Oracle数据库软件的主要目的是管理有价值的数据；这些数据位于组织内部各种操作的核心。它们的一部分价值在于这些数据是组织内部私有的，也是该组织独一无二的优势。正是出于这个原因，组织会保护自己的数据，以防未经授权的用户访问。这里，我们将会专注在数据保护的三个不同方面：

* 安全，包括用于授权他人访问的工具。
* 审计，让数据库管理员可以发现谁对数据库做了什么操作。审计过程就是记录访问历史信息，它可以帮助数据库管理员了解各种数据库操作并监控违规访问和各种访问尝试。当配置Oracle 11g时，系统会询问管理员是否需要保持系统的默认安全设置。如果选择需要，审计功能将会被打开，并会产生一个新的默认密码信息。在这个时候，还有许多其他的数据库初始化参数被重置。
* 依从性，即证明数据安全可靠的能力。目前，许多案例都会从法规上要求具有这种可证明性。尽管依从性会给许多技术人员带来致命性打击，但是仅缺乏依从性也会给企业带来重大损失，这是一个简单的事实。因而，依从性是管理的一个重要内容。

## 1、安全

在多用户的环境中有效的管理数据库有许多重要的方面，其中之一便是要创建一种安全模式来控制对数据库的访问和修改。在Oracle数据库中，管理员可以为每个用户或每个数据库角色授予一个安全检查。

安全管理通常可以在三个不同的层次来执行：

* 数据库级别。
* 操作系统级别。
* 网络级别。

在操作系统级别，DBA应该能够创建和删除数据库相关的文件，而普通数据库用户没有这类权限。Oracle在它的标准文档组中包含操作系统特定的安全信息。在许多大型的组织中，DBA或者数据库安全管理员会和系统管理员一起制定安全规范并执行相关的安全实践。

数据库安全规范用于控制用户对数据库的访问和限制用户使用用户名与密码的能力。该规范可能会限制分配给用户的资源（磁盘和CPU），并强制对用户进行审计。数据库级别的安全还能够控制对数据库中特定模式对象的访问和使用。

## 2、用户名、权限、组以及角色

DBA或者数据库安全管理员可以创建能够连接到数据库的用户名。安装过程中会自动创建两个账户：SYS和SYSTEM，并为它们赋予DBA角色。

每个数据库用户名都有一个密码，以防止未授权访问。生成的新密码和修改后的密码应该满足以下条件：

* 至少包含8个字符。
* 至少包含一个数字和一个字符。
* 不是用户名的反转。
* 在结尾添加1~100的数字来区分用户名或者使用名。
* 不要和内部的简单单词列表中的任何单词匹配。
* 至少要保证新密码和旧密码有三个字符不同（如果有旧密码的话）。

作为必须实施的安全策略，Oracle会在每次创建密码和修改密码时检查这些特征。

一旦用户成功地登录数据库，他的访问将受限于权限；所谓权限也就是执行某条SQL命令的权利。有些权限仅被授予数据库中特定的模式对象（例如，删除特定表中的行的权利）。

角色也叫做权限组，它可以被创建、修改和删除。在大多数实施中，DBA或者安全管理员会为用户创建用户名并指定用户的角色，借此来为用户授予各种权限。现在此类工作都是通过Oracle企业管理器（EM）控制台来完成的。举个例子，你为某个角色赋予了访问一个特定应用程序组（例如，“人力资源”的权限）；或者你定义了多个角色，具有某个角色的用户可以更新人力资源应用程序中的小时工资，而具有其他角色的用户则无此权利。

每个数据库都提供了一个名为PUBLIC的伪角色。所有的用户都可以使用授予PUBLIC的权限。例如，如果数据库连接是使用关键字PUBLIC创建的，那么对于那些有权限访问这些链接和同义词所指向的底层对象的用户来说，它们是可见的。正如我们在本章审计一节所描述的那样，CREATE PUBLIC DB LINK的权限现在会被审计。由于对数据库脆弱性的日益增加，你可能需要限制PUBLIC角色的权限。

## 3、身份管理

糟糕的安全管理总是会影响安全性。需要执行的管理任务越复杂，就越有可能出现错误，从而给系统留下安全漏洞。如果你期望在一个环境中从中央来控制对多个数据库的访问，Oracle身份管理提供了一种将用户信息及其授权信息存储在诸如Oracle互联网目录（OID）等LDAP目录中的解决方案。例如，可以使用OID来授权SYSDBA和SYSOPER连接。

## 4、安全的权限

有四种基本类型的数据库操作可以通过Oracle数据库的安全权限来限制：

* SELECT执行查询。
* INSERT在表或试图中插入行。
* UPDATE更新表或试图中的行。
* DELETE从表、表分区或者试图中删除行。

除了这些数据相关的权限之外，还有一些权限适用于数据库模式中的对象：

* CREATE在模式中创建表。
* DROP从模式中删除表。
* ALTER修改表或试图。

所有这些权限都可以使用两条简单的SQL命令来操作。GRANT命令用于为用户或角色赋予特定的权限，而REVOKE用户撤销特定的权限。可以使用GRANT和REVOKE来修改某个用户或角色的权限。你也可以给其他人授予重新批准权限的能力。可以使用这两个命令加PUBLIC关键字来发布或者撤销所有数据库用户的权限。

另一个安全权限EXECUTE用于批准用户可以运行PL/SQL过程或函数的权利。在默认情况下，PL/SQL例程运行时具有编译它的用户的安全权限。或者，可以指定PL/SQL例程以调用者的权限运行，这意味着该例程运行时具有调用它的用户的安全权限。

## 5、特殊角色：DBA、SYSDBA与SYSOPER

Oracle数据库定义了三种特殊的角色。DBA角色是Oracle中最重要的默认角色之一。DBA角色包括大多数系统权限。伴随数据库创建的SYS和SYSTEM这两个默认的被授予DBA角色。基表和数据字典视图存储在SYS模式中，SYSTEM模式中的表用于存储管理信息或者供各种Oracle工具和选项使用。随着各种特定Oracle特性的部署，还会创建其他许多管理用户。

DBA角色的权限并不包含SYSDBA或SYSOPER系统权限中的基本数据库管理任务。因而，需要将SYSDBA或SYSOPER权限授予管理员。这些管理员会“CONNECT AS”SYSDBA或者SYSOPER到数据库中；即便是数据库没有被打开的时候，他们也可以访问这个数据库。SYS用户或者其他具有SYSDBA权限的管理员可以将为其他人授予SYSDBA权限。授予之后，SYSDBA的权限允许用户从SQL Plus的命令行中或者登陆Oracle企业管理器执行下面的数据库操作：

STARTUP

启动数据库实例

SHUTDOWN

关闭数据库实例

ALTER DATABASE OPEN

打开被安装但关闭的数据库。

ALTER DATABASE MOUNT

利用之前启动的实例来安装数据库。

ALTER DATABASE BACKUP CONTROLFILE

启动对控制文件的备份。不过，今天备份工作通常是通过RMAN来完成。

ALTER DATABASE ARCHIVELOG

指定redo日志文件组的内容必须在被重用之前归档。

ALTER DATABSE RECOVER

逐个应用日志或者启动自动应用redo日志。

CREATE DATABASE

创建数据库，为之命名，指定数据文件大小，指定文件及大小，并设置参数限制。

DROP DATABASE

删除数据库以及控制文件中的所有文件。

CREATE SPFILE

根据文本初始化（INIT.ORA）文件创建服务器参数文件。

RESTRICTED SESSION权限

允许连接到以受限模式启动的数据库。受限模式设计用于发现并解决问题以及某些维护操作，这有些类似于SYS的职责。

作为SYSOPER连接的管理员只能执行更加有限的命令：STARTUP与SHUTDOWN，CREATE SPFILE、ALTER DATABASE OPEN或MOUNT或BACKUP、ALTER DATABASE ARCHIVELOG、ALTER DATABASE RECOVER以及RESTRICTED SESSION权限。

数据库管理员一般通过操作系统认证机制或者密码文件来认证。Oracle早期版本所支持的CONNECT INTERNAL语法现在已经不可用。当使用操作系统认证机制时，管理用户必须在OSDBA或者OSOPER定义的组中命名。对于密码文件而言，必须使用ORAPWD工具来创建。用户一般由SYS或者具有SYSDBA权限的人来添加。

## 6、策略

策略就是用来扩展安全框架的方法。可以在策略中指定附加的要求。比如，可以指定每当用户尝试激活一个角色的时候做安全检查。可以使用PL/SQL来编写策略。例如，可以编写一个策略来限制用户只能访问某个特定的IP地址或者只能在一天中的某几个小时内进行访问。

从Oracle 10g以来，Oracle企业管理器的特色之一就是它的可视化策略管理界面；利用它可以访问EM仓库中的策略框架，从而帮助管理员管理数据库的安全性。策略库用于构建和存储安全策略或规则。违反安全规则的操作将会被分为关键、告警和信息三个级别并通过EM界面上报给管理员。安全违规检查每天都会执行，这是Oracle开箱即用的一个特性。策略可以针对业务需求进行调整，安全违规的报告也可能会被忽略。

## 7、限制数据访问

有些环境中，用户需要访问一个表，但是并不需要看到表中的所有数据。例如，和你有竞争关系的供应商可能也会按这个表。比可能希望让他们看到他们自己提供额产品以及所有供应商产品的总和，而不希望让他们看到竞争对手的详细信息。在随后的几节中，可以看到有许多方法能够做到这一点。另外，下面的这几节还会另外举几个股阿奴人力资源的例子有助于你理解。

### 7.1基于视图的安全

视图可以看成是由从物理基表中提取数据的查询语句定义的虚拟表。可以用视图仅把特定用户组需要访问的行和列显示出来。

例如，在HR应用中，来自HR部门的用户能够访问员工基表中的所有数据，这些数据包括诸如员工姓名、工作电话等基本信息，也包括诸如社会保险号、家庭住址、家庭电话等访问受限信息。当公司中其他部门的员工希望查看所有员工信息时，则可以通过创建一个视图为他们显示员工表中的基本信息，而不让他们看到其他更详细的私人信息。

创建虚拟私有数据库或者使用标签安全选项则提供了一个更加安全的方法来限制对特定数据的访问。

### 7.2细粒度的访问控制

实施安全控制是一项关键但又耗时的流程，特别是当你期望根据某个具有大量数据的属性进行安全控制的时候。在前面我们提到的HR应用场景中就有这种情况的一个好例子，即要求限制HR代表只能查看自己所服务的那些员工的行。如果按照前面的方法，你可能必须为每个HR代表定义一个视图，这样就会定义很多不同的视图，每当有HR代表离职或入职的时候，必须修改对应的视图。而且如果需要为HR代表设置对自己所服务的员工信息具有写权限，对其他员工的信息具有读权限，情况则会变得更加复杂。访问控制的粒度或范围越小，创建和维护安全权限的工作量则越大。

Oracle为此提供了一种细粒度的访问控制（FGAC）。在表和视图打开虚拟私有数据库（VPD）功能之后，通过PL/SQL函数来实现的安全策略就可以与这些表和视图相关联。

安全策略能够返回一个条件，这个条件与特定的SQL语句动态关联，由它限制返回的数据。在HR这个例子中，可以假设，每个HR代表负责姓的首字母在特定范围（例如A到G）的那些员工。根据每个代表职责的不同，安全策略可以返回WHERE子句来限制返回的行。可以将每个代表负责的范围保存在一个单独的表中：安全策略函数会动态地查询这个表。这样可以简化角色和责任频繁变化时对访问控制的管理。

可以使用内置的PL/SQL包DBMS\_RLS将安全策略与特定的视图或表关联起来。利用这个包，你还可以更新，打开或关闭一个安全策略。

VPD是Oracle 10g更新的版本的一个特色，它的粒度更细；当查询引用了某个特定的列，它可以实施强制性重写。Oracle 10g通过支持并行查询改进了VPD实现中的查询性能。细粒度的安全特性本身还取决于所提交的SQL语句类型。之前讲述的安全策略可用于将UPDATE、INSERT以及DELETE操作限制在一个数据结合中，但仍然允许SELECT操作作用在不同的数据组中。

## 8、标签安全选项

有了Oracle标签安全选项，当适合使用敏感性标签时，就不再需要编写VPD PL/SQL程序来实施行级别的标签安全。标签的收集、标签的授权以及安全执行选项可以应用于整个模式或者特定的表上。

敏感性标签根据用户查看和更新数据的需要来定义。它包含一个用来表示敏感度的级别，一个用于进一步划分数据的类别，以及一个用于记录所属关系（其本质上可能是分层的）和访问的组。

标准的组定义允许用户访问包含那些组标签的数据。数据中的反向组定义了用户若要访问这些数据在他的个人信息中所必须包含的标签。

可以通过企业管理器上的策略管理工具来创建和应用策略，定义敏感性标签、设置用户标签并对之进行授权。你还可以自己添加SQL谓词与标签函数，管理受信的程序单元，Oracle VPD细粒度访问控制策略，以及VPD应用上下文。在使用Oracle互联网目录之后，Oracle 10g及之后的版本仍然支持标签安全策略管理。

## 9、安全与应用程序的角色和权限

应用程序在运行过程中会涉及到许多具有不同权限的各种模式中的数据和逻辑。为了简化这种复杂性所带来的问题，通常会在应用程序中使用角色这个概念。应用程序的角色具有运行应用程序所需的所有权限；可以为用户在操作应用程序时授予各种角色。

应用程序角色包含的权限仅当用户运行该应用程序时才被授予该用户。应用程序开发人员可以在应用程序的开始位置添加一条SET ROLE命令来为运行该程序的用户设置适当的权限。类似地，可以在PL/SQL程序中调用DBMS\_SESSION\_ROLE来为用户设置权限。

有时候，还可以通过将权限封装在存储过程中的方法来实施应用程序的安全性。这种方法不会直接为应用程序授予访问各种表的权限，而是将访问权限赋予能够访问这些表的存储过程。举个例子，可以创建一个名为HIRE\_EMPLOYEE的存储过程，并将新员工的所有数据作为它的参数，然后为这个存储过程授予访问员工表的权限，而不必将INSERT权限直接授予EMPLOYEE表。

当你正常使用存储过程时，该存储过程拥有过去被赋予它的所有者的权限；而它的所有者就是这个存储过程所在的数据库模式。如果某个特定的模式能够访问特定的数据库对象，那么这个模式中的所有存储过程都具有与模式一样的权限。任何用户调用这些存储对象的时候，他们对底层的数据对象具有相同的访问权限。

举个例子，假设存在一个名为HR\_REP的模式。该模式具有对EMP表的写权限。HR\_REP模式中的任何存储过程也具有这个权限，因此，当一个用户被授予了访问HR\_REP模式中存储过程的权限，那么不论这个用户的个人安全权限级别如何，都拥有对EMP表的写权限。当然，只有使用该模式中的存储过程才具有此权限。

警告：关于通过存储过程访问数据，这里有一个比较小但是非常重要的告诫，即

安全权限必须直接授予数据库模式，而不能授予角色。

如果在编译时给存储过程加上AUTHID CURRENT\_USER这个关键字，将会根据调用过程的用户名设置安全权限，而不是根据存储过程所在的模式（存储过程的定义者）设置安全权限。如果一个用户对特定的数据库对象具有特定的访问权限，那么他在使用这类存储过程的时候也具有相同的权限。

## 10、分布式数据库与多层安全

标准Oracle数据库可用的所有安全特性在分布式数据库环境中同样可用。13章讲述分布式数据库。不过，分布式数据库环境引入了其他一些安全特性。例如，需要支持服务器连接的用户账户必须存在于系统中所有的分布式数据库中。在创建数据库连接（它定义了分布式数据库实例之间的连接）时，要求每个点都要允许该用户的账户和角色。

### 10.1分布式安全管理

对于大型的实施而言，你可能期望为用户和角色在所有的分布式数据库之间配置全局的认证过程。有了全局的认证，你仅需为多个分布式数据库维护一个认证列表。当需要这种类型的外部认证时，Oracle高级安全选项提供了这样一种解决方案。

企业管理器通常可以用于为Oracle OID服务器配置应用程序用户。该服务器遵循LDAP协议。未经过认证的用户在访问应用程序的时候会被重新定向到登录服务器。在那里，他会被提示输入用户名和密码；用户输入的用户名和密码交给OID服务器进行检查；检查通过后，将会返回一个cookie，而该用户也会被从登录服务器重定向到该应用程序。

### 10.2多层安全

在典型的三层架构的实现中，Oracle应用服务器作为客户和数据库服务器的接口，运行着部分应用程序逻辑，同时提供Oracle身份管理（OIM）的基础架构。Oracle互联网目录为基于Oracle数据库的应用程序提供目录服务。它由目录同步服务、供给继承服务以及被授予的管理服务组成。多层应用程序的安全性通常由应用程序的权限以及在所有三个层次中保存的用户身份信息来控制。

像大型应用程序或者基于Web的应用程序那样，使用多层结构可能还会需要代理认证。应用程序通常会使用共享的连接来联系中间层，而中间层通过代理访问数据库。有些数据库会将安全性与会话关联起来，这意味着每当用户身份发生变化时都必须重新建立会话。这种限制就使得多层安全性比较难以实施。

Oracle将认证与会话分离；这样，在中间层使用代理将会非常灵活。单个会话能够支持具有不同身份的不同用户。在Oracle 10g之前，只能通过OCI接口来充分利用这种功能，这个过程需要大量编码。之后，这个限制被取消了，标准SQL以及SQL Plus这样的SQL工具都可以使用代理认证。

## 11、高级安全选项

Oracle高级安全选项（ASO），过去叫做高级网络选项（ANO），它被用于Oracle Net连接的分布式环境中。在这样的分布式环境中关注的焦点是数据的安全访问与传输。该选项可根虎用户要求对传输的数据进行加密，防止其他未经授权的用户通过Oracle Net、Net/SSL、IIOP/SSL，或者在瘦JDBC客户端和数据库之间对数据进行访问。它支持的加密算法包括RC4\_40、RC4\_56等等。另外，借助MD5和SHA-1单位那个算法，通信报文可防止数据篡改，事务重放以及数据被删减。

从Oracle 10g开始，高级安全选项开始包含透明数据加密特性。该特性Wie加密数据库中的数据提供了一种简单的方法；ASO的网络数据加密选项可用于保护数据在传输到客户端过程中的安全性。

ASO还支持各种身份认证方法来确保用户身份的准确性。它所支持的第三方认证服务包括Kerberos、RADIUS以及DCE。其中对RADIUS的支持将会打开第三方额认证设备如智能电子商务和令牌卡的支持。目前，公钥基础设施（PKI）认证广泛应用于保护基于因特网的电子商务应用的安全性；它使用X.509 v3数字证书，并可充分利用存储在Oracle Wallets中的信托信息。Oracle 10g增加了对拥有Kerberos凭证的用户进行认证的能力，从而使得基于Kerberos的认证可以通过数据库链接进行。

在典型的应用场景中，Oracle企业安全管理器用于在遵循LDAP协议的OID服务器中创建有效的应用程序用户。X.509证书机构负责在Oracle Wallets（通过Oracle电子钱包管理器）中创建私有秘钥对，并将它们发布到OID服务器。如果一个用户期望登录数据库服务器，他必须拥有一个公钥证书和一个私钥。这两件东西通常保存在用户密码保护的电子钱包中，而电子钱包则保存在LDAP目录中。当用户在客户端设备中额秘钥被发送到数据库服务器之后，数据库服务器会用它和借助SSL从LDAP目录中获取的秘钥进行比较，如果匹配，该用户就被认证通过，可以继续访问数据库。

## 12、加密

有时候，你可能需要采取额外的步骤对数据库中的数据进行机密，保护它们不被未经授权的用户访问。

目前有几个Oracle发布都支持数据加密。Oracle 10g包含恶一个名为透明数据加密的重要新特性。在引入这个特性之前，存储在Oracle数据库中的加密数据在使用之前必须由应用程序解密。这就会带来许多限制，最突出的问题就是需要应用程序来完成数据的解密。

有了透明数据加密特性之后，数据库可以自动完成数据的加密和解密工作。发往数据库的数据由Oracle来加密，有数据库出去的数据自动被解密；不需要应用程序做额外的编码，即用户可以加密现有的数据而不需要修改自己的SQL语句。

Oracle 11g允许用户使用透明数据加密特性对整个表空间进行加密；另外，该特性也减少了管理的开销。

## 13、安全备份

前面几节描述的安全特性为用户提供了几种保护Oracle数据库中数据安全性的工具。但是当数据离开了Oracle数据库（例如，当用户在执行备份数据的必要步骤时），又会怎样？

最近发生的事件表明丢失备份磁带是真实存在的情况，备份磁带可能会被偷。安全备份这个特性，它可以自动加密备份数据。而经过加密的数据只能由源数据库解密，这样一来，即便是备份磁带丢失或者被偷，拿到磁带的人也无法看到这些数据。

## 14、审计

Oracle数据库允许用户保护自己有价值的数据不被他人未经授权的访问。然而，数据库的安全性和它的实现一样，做到尽可能的好，但是人都是会犯错的。另外，管理员也希望能够掌握在数据上执行过哪些类型的操作，不论这些操作是否合法。通过审计数据库可以解决上面的两个问题。

Oracle的审计功能允许用户跟踪整个数据库或者特定用户在语句级别、权限级别以及模式对象级别的行为。审计功能还会收集数据库活动相关的数据用于规划和调优。在默认情况下会对使用管理员权限连接数据实例以及数据库的启动和关闭进行审计。

管理员也可以在用户级别审计会话，即捕捉一些基本但又特别有用的统计信息，比如：逻辑I/O的数目、物理I/O的数目以及登录的总时长等。正如前面章节所述，收集性能统计的开销比较低；Oracle 10g及之后的版本能够自动收集统计信息，并把它们存储在自动工资符合仓库（AWR）中。

审计记录通常包括下面的信息：

* 用户名
* 会话标识符
* 终端标识符
* 访问的模式对象名
* 执行或尝试执行的操作
* 操作的完整代码
* 日期和时间戳

这些记录可能被存储在数据字典表（SYS模式的AUD$表）中，这又叫做数据库审计跟踪或操作系统审计跟踪。

Oracle 9i增加了细粒度的审计功能，它使得管理员可以根据访问的特定列绑定变量对SELECT语句执行选择性的审计。Oracle 10g为细粒度审计增加了扩展的SQL支持。现在管理员可以通SQL语句对查询以及UPDATE、INSERT和DELETE操作进行细粒度审计。

在Oracle 11g中，审计功能默认被打开，AUDIT\_REAIL初始化参数被设置成DB。被审计的权限包括：

* ALTER ANY PROCEDURE
* ALTER ANY TABLE
* ALTER DATABASE
* ALTER PROFILE
* ALTER SYSTEM、ALTER USER
* AUDIT SYSTEM
* CREATE ANY JOB、CREATE ANY LIBRARY、CREATE ANY PROCEDURE、CREATE ANY TABLE、CREATE EXTERNAL JOB、CREATE PUBLIC DB LINK、CREATE SESSION、CREATE USER
* DROP ANY PROCEDURE、DROP ANY TABLE、DROP PROFILE、DROP USER
* EXEMPT ACCESS POLICY
* GRANT ANY OBJECT PRIVILEGE、GRANT ANY PRIVILEGE以及GRANT ANY ROLE

## 15、依从性

有个标语“信任，但要核查”，用来形容安全和审计的功能最确切不过。加上依从性，这个标语可扩展为“信任，核查，并证明之”，依从性讲的是工具需要证明自己对数据的使用是正当的。

依从性是以前面几节讲述的安全和审计特性为基础的。对于大多数情况而言，依从性是将一个新的元素——政府要求——引入公司范畴的结构。在美国以及其他地方，依从性日益成为政府法规所要求的特性，因而Oracle数据库很容易具有依从性这一点非常重要。对于许多组织而言，依从性是非常关键的，负责保证依从性的人员未必属于IT部门。因此，安全和审计模式的实施必须被简化，必须相互合作来满足依从性要求。

Oracle提供了两个专门设计用来解决依从性挑战的选项——Oracle数据Vault和Oracle审计Vault，后面将会对它们进行描述。其中还会涉及到Flashback数据归档能力。

### 15.1Oracle数据Vault选项

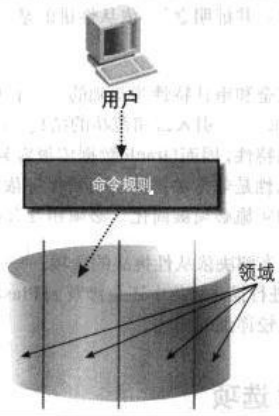
该选项2006年引入，它用于限制DBA以及其他权限较高的用户访问他们不该访问的数据。它也可用于限制应用程序的DBA操作数据库和访问其他的应用程序。安全管理员可以使用Oracle数据库Vault选项来描述组织期望实施的安全模式，而且这个选项可以使用本章前面描述的特性自动实施安全模式。

Oracle数据库Vault选项中定义的关键参数叫做因子。一个因子本质上是一个描述的尺度，它将会影响整个数据库的安全。这些因子包括特定的应用程序、位置以及每天的次数等。这个选项本身定义了40多个因子，用户可以创建自己的因子。

因子用于定义访问和审计特定安全尺度。可以创建规则限制对特定因子的访问类型，也可以定义规则及将多个因子规则结合在一起。一旦定义了规则集，便可以根据规则集创建应用角色，也可以创建命令规则根据规则的计算结果控制数据库命令的执行。例如，可以组织任何人删除特定的表。除非这个命令来自因子定义的特定位置，或者指定定义新用户必须由两位管理员同时操作。

规则也可用于定义数据库领域。数据库领域由管理员可以管理的模式和角色的子集组成。当一个组织需要使用Oracle数据库来服务于多个团体的时候，这种能力是基本的要求。管理员可以定义一个领域，并将管理员权限赋予该领域，而不会危及其他模式中数据的安全。领域的整体效果就是允许对管理职责进行安全拆分。

审计所有规则的执行是Oracle数据库Vault选项的一部分工作，它还负责提供完整的依从性所要的文档。如图显示了Oracle数据库Vault选项解决方案的各个组成部分：



### 15.2Oracle审计Vault服务器

2007年引入的Oracle审计Vault服务器负责收集Oracle和底层操作系统中审计文件里的数据。它将这些数据并入安全仓库中，并提供开箱即用的依从性报表。这个报表包含特权用户的访问、账目管理、数据访问以及失败的登录尝试等信息。这些数据存储在Oracle数据仓库模式中。

由于Oracle审计Vault服务器能够监控所有到达的审计数据，因而它可以根据IT策略产生告警。从Oracle 9i开始，Oracle数据库都可以被监控。管理员可以使用软件开发工具集（SDK）来构建定制的审计信息收集器。

### 15.3Flashback数据归档

Flashback技术基于回滚段。尽管Flashback最初是由Oracle 9i引入，但是Oracle 11g为Flashback提供了一个特殊的用法，即用它来解决依从性的问题。

Flashback数据归档特性使得数据库管理员可以看到是记录在整个生命周期中的所有变化。这种类型的历史跟踪信息可以为证明依从性提供关键性的信息，也可用于追踪依从性或者用法的错误源头。