نمونه سوالات درس بانکهای اطلاعاتی امن

استاد:

مهندس سارنگ قربانیان

تهیه کننده:

زهرا میثاقیان

نیمسال نخست سال تحصیلی ۹۳-۱۳۹۴

دانشکده انفورماتیک شرکت داده پردازی ایران

(تاریخ ویرایش نهایی ۱۳ دی ماه ۱۳۹۳)

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

۱-امنیت در طراحی بانک اطلاعاتی

۲- بکارگیری ابزارهای امنیتی بانک اطلاعاتی

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

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

۳–بانک اطلاعاتی رابطه ای RBDBMS را تعریف و مفهوم Relationship را بیان کنید؟

این نوع بانک اطلاعاتی بر اساس تئوری ریاضی مجموعه ها و رابطه ها تعریف می شود و عملکردی که روی مجموعه ها و یا رابطه ها شکل می گیرد را relationship می گویند.

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

تعریف حوزه مقادیر جهت ثبت واحدهای مرتبط با داده ها – داده های مهم Domain نام خانوادگی

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

بیشتر Account ، کارت های اعتباری و گواهینامه ها 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

۶– سطوح امنیت بانک شامل چه مواردی است؟(نام ببرید)

۱. سطح امنیت انسانی
۲. سطح برنامه کاربردی
۳. سطح بانک اطلاعاتی
۴. سطح امنیتی لایه فیزیکی
۵. سطح امنیت شبکه
۶. سطح امنیتی سیستم عامل

۷–(سوال مهم)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.

۸–عمده اختلافات و ناامنی ها و اختلال در بانک شامل چه موارد 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

۹– موارد نرمالیزه کردن را بیان کنید؟

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

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

۱. کوئری های متداخل
۲. دام پیوندی
۳. ایجاد گسل زمانی که از یک جدول کوئری می گیریم و ارتباط با جدول متناظرش را نخواهیم داشت.
۴. حملات تغییر ماهیت دیتا و تغییر صفحات
۵. تزریق کد
۶. ردیابی دیتا (Data)

۱۱– 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.

۱۲– (سوال مهم) نیازمندی های امنیتی بانک اطلاعاتی را بیان کنید؟

۱-لایه امنیتی فیزیکی ، در نشست دیتا روی ابزار مکانیکی و جامعیت فیزیکی Data

۲-امنیت منطقی شامل کلیدها و رفرنس ها و توزیع شدن دیتابیس در چندین شبکه

۳-جامعیت مولفه ها ویا المان های Data Base و کنترل ارجاعات و ذخیره سازی درجه اول

۴-دستیابی یا قابلیت های تعویض مجوز و ثبت وقایع و کنترل جداول ، تعریف مجوز و ثبت وقایع

۵-Access Control (تعریف دستورات کنترلی record و grant یا تعریف Revoke های دیتابیس)

۶-تشخیص user یا هویت کاربر (تعریف کاربر و کنترل دستیابی کاربران)

۷-قابلیت در دسترس بودن (Availability)

۱۳– (سوال مهم) طراحی نقشه امنیتی برای بانک های اطلاعاتی چگونه است؟(نام ببرید)

۱-Platform بانک اطلاعاتی یا سیستم عامل Data Base

۲- نام Data Base یا SID

۳-Function Data Base

۴-Application

۵-مالک برنامه کاربردی یا Application Owner

۶-User Name و Password

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

۱۱- تعریف Role

۱۲- شناسایی Application ها و داده های آنها و اجازه انجام Recovery و Backup

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

دادن مجوز به یکسری از سرویس ها برای دسترسی کاربر

Grant Privilege On Object To Users
Revoke Privilege On Object From Users

۱۵–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

۱۶–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 Form , Password , Login 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 :

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

۱۷– Multitier Programming و دفاع در برابر حملات چگونه شکل می گیرد ؟

برنامه نویسی لایه ای می باشد که در سه لایه و با کمک Framework و Pattern های برنامه نویسی انجام می شود و به کمک لایه Business لایه بیرونی تعریف می شود و لایه دیتا، لایه درونی را تشخیص می دهد و لایه fasad عامل مدیریت دسترسی به دیتا و business است.

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

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

۱۹–امنیت در Data Base Oracle را بیان کنید؟

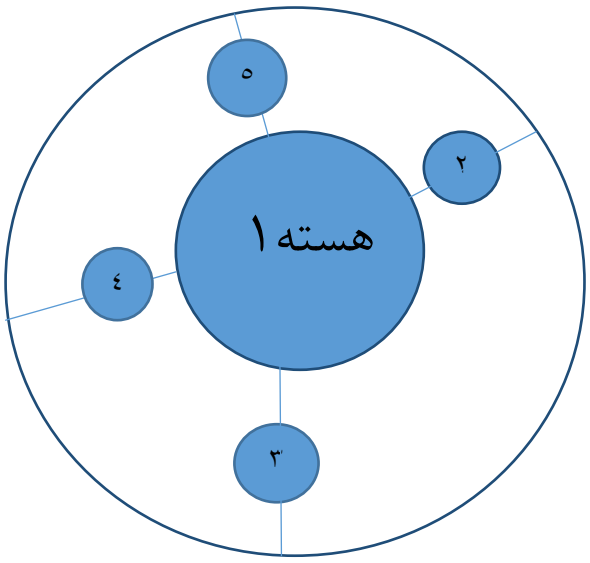
رمزگذاری با استاندارد BLP، استفاده از کلیدهای نامتقارن، تعریف دستیابی و مجوزهای دستیابی در سه مرحله ، تعریف فایل سیستم مجزا از سیستم عامل و رمزکننده فایل است.

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

۱- Requlatory – Risk
۲- Detterence
۳- Detection & Recovery

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

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 برچسب 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

کاربرد

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

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

۱-DBMS-Crypte

۲-DBMS-OBFUSCATION-Tool

در این رمزگذاری ها الگوریتم های رمزنگاری شامل DES-۲Key , RC۴ , ۳DES , DES برای رشته ای خواندن Data و Black Sofery از رمزنگاری ECB , CFB , CBC استفاده می کند.در رمزنگاری Hash از رمزهای MD۵ و SHA۱ استفاده می کند. برای تولید رمز از اعداد تصادفی با رنج بالای Integer استفاده می کند.

۲۳– امکانات رمزگذاری شده در نسخه ۱۰ Oracle را بیان کنید و Master Key را بیان کنید؟

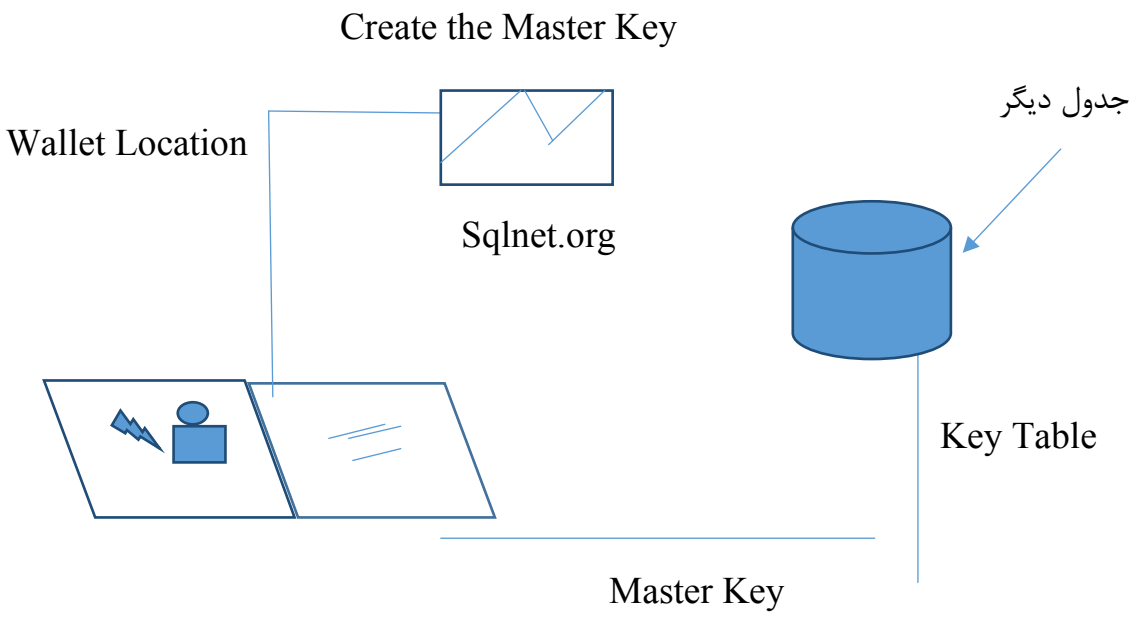
کلیدها قابلیت مدیریت و بصورت پویا است ، Transparent اضافه شده روی لایه Application ، آدرس محل ذخیره سازی در سمت DBMS است بخاطر همین قابل دسترسی نیست. با توجه به امکانات امنیتی ۱۰g این Data Base در سطح Application نیز رمزگذاری متفاوت Data را داریم همچنین کلیدهای رمزنگاری قابل تغییر و قابل مدیریت هستند و آدرس Data Base و فایل های اصلی آن درون Data Base درون DBMS شخصی سازی و مخفی می گردد.

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.

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

(شکل و توضیحات مهم هست)

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.



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.

Alter system Set Wallet Open IDENTIFIED By “Welcome”

۲۵–در رمزنگاری ۱۰g ، Oracle چه امکاناتی نسبت به ورژن ۹.I دارد؟ و گزینه های رمزگذاری بهینه را بیان کنید؟

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.
رمزنگاری بهینه

الف) کل Table را رمزگذاری می کند و محل استقراری آن ها
Pace Encryption Table
ب) Master Key می تواند در یک Device دیگر مثل USB , Token ، موبایل و غیره ذخیره سازی می شود.
Stored In HSM Device Master Key
ج) امکان رمز گذاری Object های بزرگ در این ورژن Oracle وجود دارد.
Secure File LOB Encryption

۲۶–هر Repazitory شامل بخش های زیر است نام ببرید ؟

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

۲۷– گزینه دیکشنری در پارامترهای name چه تعریفی را انجام می دهد؟

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.

۲۸- bitmap_meger_area_size را بیان کنید؟

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 ۱ MG می باشد.

۲۹- hash_area_size را توضیح دهید؟

این قسمت فضایی هست که د ر مرتب سازی و دستیابی به Bitmap تعریف می شود و در هنگام رمزگشایی Database این فضا به فضای cache پیوند می خورد.

۳۰- Java_max_sessionspace_size را شرح دهید؟ (سوال حذف)

۳۱- محدودیت های اجرایی Instance را نام ببرید؟

۱- Instance_Max_ Session
۲- Instance_Max_Users
۳- Instance_ Session_warning

۳۲- تعریف Session را در سیستم Oracle توضیح دهید؟

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.

۳۳- Resource Consumer Groups را نام برده و شرح دهید؟(سوال حذف)

۳۴- (سوال مهم) Resource Plan را بیان کنید؟

بعد 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_QUESCE , INTERNAL_PLAN 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.

۳۵– در security در سیستم اواکل تفاوت system Privilege و object Privilege در چیست؟

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.

۱- 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 execute , insert , update , delete , select 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)

۲-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.

۳-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.

موفق و پیروز باشید