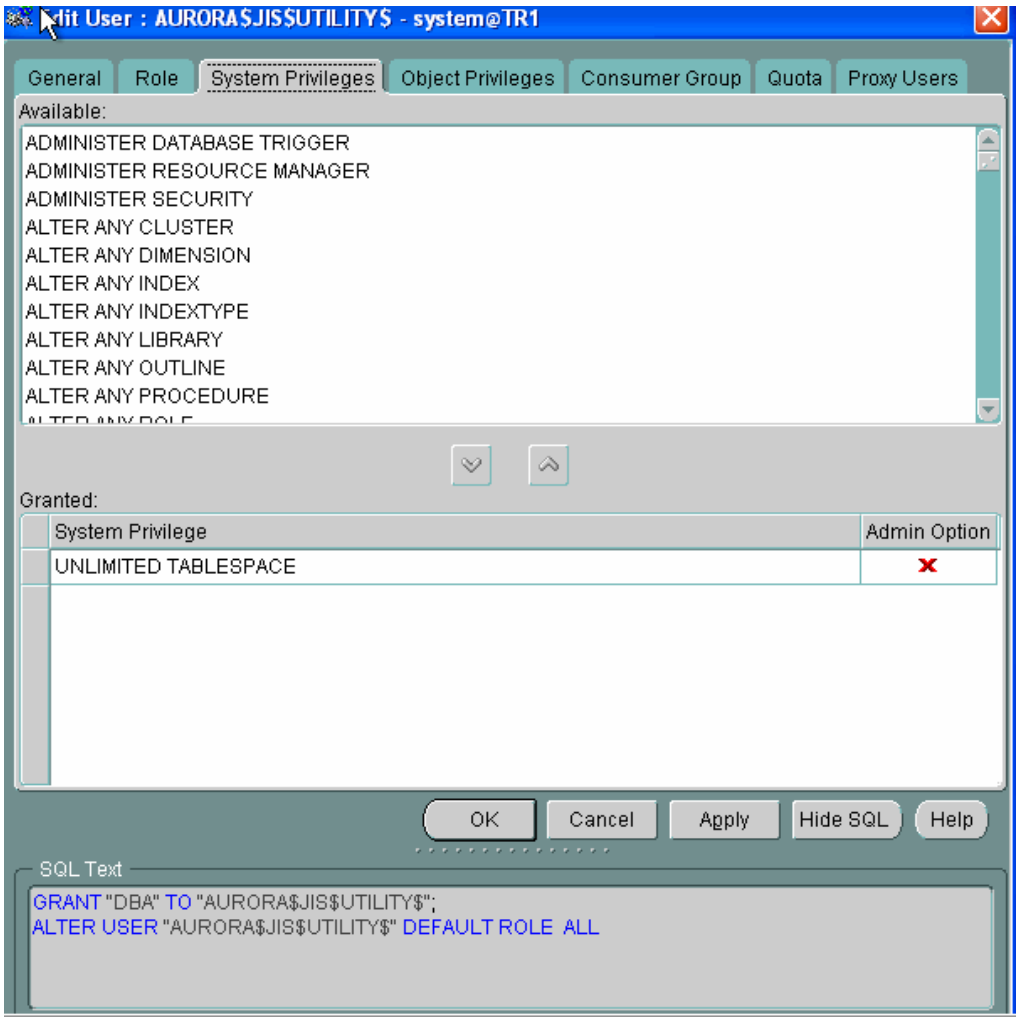


در قسمت Roles می توانیم به User تعریف شده اجازه استفاده از Role های مختلف را بدهیم و آن را به عنوان Admin یا initial تعریف می کنیم.



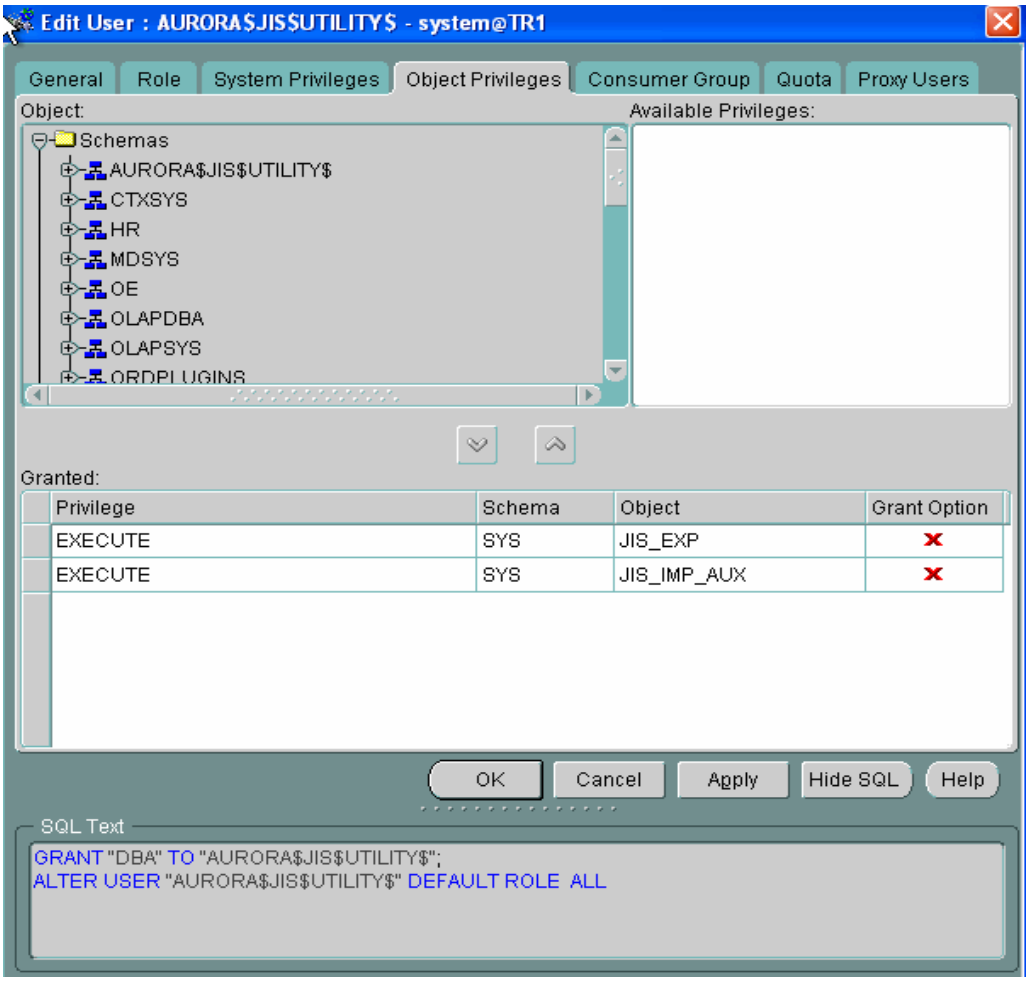
System Privilege :

مجوزهای عملکرد User در این قسمت به User ایجاد شده یا موجود مجوز اجرای دستورالعمل های مهم وحیاتی سیستم را می دهیم و هر دستور العمل که با دابل کلیک انجام شود در آن صورت در لیست مجوزهای User قرار می گیرد.



Object Privilege :

در این قسمت به User در Schema و جزء به جزء Schema اجازه داده می شود تا مجوزهای select , delete , update , insert , execute انجام شود.



Consumer Group :

User تعریف شده یا موجود را به یکی از سه دسته گروه های استفاده کننده نسبت می دهیم.

Low- Groups ، Default_ Consumer Group ، SYS Groups هر User می تواند از هر یک از موارد زیر فضایی از هارد دیسک یا مودم را اشغال کنیم که به آن Quota می گویند. که به این فضا Tablespaces ، Quota می گویند.

Cwmlite , Drsys , Example , Index , System , Temp , Tool , Undotbs , Users

این فضا به سه صورت در اختیار کاربر قرار می گیرد :

۱-none هیچ فضایی اختصاص نمی یابد

۲-Unlimited این فضا محدود می شود

۳-Value مقدار می دهیم

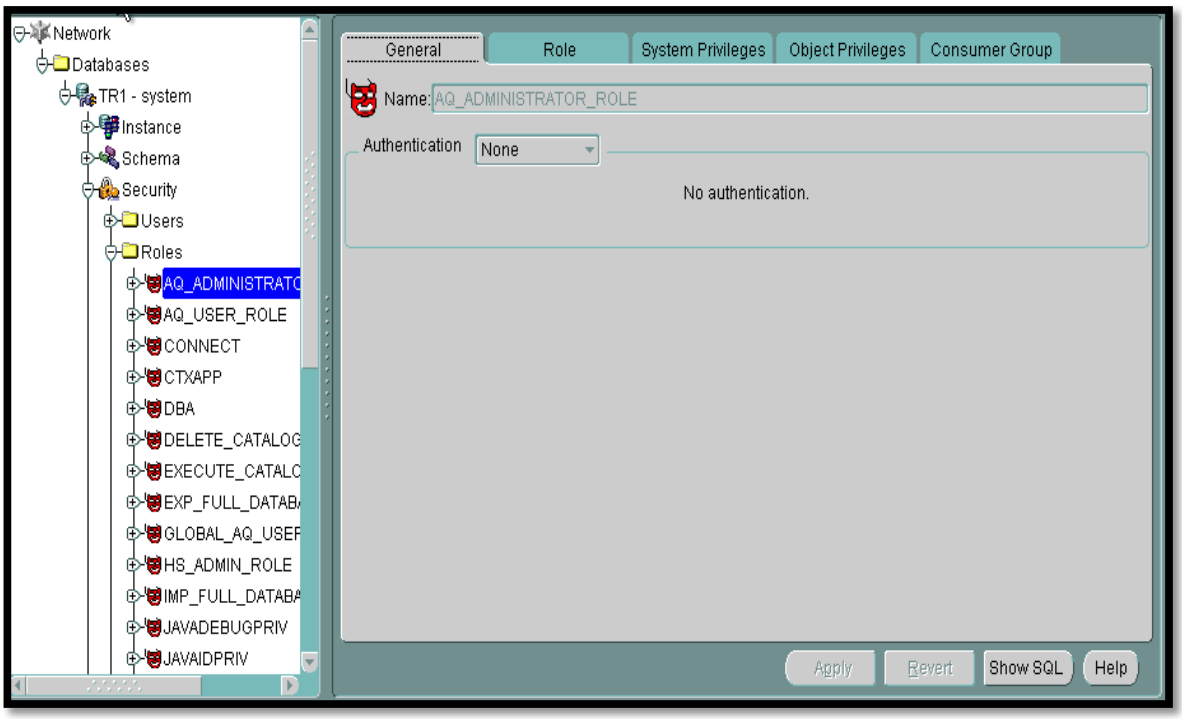
Proxy User :

برای User تعریف شده یا User انتخاب شده می توانیم Proxy User تعریف کنیم. حتی می توانیم Proxy را ورودی و خروجی کنیم یعنی این User را برای User های دیگر Proxy کنیم (Proxy اینجا به دو معنی است ۱- Cash ۲- Filter)

2-Roles :

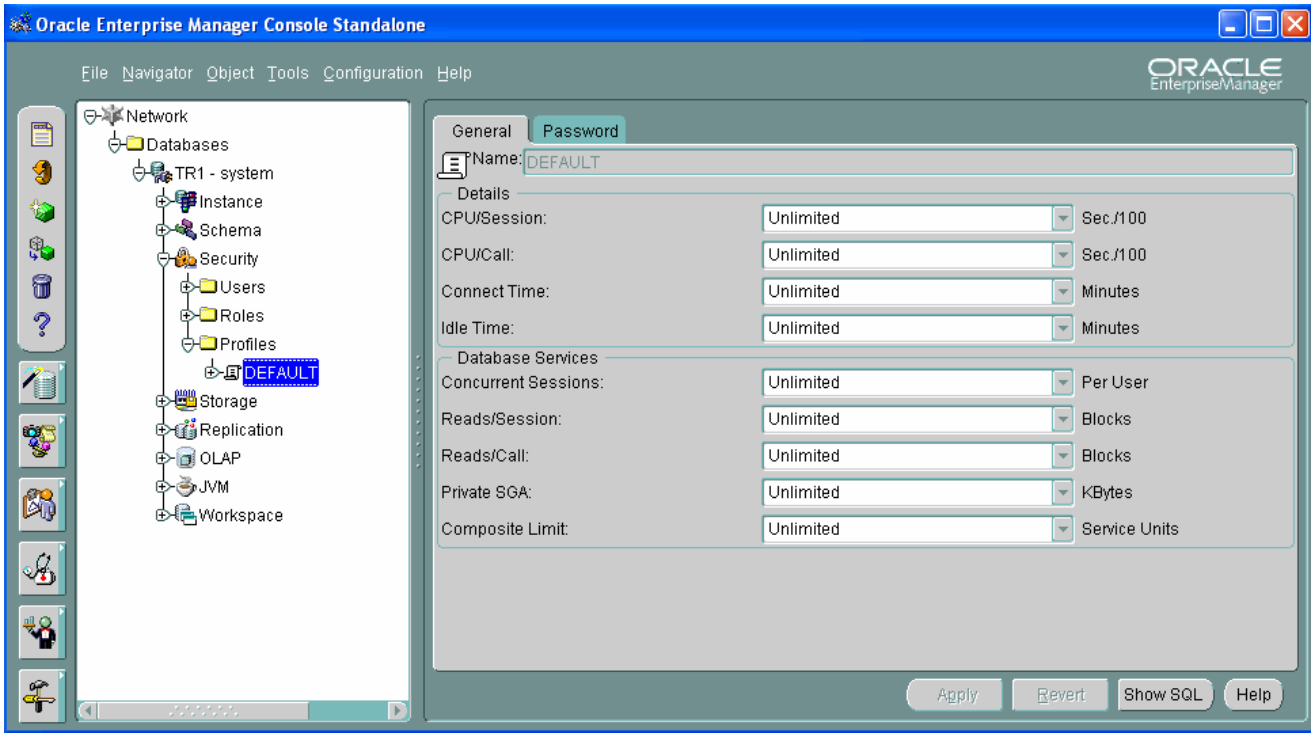
در این قسمت Role های تعریف شده وجود دارد و برای آن ها Authentication نوشته می شود و همچنین گزینه های اجرایی آن ها نیز مشخص می گردد و هر Role دارای بخش های زیر است.

General , Role , System Privilege , Object Privilege , Consumer Group است.



3-Profile :

Profile موجود یا جدید را می توان برای موارد زیر تعریف کرد



در قسمت Name اسم آن را وارد می کنیم

قسمت Details آن شامل

CPU / Session

CPU /Call

چند بار CPU کار می کند.

Connect Time

چه موقعه connect می شویم نشان می دهد

Idle Time

زمان انتظار را نشان می دهد

در قسمت Data Base شامل

Concurrent Session

Reads/ Session

Reads/call

Private SGA

Composite Limit

برای Profile می توانیم Password تعریف کنیم و حتی برای آن تاریخ انقضا تعریف کنیم یا مدت زمان ماندگاری یا عدم ماندگاری تعریف کنیم.

نمونه سوال های امتحانی:

۱-در طراحی امنیت بانک چند موضوع مورد بررسی قرار می گیرد؟

۲-در طراحی هنگام پیاده سازی باید به چه موارد دقت کنید؟ و چه امکاناتی روی Data Base بهتر است تعریف شود؟

۳-بانک اطلاعاتی رابطه ای RBDBMS را تعریف و مفهوم Relation Ship را بیان کنید؟

۴-کاربرد Domain را بیان کنید و داده های مهم آن چه هستند؟

۵-دزدی اطلاعات از Data Base شامل چه موارد هستند و نگرانی های دزدی از Data Base در چه بخشی هایی بیشتر است؟

۶- سطوح امنیت بانک شامل چه مواردی است؟

۷-امنیت در بانک اطلاعاتی Data Base Security چه مفاهیمی دنبال می شود؟

۸-عمده اختلافات و ناامنی ها و اختلال در بانک شامل چه موارد است؟

۹-موارد نرمالیزه کردن را بیان کنید؟

۱۰-خطرات محیطی بانک اطلاعاتی شامل چه مواردی خواهد بود؟

۱۱-برای تامین امنیت بانک اطلاعاتی چه مواردی را باید در نظر بگیرید؟

۱۲-نیازمندی های امنیتی بانک اطلاعاتی را بیان کنید؟

۱۳-طراحی نقشه امنیتی برای بانک های اطلاعاتی چگونه است؟

۱۴-Privilege چیست و چه دستوراتی جهت کنترل و دستیابی بانک نوشته می شود؟

۱۵-در بانک اطلاعاتی برای کنترل حملات و آمارگیری به چه مواردی باید دقت داشته باشیم؟

۱۶-تعریف نقاط آسیب پذیری در Data Base ها بیشتر روی چه مناطقی از Data Base تاثیر گذار است؟

۱۷- Multi Three Programming و دفاع در برابر حملات چگونه شکل می گیرد ؟

۱۸- ۱۰ عنوان امنیتی برتر برای تهدیدات امنیتی بانک های اطلاعاتی را نام ببرید؟(۵ مورد)

۱۹-امنیت در Data Base Oracle را بیان کنید؟

۲۰-تصمیم گیری بر مدیریت ریسک ممیزی یا Accounting شامل چه گزینه هایی می شود؟

۲۱-چرخه Oracle را بیان و کاربرد آن را شرح دهید؟ با شکل

۲۲-در رمزنگاری معماری Oracle چند نوع رمزنگاری مطرح می شود؟ شرح دهید

۲۳-امکانات رمزگذاری شده در نسخه Oracle 10 را بیان کنید و Master Key را بیان کنید؟

۲۴-Wallet را تعریف کرده و طریقه استفاده از Wallet چگونه است با شکل بیان کنید؟

۲۵-در رمزنگاری Oracle ، 10g چه امکاناتی نسبت به ورژن 9.I دارد؟ و گزینه های رمزگذاری بهینه را بیان کنید؟

۲۶-هر Repazitory شامل بخش های زیر است نام ببرید و ۴ مورد را به دلخواه توضیح دهید؟

۲۷- ۵ مورد از Parameter Name را بدلخواه نام برده و شرح دهید؟

۲۸- bitmap_meger_area_size را بیان کنید؟

۲۹- hash_area_size را توضیح دهید؟

۳۰- Java_max_sessionspace_size را شرح دهید؟

۳۱- محدودیت های اجرایی Instance را نام برده و شرح دهید؟

۳۲- تعریف Session را در سیستم Oracle توضیح دهید؟

۳۳- Resource Consumer Groups را نام برده و شرح دهید؟

۳۴- Resource Plan را بیان کنید؟

۳۵- Security موارد آن را نام ببرید و بطور خلاصه شرح دهید؟