深入了解 Oracle Database Vault

公益讲座11：00准时开始，请大家先浏览云技术微信公众号技术文章。资料会在各群同步发布，已入群客户请勿重复入群!

20-22

数据库和云讲座群

甲骨文云技术公众号

B站专家系列课程

* 活动最终解释权归甲骨文公司所有

立即扫码进行 1V1 免费咨询

2023 年 10 月，MySQL 5.7 将终止官方支持和更新。

立刻升级至更快、更稳定、更安全的 MySQL 8.0 / MySQL Database Service，获取 300+ 项新特性，使开发更加灵活和高效，更好的满足业务发展需求。

免费咨询热线：

400-699-8888

深入了解 Oracle Database Vault
数据库保险库（DV）

甲骨文技术公益课 - 数据库专场

2023 年 10 月 20 日 11:00

线上直播

Jim Kong

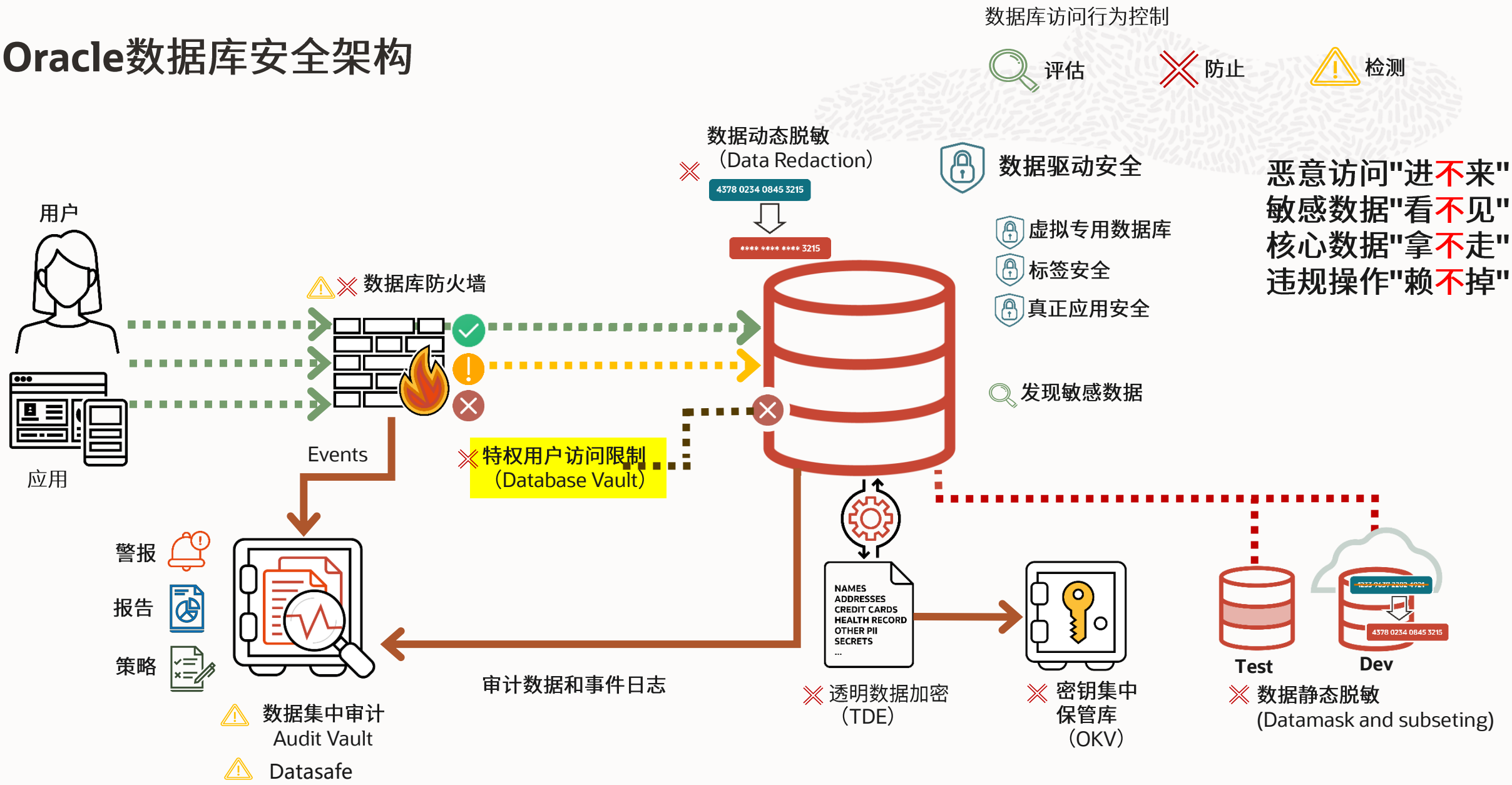
内容

深入了解Oracle数据库保险库(Database Vault)

- 概述
- 数据库保险库用例
- 动手实验
- 使用指南
- FAQ

概述

Oracle数据库安全架构



数据安全实战演练系列—往期内容

【Oracle 公益课堂】深入了解Oracle Key Vault密钥保险箱

365 9-8

【Oracle 公益课堂】深入了解Oracle动态数据脱敏

481 8-25

【Oracle 公益课堂 】深入了解Oracle审计仓库和数据库防火墙

487 8-4

【Oracle 公益课堂 】Oracle透明数据加密(TDE)

711 6-30

https://space.bilibili.com/28628293/channel/seriesdetail?sid=3509649

免费咨询热线：400-699-8888

陌生人进入房间的多种方法

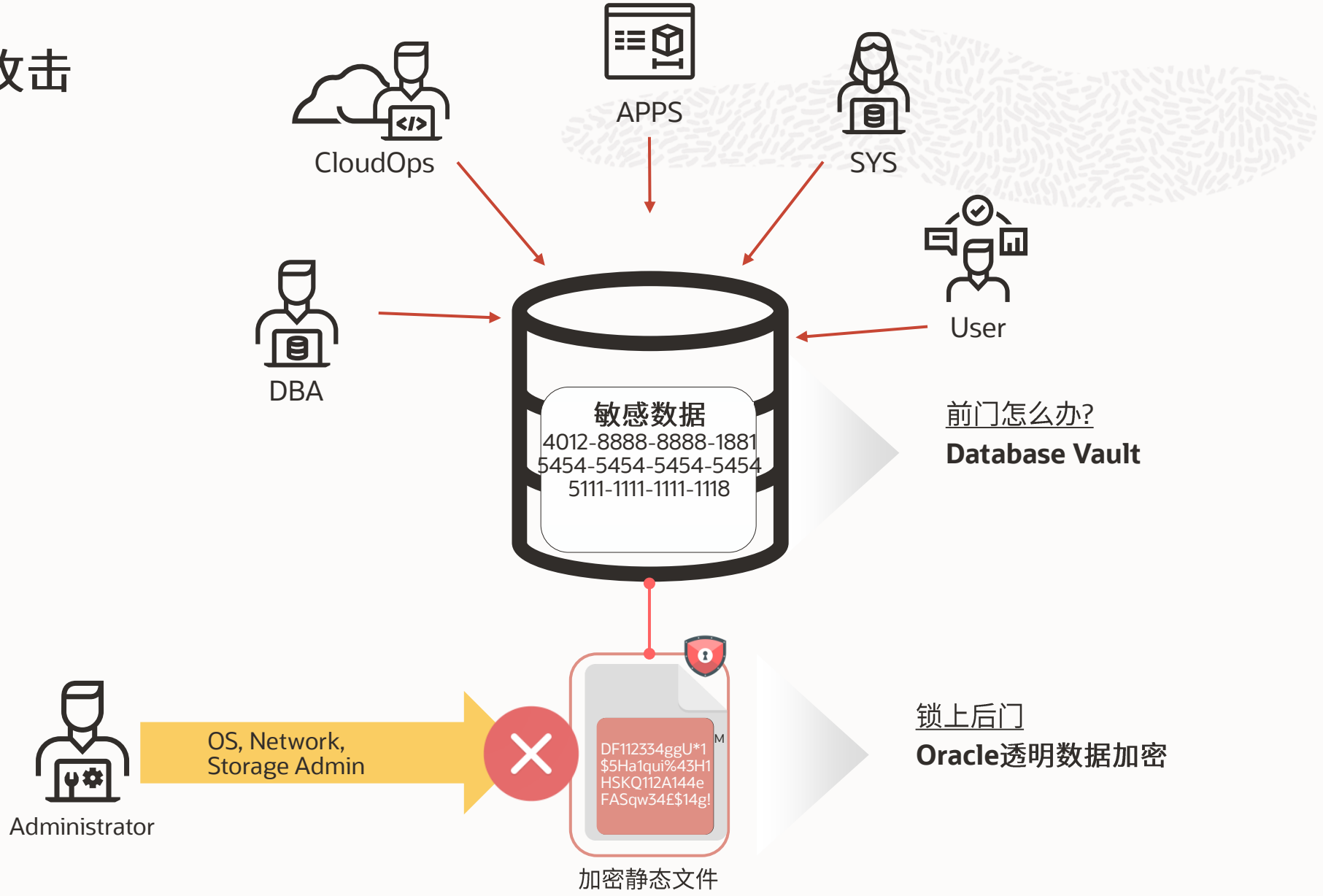
从后门偷偷溜进

从烟囱爬进

打破窗户爬进去

敲门并从前门进入

防范特权用户的攻击
在数据库中



什么是Oracle数据库保险库

提供控制措施，以防止未经授权的特权用户访问敏感数据或进行未经授权的数据库更改。

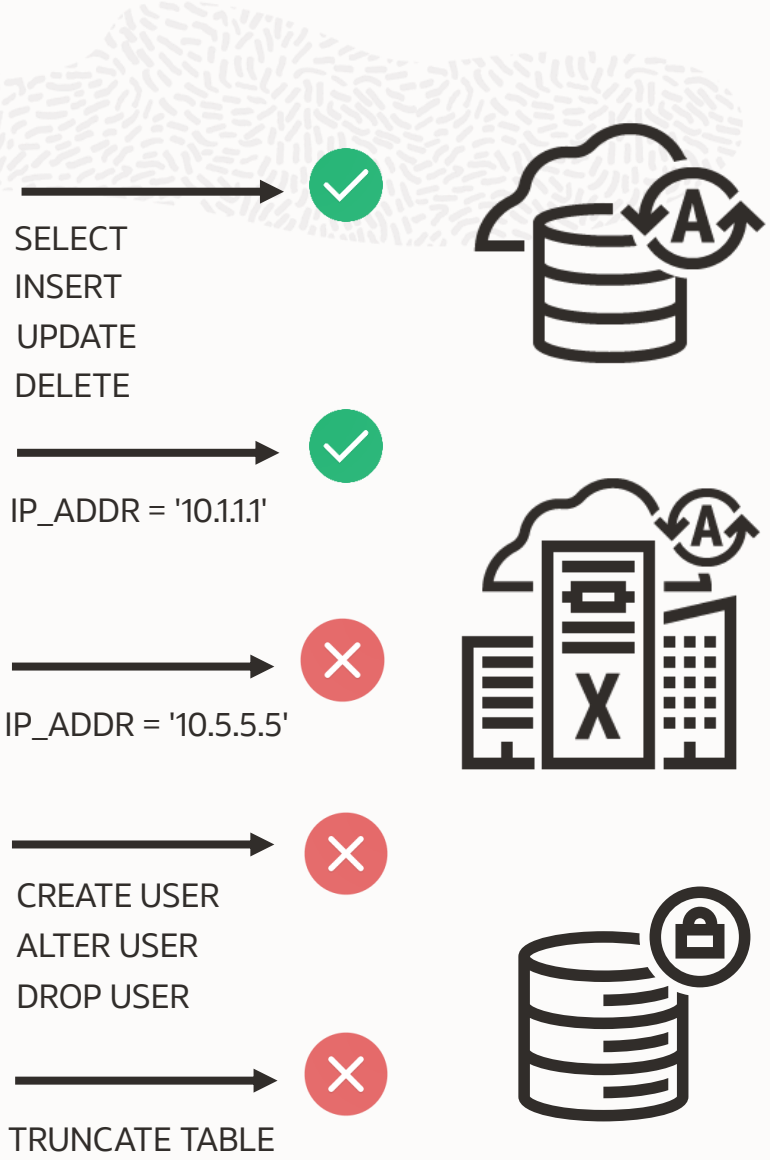
Oracle 数据库企业版的一个选项

也可应用在其他Oracle数据库服务中

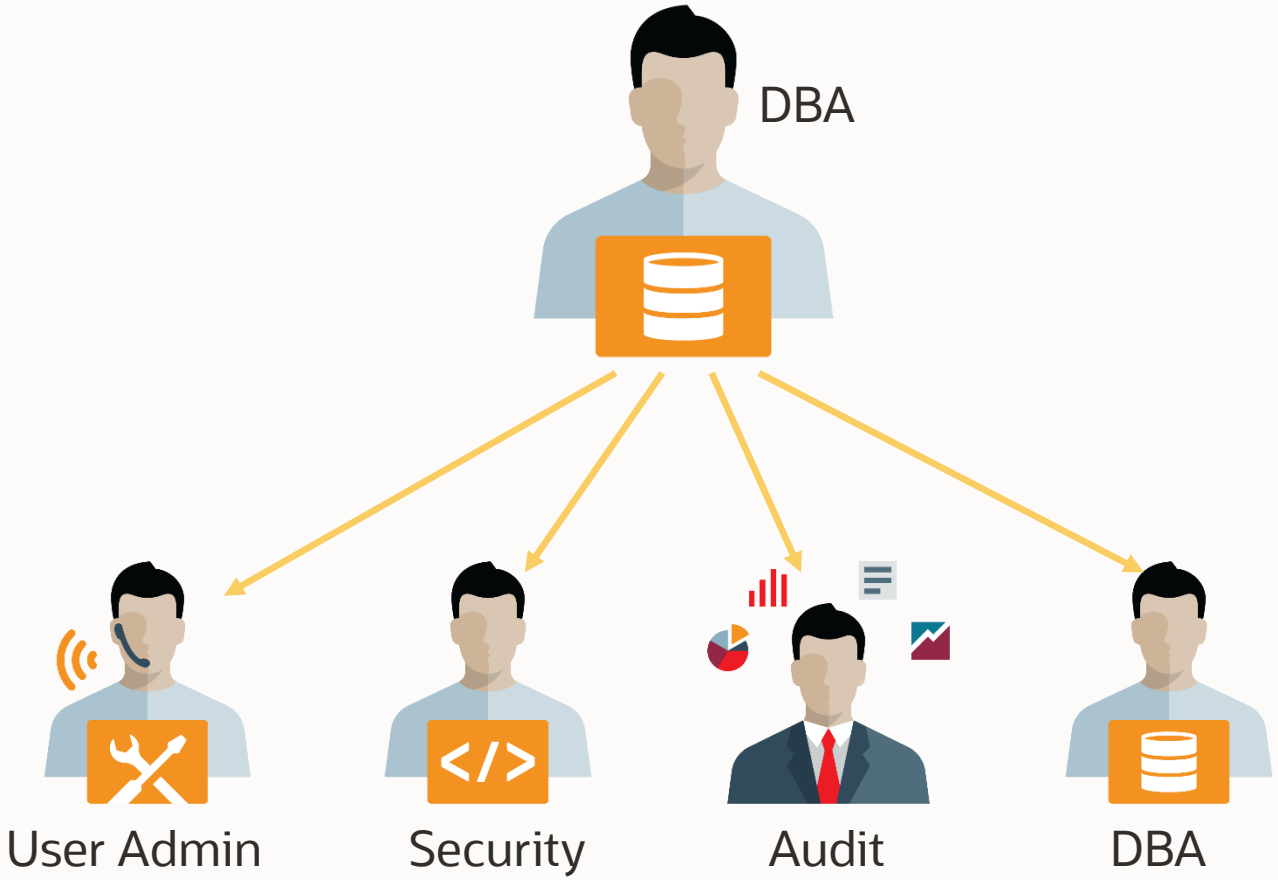
- Autonomous Databases
- Exadata Cloud Service
- Exadata Cloud@Customer
- 高/极限性能 Oracle 基础数据库系统

当合规性或法规要求限制对敏感数据的访问或实施职责分离时，可以提供协助

- 分离用户帐户、数据库管理和数据管理



职责分离



- 数据库保险库职责分离包括
  - 用户管理（dv_acctmgr 角色）
  - 安全管理（dv_admin 角色）
  - 审计管理（dv_audit_cleanup 角色）
  - 数据库管理（dba 角色）
- 根据需要，职责分离可以放宽或扩展

数据库保险库组件

领域(Realms)

- 领域是数据库内部的一种保护区域，用于保护数据库schema、对象和角色。
- 访问受领域保护的对象需要领域授权（所有者或参与者）

命令规则（Command Rules）

- 控制用户如何执行SQL语句，包括SELECT、ALTER SYSTEM、DDL、DML和DCL。
- 必须与规则集相关联，以确定是否允许执行SQL语句

规则集和规则（Rule Sets & Rules）

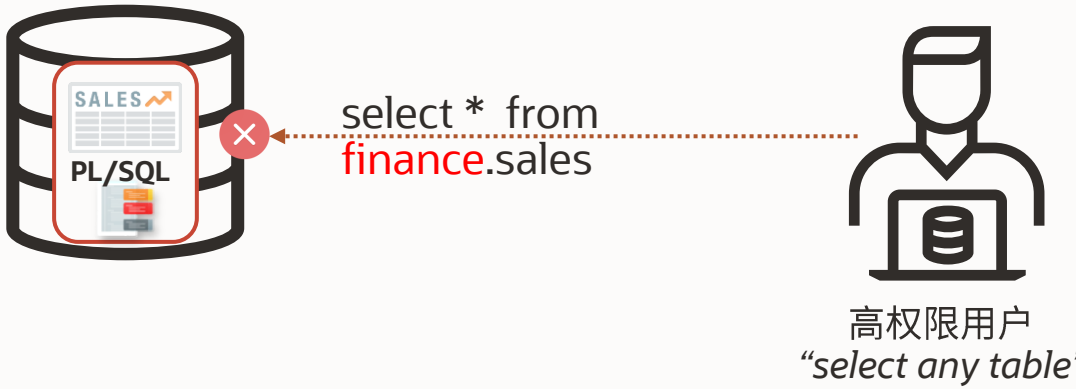
- 规则集是包含一个或多个规则的集合，可以与领域授权、命令规则、因子分配或安全应用角色相关联。规则集中的规则是一个评估为真或假的PL/SQL表达式。

安全应用角色（Secure Application Roles）

- 一种特殊的Oracle数据库角色，可以基于规则集的评估进行启用。

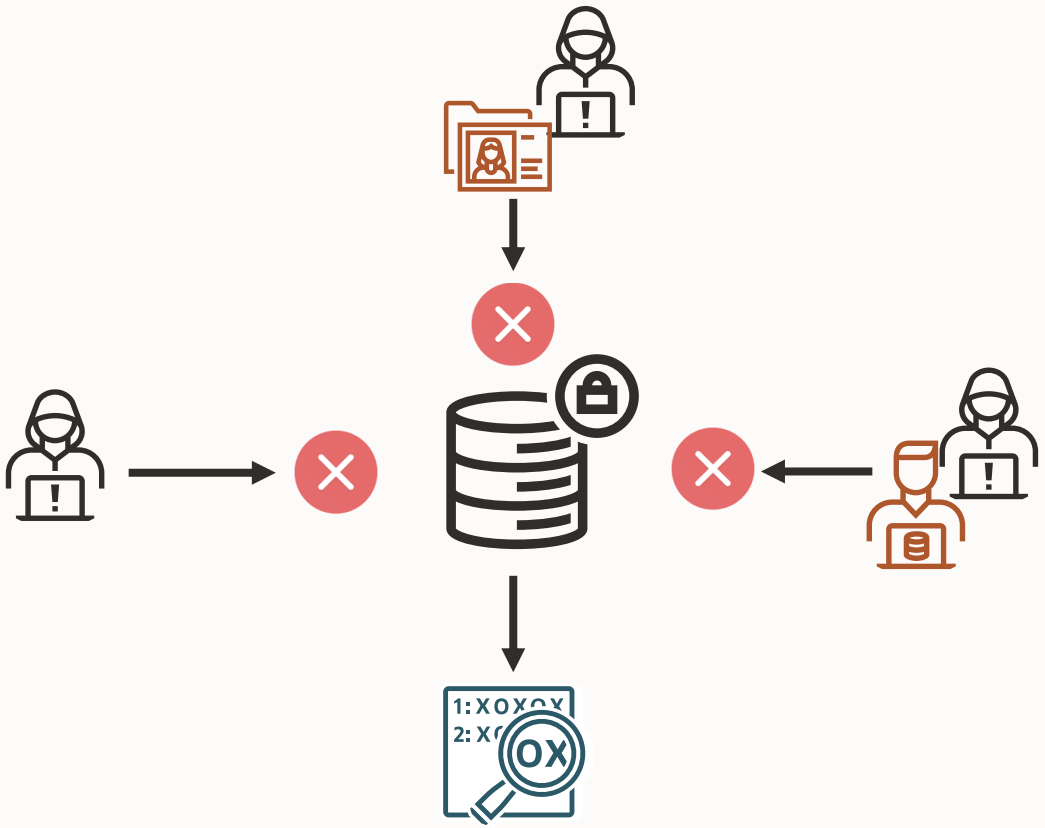
因子（Factors）

- 因子是一种具有名称的变量或属性，如用户位置、数据库IP地址或会话用户，数据库保险库可以识别和使用。



数据库保险库用例

为数据库提供强大的访问控制



1. 防止特权用户或应用账户被滥用
2. 限制对敏感应用数据的访问,只有通过授权才可以
3. 限制在维护窗口期才能对生产数据库进行更改
4. 强制执行职责分离
5. 获取高价值的审计数据

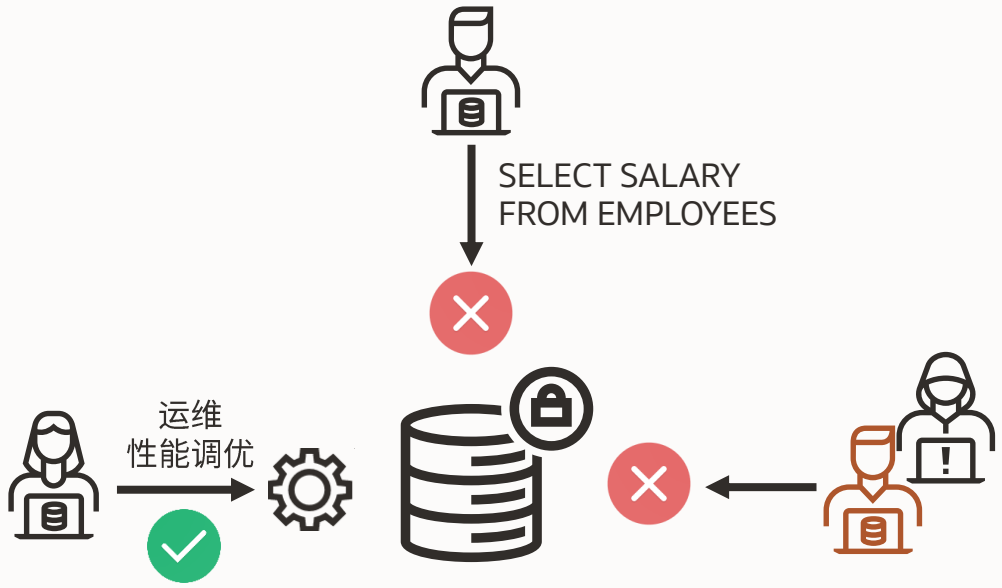
1.防止特权用户被滥用

问题

- 特权用户账户是网络攻击者的主要目标，可以访问数据库中的任何数据
- 特权用户可能会因社交媒体应用程序而成为网络钓鱼攻击的目标
- 特权用户可能会窥探敏感数据（如医院的重要患者信息、未发布的财务数据、工资信息和知识产权等）

解决方案

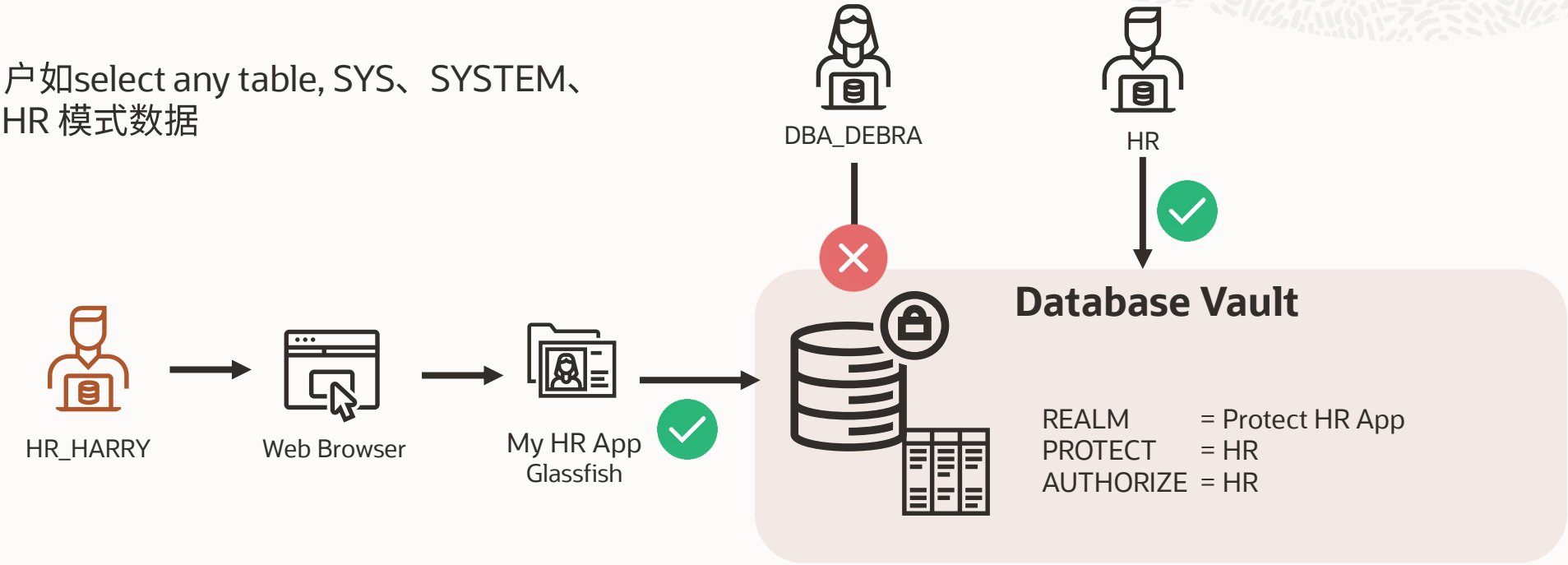
- 数据库保险库领域（realms）保护敏感数据
- DBA 仍然可以执行日常运维工作，但无法访问敏感数据
- 合规条款要求对敏感数据访问实施强大的控制措施



2.使用Oracle数据库保险库来保护应用程序数据

目标

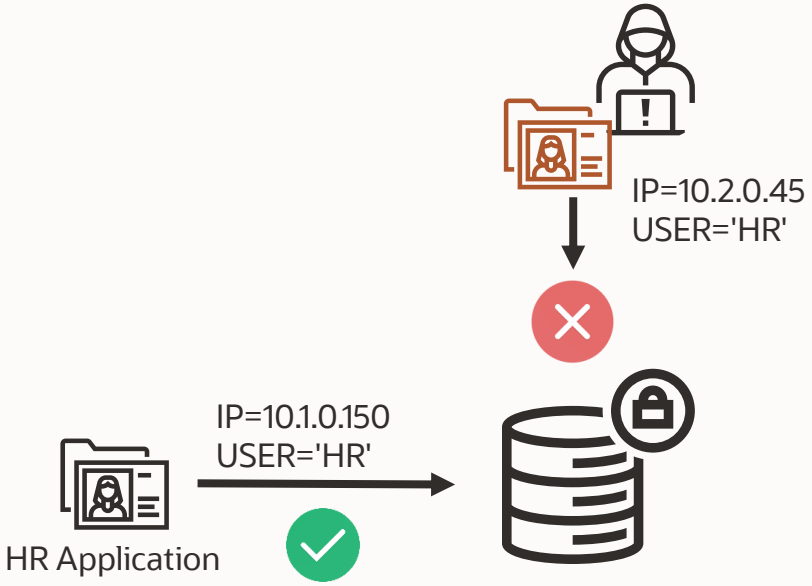
- 防止特权用户如select any table, SYS、SYSTEM、DBAs 访问 HR 模式数据



其他信息

IP = 10.0.0.150
USER = HR
TABLES = HR_APP_USERS (HR_HARRY)
HR_EMPLOYEES (SALARY)

将对敏感数据的访问限制在适当的应用程序上



问题

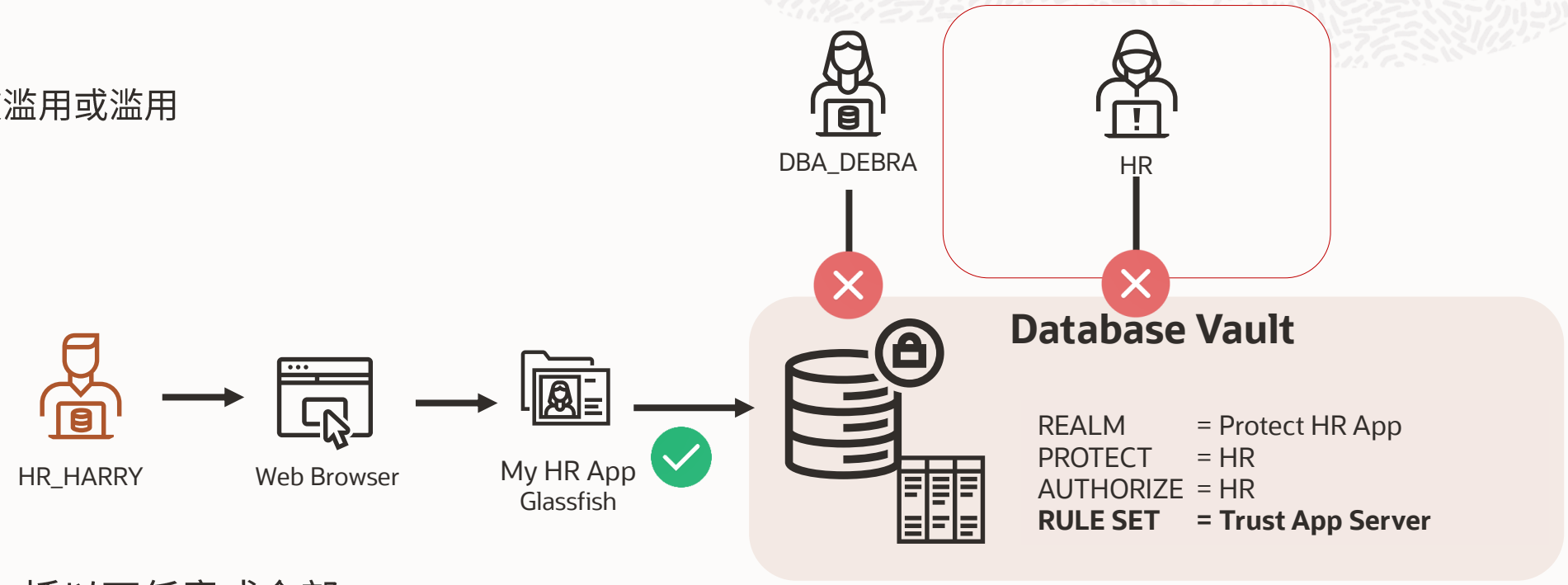
- 应用程序经常以弱混淆或明文方式存储访问凭证（密码，秘钥）
- 网络攻击者会使用窃取的帐户凭证，达到他们获取敏感数据的目的

解决方案

- 使用数据库保险库将访问限制仅限于应用程序服务
- 如果没有授权，窃取的凭证会毫无价值

保护应用密码被误用

目标
- 防止应用程序被滥用或滥用



规则集因子可以包括以下任意或全部
- 应用服务器IP地址
- 应用服务器主机名
- 时间
- 程序连接（例如，JDBC Thin客户端）
- 数据库用户和操作系统用户

环境信息

IP = 10.0.0.150
USER = HR
TABLES = HR_APP_USERS (HR_HARRY)
HR_EMPLOYEES (SALARY)

3.恶意用户禁用或意外修改

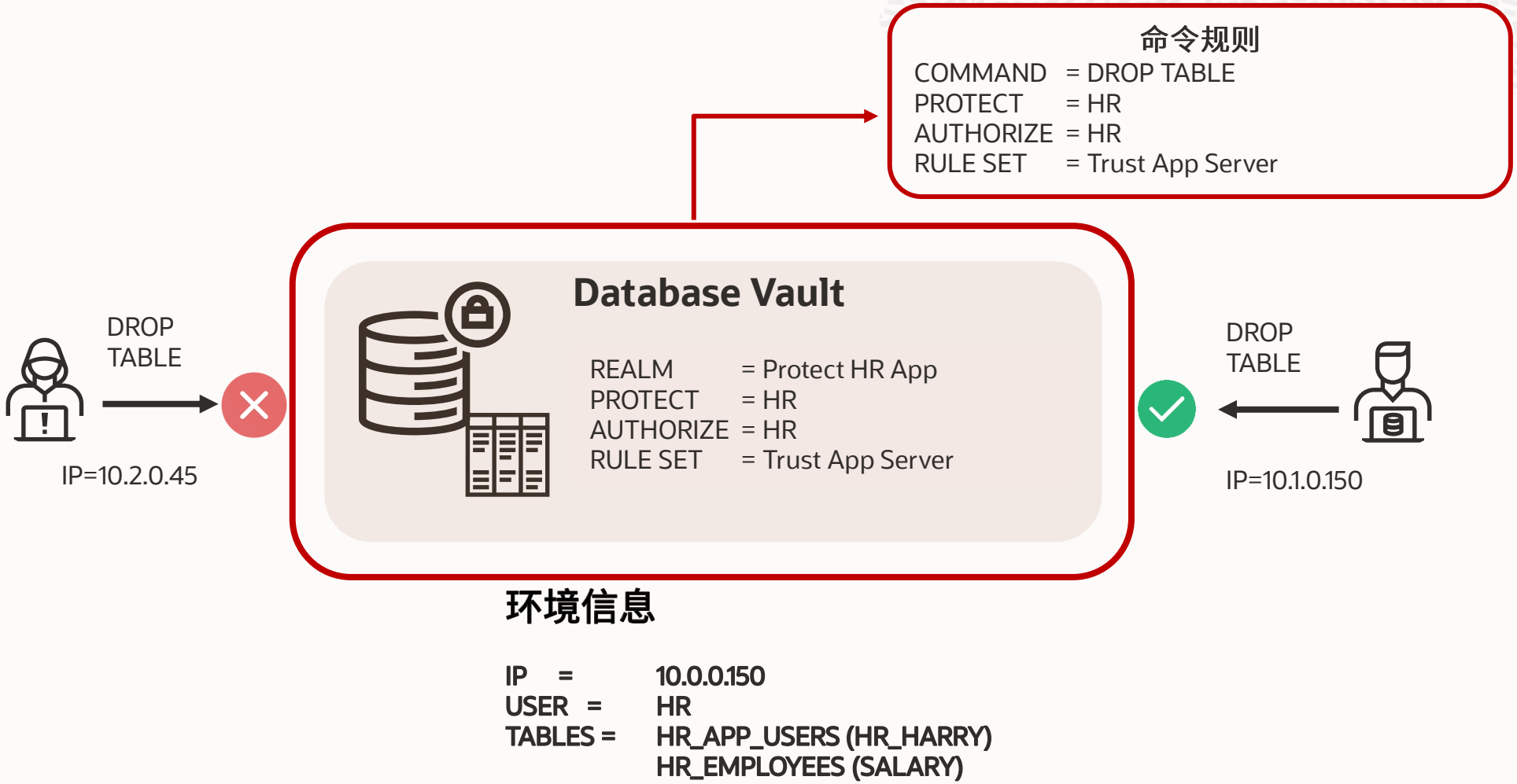
恶意用户可以禁用数据库，对schema或数据进行更改

特权用户可能没有意识到他们在生产环境上执行了错误的命令或运行了导致错误的脚本

解决方案

- 领域（Realms）防止特权用户访问数据
- 命令规则（Command Rules）阻止对数据库、表或数据的更改
- 规则集（Rule Sets）为领域或命令规则添加上下文授权条件

示例：防止执行 DROP TABLE 命令



避免在业务运行时间内的更改

在维护时间窗口之外进行的更改影响业务运营或系统性能

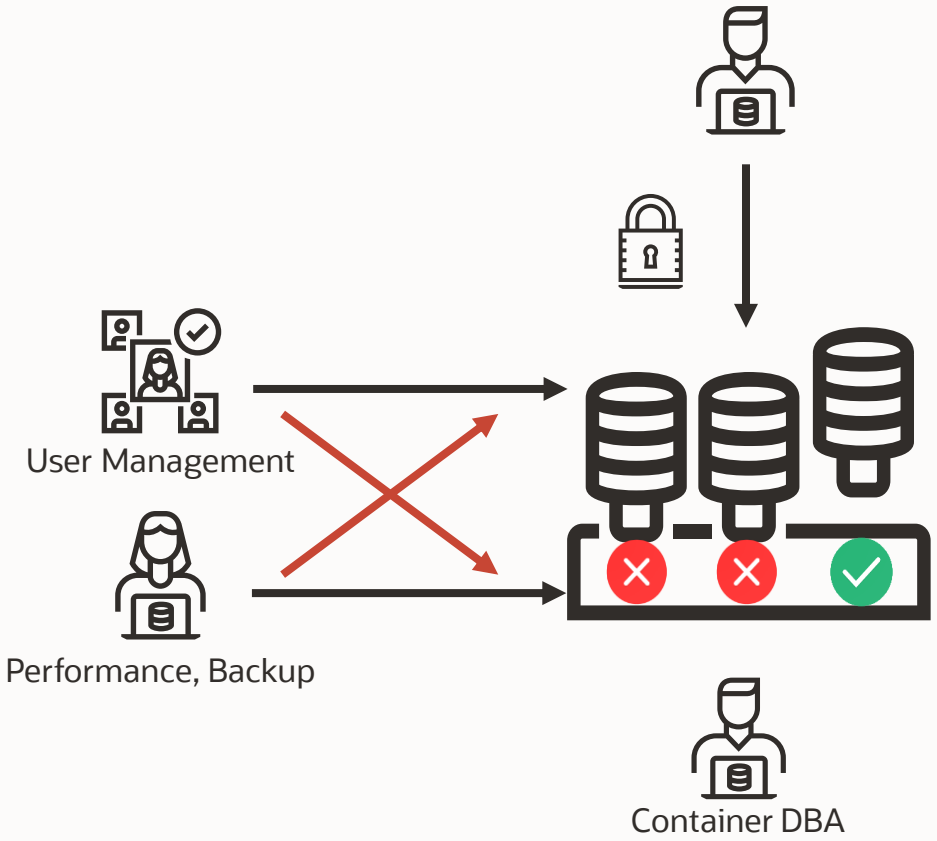
解决方案：

- 领域（Realms）和命令规则（Command Rules）允许您添加规则集，用于基于上下文的授权条件。
- 条件由你任意选择

创建规则:

extract(hour from systimestamp) between 6 and 18

4.强制执行职责分离



问题

- 特权用户拥有对数据、安全控制和审计日志的完全访问权限
- 特权用户凭据的丢失使攻击者能够访问授予该用户的所有资源

解决方案

- 数据库保险库强制执行职责分离，而不仅仅通过组织策略
  - 安全管理员
  - 数据库管理员
  - 数据管理员
  - 用户管理员
- 数据库保险库运营控制允许容器DBA执行管理任务而无需访问数据。

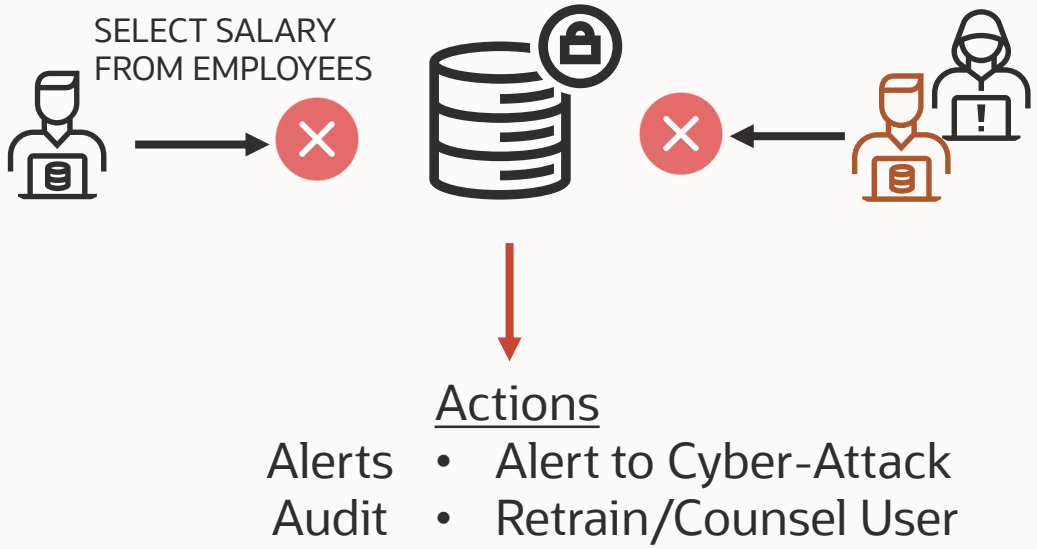
5.获取可操作的警告

问题

- 警告经常被忽视，因为要么毫无意义，要么不可操作。

解决方案

- 数据库保险库对于错误/故障的审计
  - 早期的攻击者探测
  - 内部人员需要采取纠正措施



动手实验

实验内容

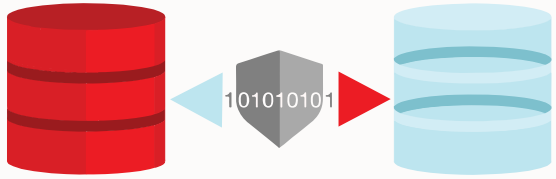
1. 如何启用数据库保险库
2. 如何创建领域
3. 如何配置可信路径
4. 如何使用模拟模式
5. 如何启用运维控制

使用指南

Oracle 数据库保险库使用策略

单实例环境

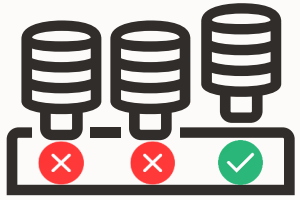
RAC环境



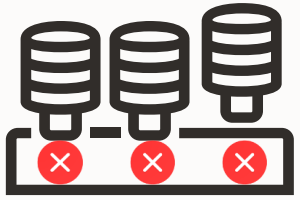
Data Guard环境

在单实例上启用DV

DV management by CDB



DV management by PDBs



DV management via Ops Control

DV_OWNER角色的用户
dbms_macadm.enable_dv;

As SYSDBA or SYSOPER
重启

数据库保险库 – 用户配置文件

Oracle建议创建不会锁定的数据库用户配置文件

具有DV_OWNER或DV_ACCTMGR权限的用户应被视为服务帐户，不应该因密码尝试失败而自动锁定或永久锁定。

该示例在5次登录尝试失败后会暂时锁定账户1分钟。

容器用户配置文件

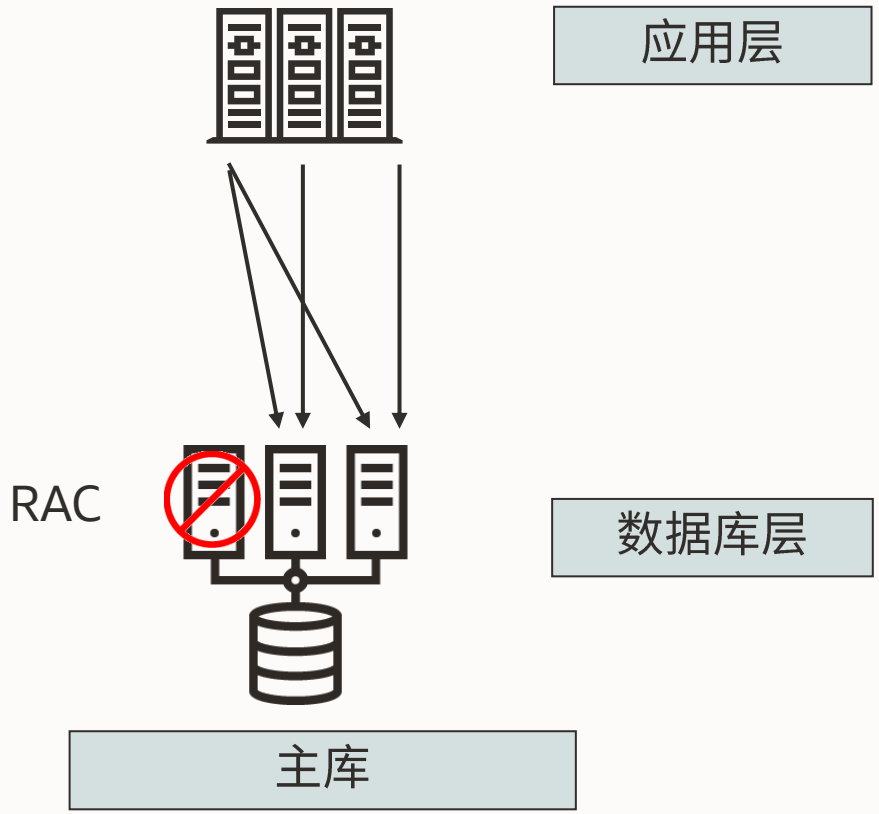
```
CREATE PROFILE C##DV_PROFILE LIMIT
  FAILED_LOGIN_ATTEMPTS 5
  PASSWORD_VERIFY_FUNCTION ora12c_verify_function
  PASSWORD_LOCK_TIME 1/1440
  CONTAINER=all;
```

本地用户配置文件

```
CREATE PROFILE DV_PROFILE LIMIT
  FAILED_LOGIN_ATTEMPTS 5
  PASSWORD_VERIFY_FUNCTION ora12c_verify_function
  PASSWORD_LOCK_TIME 1/1440;
```

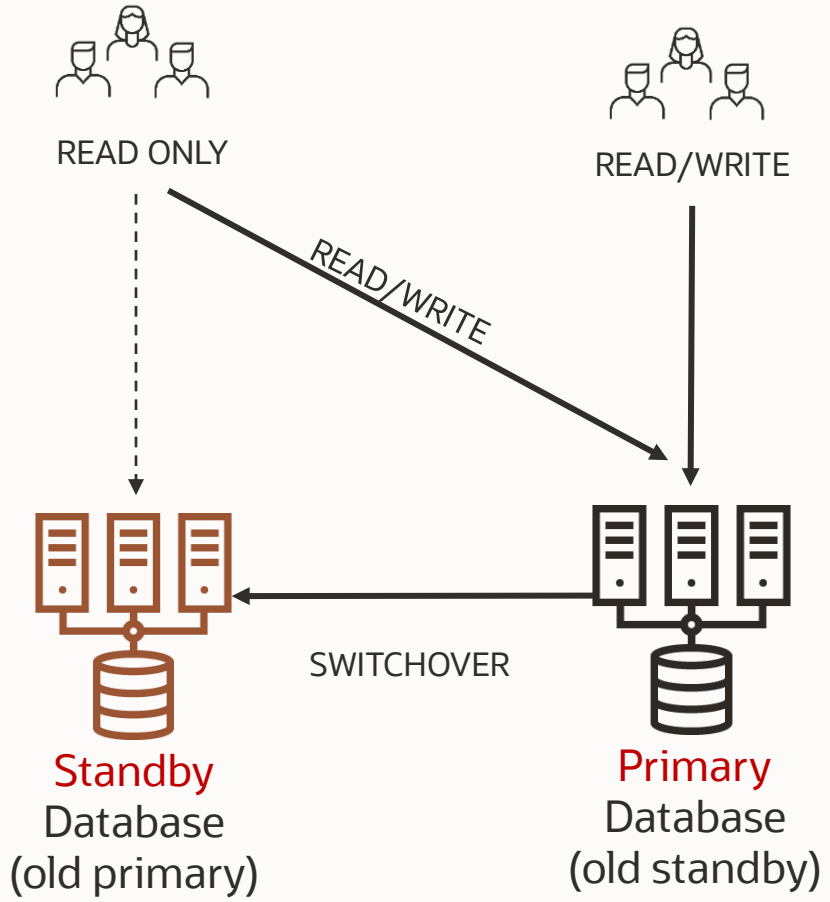
Oracle Real Application Clusters (Oracle RAC)

数据库保险库滚动启用



- 执行与单实例数据库相同的配置和启用步骤
- 按照MAA（Maximum Availability Architecture）计划的维护步骤进行操作
  1. 数据库服务重定位
  2. 服务在其他RAC实例上运行
  3. 连接到服务的会话被逐渐关闭
  4. 新的会话连接到其他实例上的服务
  5. 数据库请求的结果返回给用户
  6. 维护活动可以在第一个节点上开始（逐个滚动进行）

Data Guard环境启用数据库保险库



- Data Guard 是一种容灾解决方案，具有从备库读取数据的能力。它不像 RAC 那样是一个纯粹的高可用性解决方案

  执行与单实例数据库相同的配置和启用步骤

  在主库启用DV之前，先在备用数据库上启用数据库保险库

  在计划的主备切换操作期间，在“原主库”上启用DV

数据库保险库- 数据导入导出

- DB Data Pump是一个高度可信的程序，用于从Oracle数据库导出和导入数据和元数据。
- 除非经过特定授权（对DB、模式或表），否则数据库保险库会阻止Data Pump活动

```
CREATE USER dpuser IDENTIFIED BY Oracle123;
GRANT EXP_FULL_DATABASE TO dpuser;
```

→

```
expdp userid=dpuser/Oracle123@pdb1 ...
impdp userid=dpuser/Oracle123@pdb1 ...
```

```
ORA-39327: Oracle Database Vault data is being stored unencrypted in dump file set.
ORA-31685: Object type USER:"HR" failed due to insufficient privileges.
ORA-39126: Worker unexpected fatal error in KUPW$WORKER.FETCH_XML_OBJECTS [ORA-01031: insufficient privileges
ORA-47410: Realm violation for GRANT on CREATE SESSION / UNLMITED TABLESPACE / RESOURCE / etc...
```

```
SQL> desc DBMS_MACADM
...
PROCEDURE AUTHORIZE_DATAPUMP_USER
 Argument Name    Type       In/Out Default?
 ---------------- ---------- ------ --------
 UNAME            VARCHAR2   IN
 SNAME            VARCHAR2   IN     DEFAULT
 OBJNAME          VARCHAR2   IN     DEFAULT
 ACTION           VARCHAR2   IN     DEFAULT
```

→ `exec dbms_macadm.authorize_datapump_user('DPUSER');`

→ `exec dbms_macadm.authorize_datapump_user('DPUSER','HR');`

```
exec dbms_macadm.AUTH_DATAPUMP_CREATE_USER('DPUSER');
exec dbms_macadm.AUTH_DATAPUMP_GRANT('DPUSER');
exec dbms_macadm.AUTH_DATAPUMP_GRANT_ROLE('DPUSER');
```

→ `exec dbms_macadm.authorize_datapump_user('DPUSER','HR','EMP');`

数据库保险库 – 打补丁和升级

在19c中对开启数据库保险库的数据库进行打补丁和升级非常简单:

1. 参数授予DV_PATCH_ADMIN权限给SYS用户
2. 打补丁或升级
3. 从SYS用户中撤销DV_PATCH_ADMIN权限

```
wget --http-user=<MOS Username> --ask-password --no-check-certificate \
 --output-document=<patch_name.zip> \
 "https://updates.oracle.com/Orion/Download/download_patch/<patch_name.zip>"
```

下载补丁

```
unzip <patch_name.zip>
```

解压

```
grant DV_PATCH_ADMIN to SYS CONTAINER=ALL;
```

授予DV_PATCH_ADMIN角色

```
opatch prereq CheckConflictAgainstOHWithDetail -ph ./
...
opatch apply
...
./datapatch -verbose
...
@?/rdbms/admin/utlrp.sql
```

开始升级步骤

```
revoke DV_PATCH_ADMIN from SYS CONTAINER=ALL;
```

撤销DV_PATCH_ADMIN角色

数据库保险库 - RMAN 恢复表或schema

在默认情况下，在启用Oracle数据库保险库的环境中，RMAN表或schema恢复操作将被数据库保险库阻止，因为这个过程需要使用Data Pump、数据库字典，以及潜在的受领域或命令规则保护的对象（如HR.EMPLOYEES等）

问题

```
ORA-39327: Oracle Database Vault data is being stored unencrypted in dump file set.
ORA-31685: Object type USER:"HR" failed due to insufficient privileges.
ORA-39126: Worker unexpected fatal error in KUPW$WORKER.FETCH_XML_OBJECTS [ORA-01031: insufficient privileges
ORA-47410: Realm violation for GRANT on CREATE SESSION / UNLMITED TABLESPACE / RESOURCE / etc...
```

解决

```
grant DV_PATCH_ADMIN to SYS;
exec DVSYS.DBMS_MACADM.ADD_AUTH_TO_REALM(realm_name => 'HR Tables', grantee => 'SYS', rule_set_name => null);
exec DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('SYS');
GRANT DV_DATAPUMP_NETWORK_LINK to SYS;
```

常见问题

常见问题1

问：Oracle数据库保险库如何提高安全性和合规性?

答：Oracle数据库保险库通过减少特权用户攻击的风险，这是最常见的网络攻击形式之一，来提高安全性。大多数合规性要求包括职责分离和防止对敏感数据的管理访问的控制。由于Oracle数据库保险库在数据库引擎内实施安全性，这些安全控件将始终存在，无论网络或服务器攻击源来自何处。

问：可以使用Oracle数据库保险库来满足Sarbanes-Oxley、PCI、HIPAA、ITAR和EU GDPR等合规性要求吗?

答：Oracle数据库保险库旨在帮助满足Sarbanes-Oxley、PCI、HIPAA、ITAR和EU GDPR等各种法规中的技术安全性要求。客户还需要遵循这些法规所要求的流程和程序。Oracle数据库保险库提供了强大的数据库内部控制，控制了应用程序数据可以由谁、何时、从何处以及如何访问。此外，Oracle数据库保险库还控制了对数据库可以进行哪些更改，有助于保持数据库的可用性和安全性。

问： 新的Oracle数据库保险库角色是否会改变我的数据库管理员今天的工作方式?

答： 大多数数据库管理员的任务不会发生变化。变化的一个领域是创建和管理用户和配置文件。这项与安全性相关的任务只能由具有DV_ACCTMGR角色的用户执行。此外，可能会暴露敏感数据的任务，如Datapump和作业调度，需要来自具有DV_OWNER角色的帐户的单独授权。

常见问题2

问：小型组织如何使用 Oracle Database Vault 完成职责分离

答：Oracle Database Vault 提供的额外角色（DV_OWNER , DV_ACCTMGR等），分别分配不同的管理员。这些管理员与数据库管理员是分开的。然而，在小型组织中，可能不容易实现这种分离。在这种情况下，同一个人可以管理多个拥有这些角色的用户。这有助于减小被恶意用户攻击，窃取其中一个帐户所造成的影响。

问： 如何将Oracle数据库保险库安全策略从开发系统移植到生产系统?

答：有两种方法可以实现这一目标：

Oracle Enterprise Manager允许您将Oracle数据库保险库安全策略从一个Oracle数据库移植到多个其他Oracle数据库。

Oracle Enterprise Manager还允许您从现有安全策略生成Oracle数据库保险库API脚本。然后，您可以在任意数量的目标Oracle数据库上编辑和运行此API脚本以创建相应的安全策略。

* 活动最终解释权归甲骨文公司所有

立即扫码进行 1V1 免费咨询

2023 年 10 月，MySQL 5.7 将终止官方支持和更新。

立刻升级至更快、更稳定、更安全的 MySQL 8.0 / MySQL Database Service，获取 300+ 项新特性，使开发更加灵活和高效，更好的满足业务发展需求。

免费咨询热线：

400-699-8888

数据库和云讲座群

20-22

甲骨文云技术公众号

技术专家1V1深入交流