三个久经验证的评估数据库安全态势的方法

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！

20-23

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

基于 Oracle 数据库
免费企业数据健康检查

- 及时了解数据库健康状况，发现并解决潜在问题
- 维护数据库系统良好状态，保护数据资产的安全
- 提升数据库性能、稳定性和安全性，降低业务风险

免费咨询热线：

400-699-8888

* 活动最终解释权归甲骨文公司所有

ORACLE

DatabaseWorld

at CloudWorld

保护您的数据

Secure your data

三个久经验证的评估数据库安全态势的方法

3 Proven ways to assess your Database Security Posture

张华

资深解决方案工程师

1-Apr-24

您不知道的安全隐患有哪些? What you don’t know can hurt you

数据库是否按照Oracle的优秀实践配置?Is the database configured according to Oracle’s best practices?

已经有哪些安全控制?What security controls are already in place?

我还可以使用哪些其他安全控制?What other security controls are available to me?

数据库中有哪些用户? What users are in the database?

用户有什么访问权限?What access do users have?

数据库中有哪些敏感数据? What sensitive data is in this database?

……

十大发现Top 10 findings

来自真实世界客户的数据库安全评估From real-world customer’s database security assessments

没有数据库安全策略No Database Security policies/strategy in place

没有打补丁/补丁管理策略No patching/patch management policy in place

没有按需定义账号；没有权责分离；过度赋权账号No personalized accounts; No separation of duties; Over-privileged accounts

没有加密机密/受管制的数据No encryption of sensitive/regulated data

没有监视/审计No monitoring/auditing in place

没有密码策略；弱密码管理No password policies; Weak password management

使用生产数据的非生产（开发/测试/培训）系统Non-Production (DEV/TEST/TRAINING) systems with production data

没有清除测试/示例账号No cleanup of test/sample accounts

没有匿名化的数据，发送给第三方No anonymization of data sent to third parties

没有操作系统加固No OS hardening

数据库安全评估工具（DBSAT）

Database Security Assessment Tool

用于快速执行数据库安全评估的命令行工具

Command-line tool for a quick database security assessment

在黑客来敲门之前评估您的数据库安全性Assess your database security before hackers come knocking

评估配置Assess Configuration

补丁Patches

数据加密Data Encryption

审核策略Auditing policies

操作系统文件权限OS file permissions

数据库配置Database configuration

监听器配置Listener configuration

细粒度访问控制Fine-grained access control

识别风险用户Identify Risky Users

数据库账号Database accounts

用户特权User privileges

用户角色User roles

发现敏感数据Discover Sensitive Data

哪些类型？在哪里？有多少？ What type, where, and how much?

基于希腊语、德语、荷兰语、法语、西班牙语、意大利语和葡萄牙语的数据模型的示例模式文件Sample pattern files for Greek, German, Dutch, French, Spanish, Italian, and Portuguese based data models

评估报告Assessment Reports

概要和详细信息Summary and detailed information

优先的、可操作的、目标明确的建议Prioritized, actionable and target specific recommendations

映射到欧盟GDPR, STIG和CIS基准Mapping to EU GDPR, STIG and CIS Benchmark

支持11g到23c Oracle数据库Runs on 11g to 23c Oracle Databases

安全规范参考基准 + OBP

CIS Center for Internet Security®

Creating Confidence in the Connected World.®

- **Internet 安全中心**是一个非盈利性实体，其任务是“确定、开发、验证、升级和维持针对网络防御的最佳做法解决方案”。 它借鉴了来自世界各地政府、企业和学术界网络安全及 IT 专业人员的专业知识。 为了制定标准和最佳做法（包括 CIS 基准、控制措施和强化映像），他们遵循一致的决策制定模型。
- **CIS 基准**是安全配置系统的配置基线和最佳做法。 每则指导建议都参考了一个或多个 CIS 控制措施，可帮助组织改进其网络防御能力。 CIS 控制措施与许多已建立的标准和规章框架对应，包括 NIST 网络安全框架 (CSF) 和 NIST SP 800-53、ISO 27000 系列标准、PCI DSS、HIPAA 等等。

STIGs

安全技术实施指南STIG(Security Technical Implementation Guides)

- 美国国防信息系统局（DISA）的一组配置基准。
- 提供了有关配置系统以满足在美国国防部 (DoD) IT 网络系统中部署的网络安全要求的指南。
- STIG 要求通过关注基础设施和网络安全并减少漏洞，帮助保护您的网络免受网络安全威胁

易用Easy as…

1 运行Run
./dbsat collect

2 运行Run
./dbsat report

3 运行Run
./dbsat discover

收集&报告

收集有关用户、角色、权限、安全配置和策略的元数据信息。生成安全评估报告。 Collects metadata information on users, roles, privileges, security configuration, and policies in place. Generates a Security Assessment report.

- **生成具有优先级发现的摘要输出**Generates summary output with prioritized findings

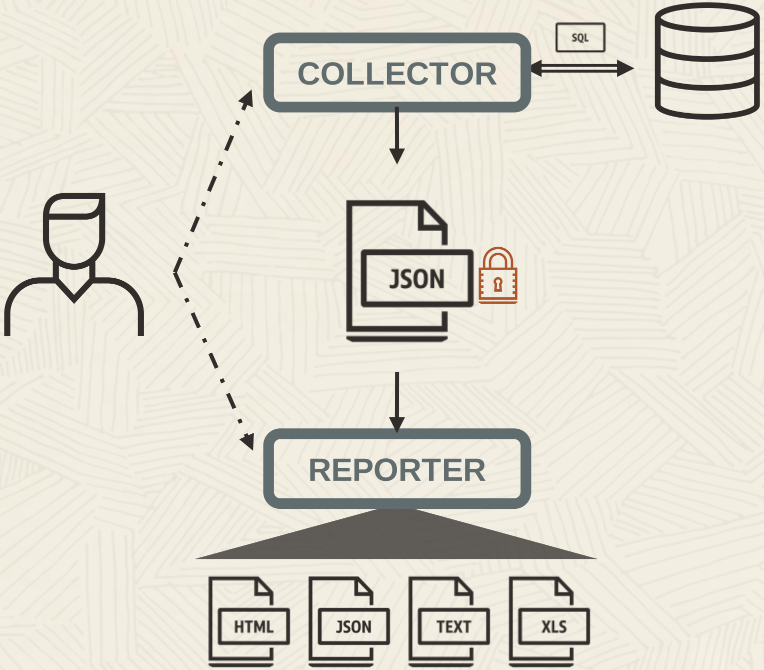
  包含按域组织的已识别风险的汇总表：基本信息、用户帐户、特权和角色、授权控制、细粒度访问控制、审计、加密、配置（数据库，网络，操作系统）等。 Summary table with identified risks organized by domains: Basic information, user accounts, privileges and roles, authorization control, fine-grained access control, auditing, encryption, config, etc.

- **超过120项详细发现及备注**Over 120 detailed findings with remarks

  每个发现都包含一行对预期内容、风险级别、细节和优秀实践注释的解释。 Each finding contains a one line explanation of what is expected, a risk level, details, and remarks on best practices.

- **参考OBP，CIS基准，STIG规则和GDPR章节/条款**References to Oracle Best Practices, CIS Benchmark, STIG Rules and GDPR articles/recitals

  除了Oracle数据库安全开发组织优秀实践之外，还有到CIS、STIG规则和EU GDPR章节/条款的映射。 Along with Oracle Database security development organization best practices, there is a mapping to CIS, STIG rules, and EU GDPR articles and recitals.



发现

扫描列名和注释元数据以发现敏感数据。生成敏感数据评估报告。 Scan column names and comments metadata to discover sensitive data. Generates a Sensitive Data Assessment report.

- **发现敏感数据**Discovers sensitive data

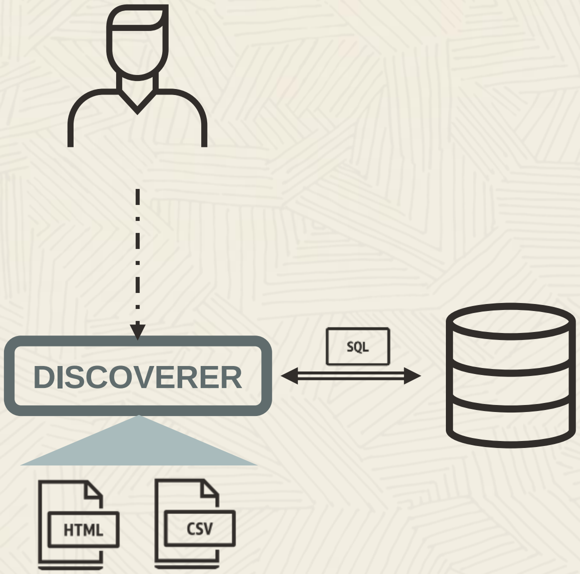
  获取敏感数据类别和类型(125+)、表、列、行和风险级别的摘要和详细信息。 Get summary and details on Sensitive Data Categories and Types (125+), tables, columns, rows, and risk levels.

- **提供有关安全控制的建议**Provides recommendations on security controls

  获取有关应采取哪些安全控制措施来保护敏感数据的建议。 Get recommendations on which security controls to put in place to protect your sensitive data.

- **可定制**Customizable

  利用现有的示例文件扩展或适应您的特定需求。 Leverage the existing sample files to expand or adapt to your specific needs.



发现例释Sample finding

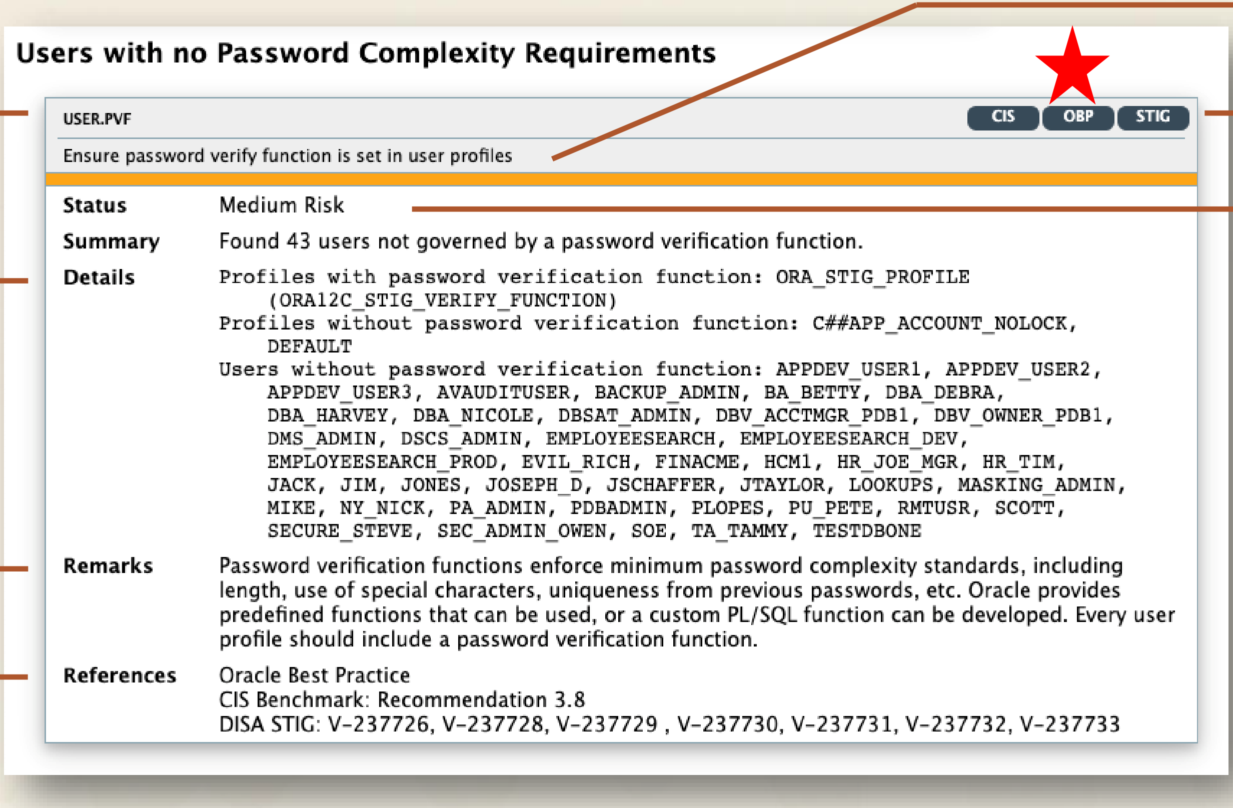
一句话描述应该做什么A single sentence that describes what should be done

发现的类别
Category of the Finding

发现详情Detail of the Finding

理据及建议Rationale and Recommendations

规则映射Mapping to Regulations



Users with no Password Complexity Requirements

USER.PVF

Ensure password verify function is set in user profiles

Status Medium Risk

Summary Found 43 users not governed by a password verification function.

Details

```
Profiles with password verification function: ORA_STIG_PROFILE
    (ORA12C_STIG_VERIFY_FUNCTION)
Profiles without password verification function: C##APP_ACCOUNT_NOLOCK,
    DEFAULT
Users without password verification function: APPDEV_USER1, APPDEV_USER2,
    APPDEV_USER3, AVAUDITUSER, BACKUP_ADMIN, BA_BETTY, DBA_DEBRA,
    DBA_HARVEY, DBA_NICOLE, DBSAT_ADMIN, DBV_ACCTMGR_PDB1, DBV_OWNER_PDB1,
    DMS_ADMIN, DSCS_ADMIN, EMPLOYEESEARCH, EMPLOYEESEARCH_DEV,
    EMPLOYEESEARCH_PROD, EVIL_RICH, FINACME, HCM1, HR_JOE_MGR, HR_TIM,
    JACK, JIM, JONES, JOSEPH_D, JSCHAFFER, JTAYLOR, LOOKUPS, MASKING_ADMIN,
    MIKE, NY_NICK, PA_ADMIN, PDBADMIN, PLOPES, PU_PETE, RMTUSR, SCOTT,
    SECURE_STEVE, SEC_ADMIN_OWEN, SOE, TA_TAMMY, TESTDBONE
```

Remarks Password verification functions enforce minimum password complexity standards, including length, use of special characters, uniqueness from previous passwords, etc. Oracle provides predefined functions that can be used, or a custom PL/SQL function can be developed. Every user profile should include a password verification function.

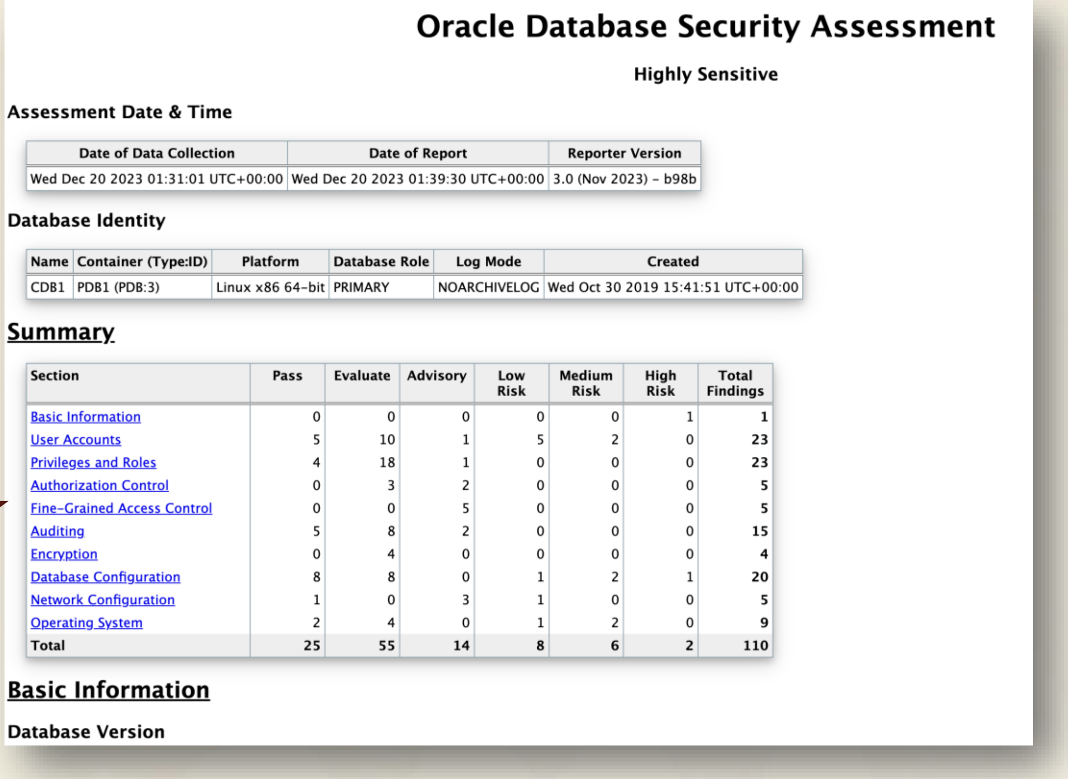
References Oracle Best Practice
CIS Benchmark: Recommendation 3.8
DISA STIG: V-237726, V-237728, V-237729 , V-237730, V-237731, V-237732, V-237733

规则适用性
Applicability to Regulations

可以是评估、建议、低、中、高风险Can be Evaluate, Advisory, Low, Medium, or High Risk

演示DEMO

数据库安全评估 – 概要



Oracle Database Security Assessment

Highly Sensitive

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Wed Dec 20 2023 01:31:01 UTC+00:00	Wed Dec 20 2023 01:39:30 UTC+00:00	3.0 (Nov 2023) – b98b

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
CDB1	PDB1 (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Oct 30 2019 15:41:51 UTC+00:00

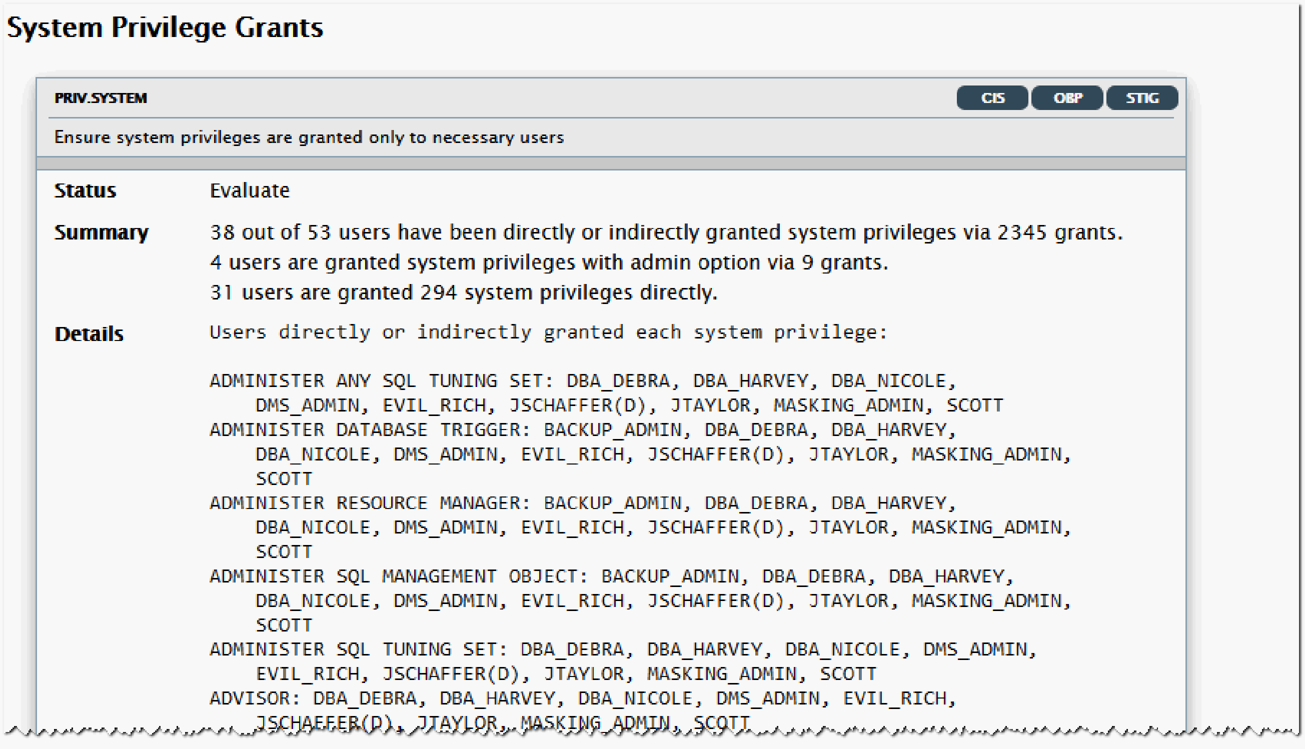
Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	5	10	1	5	2	0	23
Privileges and Roles	4	18	1	0	0	0	23
Authorization Control	0	3	2	0	0	0	5
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	5	8	2	0	0	0	15
Encryption	0	4	0	0	0	0	4
Database Configuration	8	8	0	1	2	1	20
Network Configuration	1	0	3	1	0	0	5
Operating System	2	4	0	1	2	0	9
Total	25	55	14	8	6	2	110

Basic Information

Database Version

特权 – 系统



System Privilege Grants

PRIV.SYSTEM

Ensure system privileges are granted only to necessary users

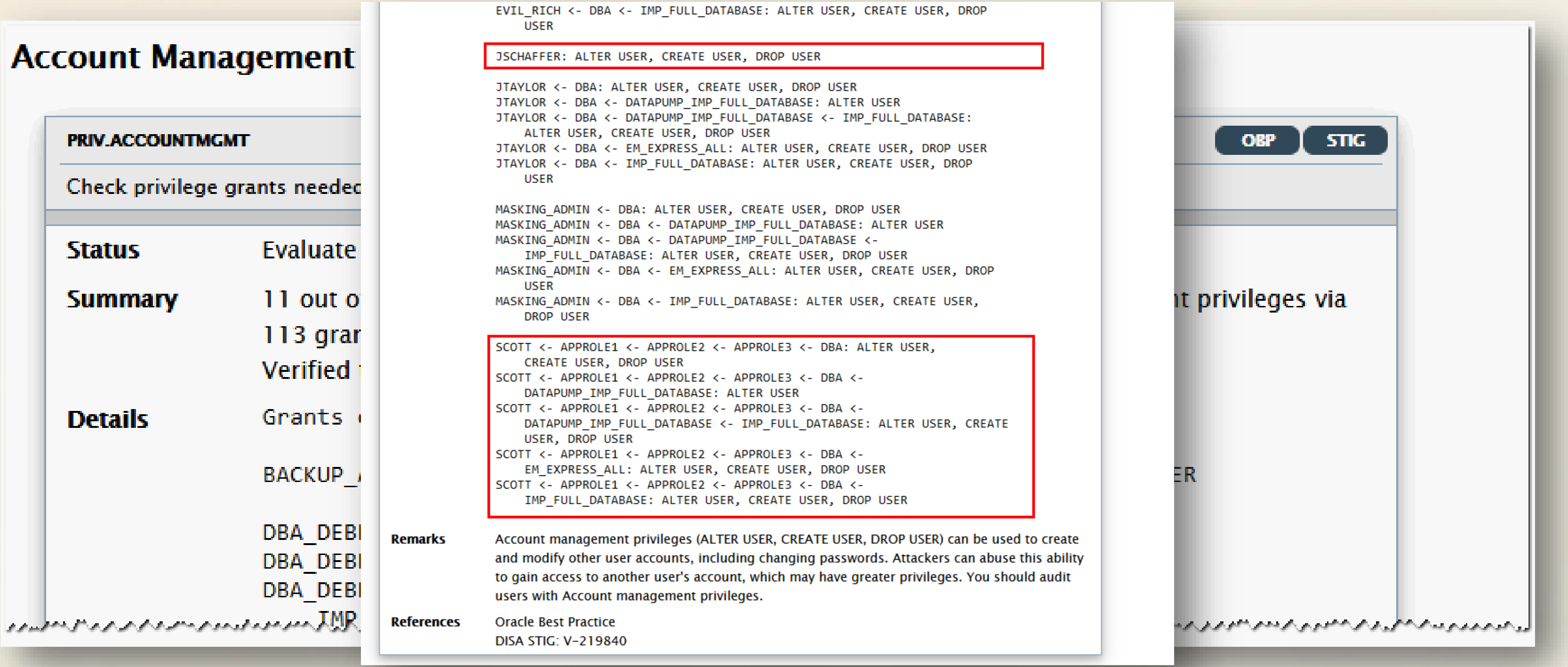
Status Evaluate

Summary 38 out of 53 users have been directly or indirectly granted system privileges via 2345 grants.
4 users are granted system privileges with admin option via 9 grants.
31 users are granted 294 system privileges directly.

Details

```
Users directly or indirectly granted each system privilege:

ADMINISTER ANY SQL TUNING SET: DBA_DEBRA, DBA_HARVEY, DBA_NICOLE,
    DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN, SCOTT
ADMINISTER DATABASE TRIGGER: BACKUP_ADMIN, DBA_DEBRA, DBA_HARVEY,
    DBA_NICOLE, DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN,
    SCOTT
ADMINISTER RESOURCE MANAGER: BACKUP_ADMIN, DBA_DEBRA, DBA_HARVEY,
    DBA_NICOLE, DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN,
    SCOTT
ADMINISTER SQL MANAGEMENT OBJECT: BACKUP_ADMIN, DBA_DEBRA, DBA_HARVEY,
    DBA_NICOLE, DMS_ADMIN, EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN,
    SCOTT
ADMINISTER SQL TUNING SET: DBA_DEBRA, DBA_HARVEY, DBA_NICOLE, DMS_ADMIN,
    EVIL_RICH, JSCHAFFER(D), JTAYLOR, MASKING_ADMIN, SCOTT
ADVISOR: DBA_DEBRA, DBA_HARVEY, DBA_NICOLE, DMS_ADMIN, EVIL_RICH,
    JSCHAFFER(D), JTAYLOR, MASKING_ADMIN, SCOTT
```

特权 – 账号管理



Account Management

PRIV.ACCOUNTMGMT

Check privilege grants neede

OBP STIG

Status Evaluate

Summary 11 out o
113 grar
Verified

t privileges via

Details Grants

BACKUP_

DBA_DEBI
DBA_DEBI
DBA_DEBI
IMP

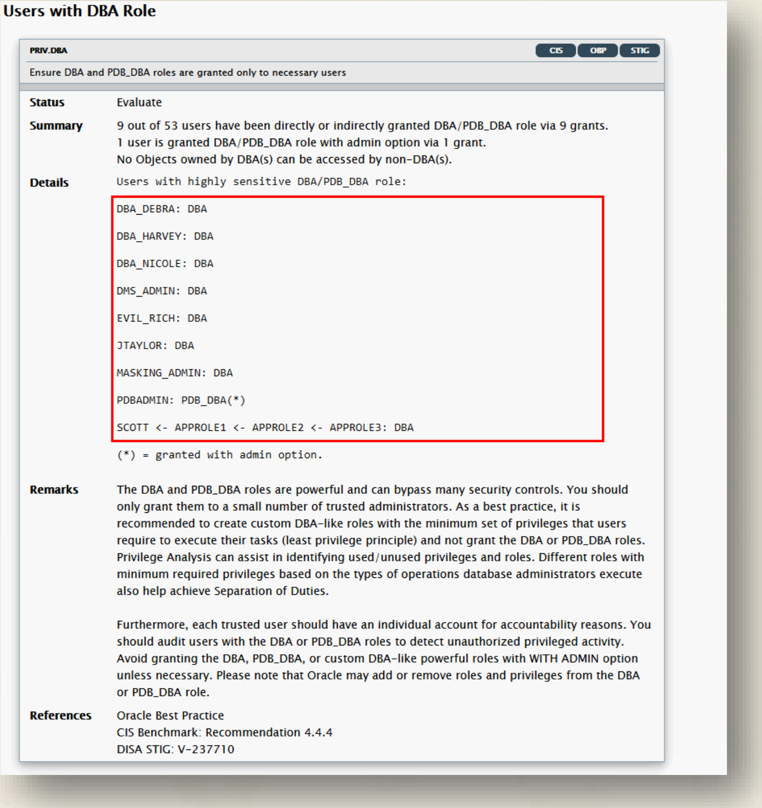
ER

```
EVIL_RICH <- DBA <- IMP_FULL_DATABASE: ALTER USER, CREATE USER, DROP
    USER

JSCHAFFER: ALTER USER, CREATE USER, DROP USER

JTAYLOR <- DBA: ALTER USER, CREATE USER, DROP USER
JTAYLOR <- DBA <- DATAPUMP_IMP_FULL_DATABASE: ALTER USER
JTAYLOR <- DBA <- DATAPUMP_IMP_FULL_DATABASE <- IMP_FULL_DATABASE:
    ALTER USER, CREATE USER, DROP USER
JTAYLOR <- DBA <- EM_EXPRESS_ALL: ALTER USER, CREATE USER, DROP USER
JTAYLOR <- DBA <- IMP_FULL_DATABASE: ALTER USER, CREATE USER, DROP
    USER

MASKING_ADMIN <- DBA: ALTER USER, CREATE USER, DROP USER
MASKING_ADMIN <- DBA <- DATAPUMP_IMP_FULL_DATABASE: ALTER USER
MASKING_ADMIN <- DBA <- DATAPUMP_IMP_FULL_DATABASE <-
    IMP_FULL_DATABASE: ALTER USER, CREATE USER, DROP USER
MASKING_ADMIN <- DBA <- EM_EXPRESS_ALL: ALTER USER, CREATE USER, DROP
    USER
MASKING_ADMIN <- DBA <- IMP_FULL_DATABASE: ALTER USER, CREATE USER,
    DROP USER

SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3 <- DBA: ALTER USER,
    CREATE USER, DROP USER
SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3 <- DBA <-
    DATAPUMP_IMP_FULL_DATABASE: ALTER USER
SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3 <- DBA <-
    DATAPUMP_IMP_FULL_DATABASE <- IMP_FULL_DATABASE: ALTER USER, CREATE
    USER, DROP USER
SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3 <- DBA <-
    EM_EXPRESS_ALL: ALTER USER, CREATE USER, DROP USER
SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3 <- DBA <-
    IMP_FULL_DATABASE: ALTER USER, CREATE USER, DROP USER
```

Remarks Account management privileges (ALTER USER, CREATE USER, DROP USER) can be used to create and modify other user accounts, including changing passwords. Attackers can abuse this ability to gain access to another user's account, which may have greater privileges. You should audit users with Account management privileges.

References Oracle Best Practice
DISA STIG: V-219840

特权 – DBA



Users with DBA Role

PRIV.DBA

Ensure DBA and PDB_DBA roles are granted only to necessary users

Status Evaluate

Summary 9 out of 53 users have been directly or indirectly granted DBA/PDB_DBA role via 9 grants.
1 user is granted DBA/PDB_DBA role with admin option via 1 grant.
No Objects owned by DBA(s) can be accessed by non-DBA(s).

Details

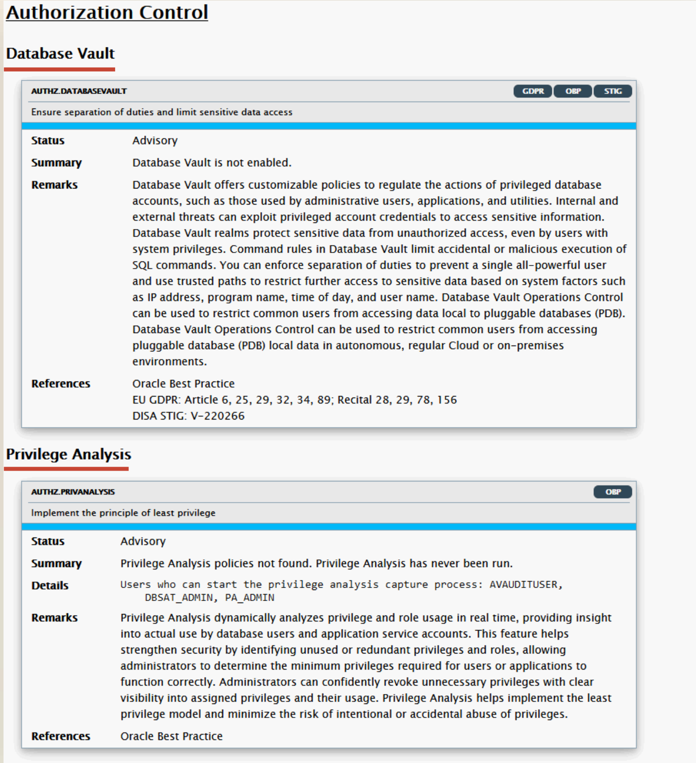
```
Users with highly sensitive DBA/PDB_DBA role:

DBA_DEBRA: DBA

DBA_HARVEY: DBA

DBA_NICOLE: DBA

DMS_ADMIN: DBA

EVIL_RICH: DBA

JTAYLOR: DBA

MASKING_ADMIN: DBA

PDBADMIN: PDB_DBA(*)

SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3: DBA

(*) = granted with admin option.
```

Remarks The DBA and PDB_DBA roles are powerful and can bypass many security controls. You should only grant them to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with the minimum set of privileges that users require to execute their tasks (least privilege principle) and not grant the DBA or PDB_DBA roles. Privilege Analysis can assist in identifying used/unused privileges and roles. Different roles with minimum required privileges based on the types of operations database administrators execute also help achieve Separation of Duties.

Furthermore, each trusted user should have an individual account for accountability reasons. You should audit users with the DBA or PDB_DBA roles to detect unauthorized privileged activity. Avoid granting the DBA, PDB_DBA, or custom DBA-like powerful roles with WITH ADMIN option unless necessary. Please note that Oracle may add or remove roles and privileges from the DBA or PDB_DBA role.

References Oracle Best Practice
CIS Benchmark: Recommendation 4.4.4
DISA STIG: V-237710

授权控制



Authorization Control

Database Vault

AUTHZ.DATABASEVAULT GDPR OBP STIG

Ensure separation of duties and limit sensitive data access

Status	Advisory
Summary	Database Vault is not enabled.
Remarks	Database Vault offers customizable policies to regulate the actions of privileged database accounts, such as those used by administrative users, applications, and utilities. Internal and external threats can exploit privileged account credentials to access sensitive information. Database Vault realms protect sensitive data from unauthorized access, even by users with system privileges. Command rules in Database Vault limit accidental or malicious execution of SQL commands. You can enforce separation of duties to prevent a single all-powerful user and use trusted paths to restrict further access to sensitive data based on system factors such as IP address, program name, time of day, and user name. Database Vault Operations Control can be used to restrict common users from accessing data local to pluggable databases (PDB). Database Vault Operations Control can be used to restrict common users from accessing pluggable database (PDB) local data in autonomous, regular Cloud or on-premises environments.
References	Oracle Best Practice EU GDPR: Article 6, 25, 29, 32, 34, 89; Recital 28, 29, 78, 156 DISA STIG: V-220266

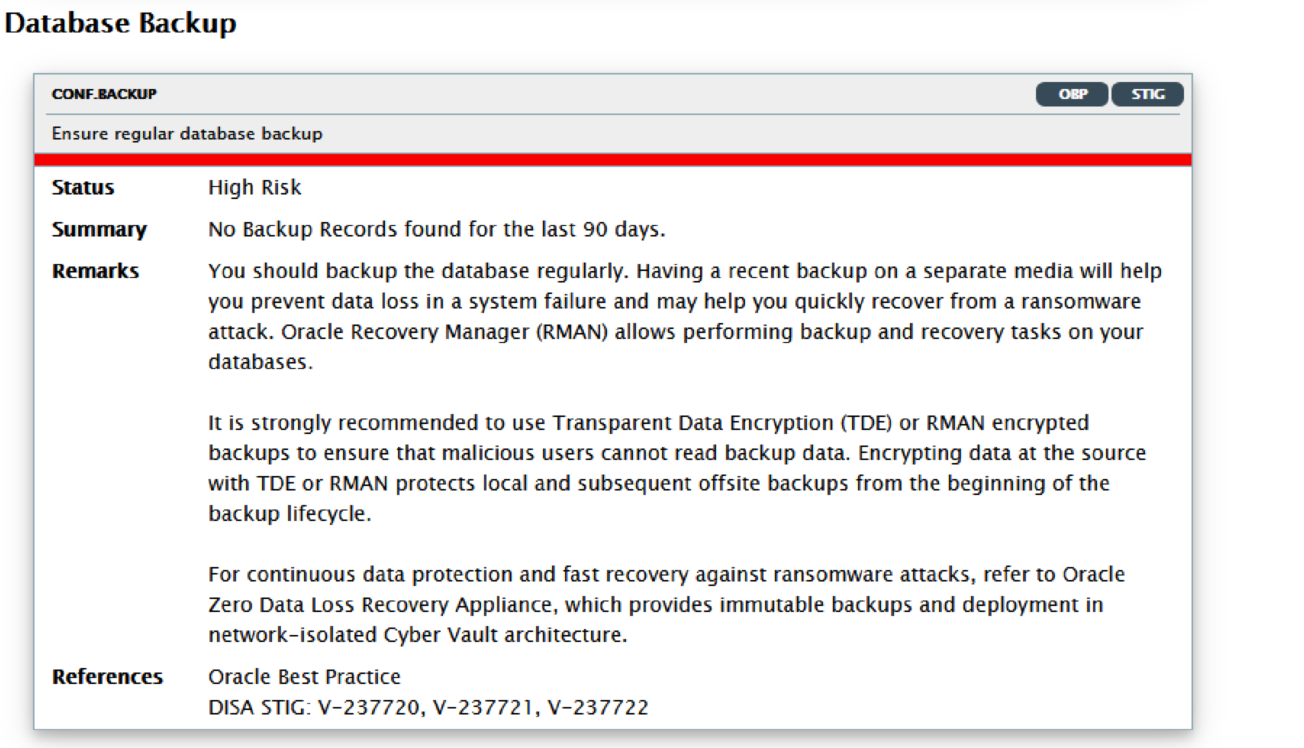
Privilege Analysis

AUTHZ.PRIVANALYSIS OBP

Implement the principle of least privilege

Status	Advisory
Summary	Privilege Analysis policies not found. Privilege Analysis has never been run.
Details	`Users who can start the privilege analysis capture process: AVAUDITUSER, DBSAT_ADMIN, PA_ADMIN`
Remarks	Privilege Analysis dynamically analyzes privilege and role usage in real time, providing insight into actual use by database users and application service accounts. This feature helps strengthen security by identifying unused or redundant privileges and roles, allowing administrators to determine the minimum privileges required for users or applications to function correctly. Administrators can confidently revoke unnecessary privileges with clear visibility into assigned privileges and their usage. Privilege Analysis helps implement the least privilege model and minimize the risk of intentional or accidental abuse of privileges.
References	Oracle Best Practice

配置 – 备份



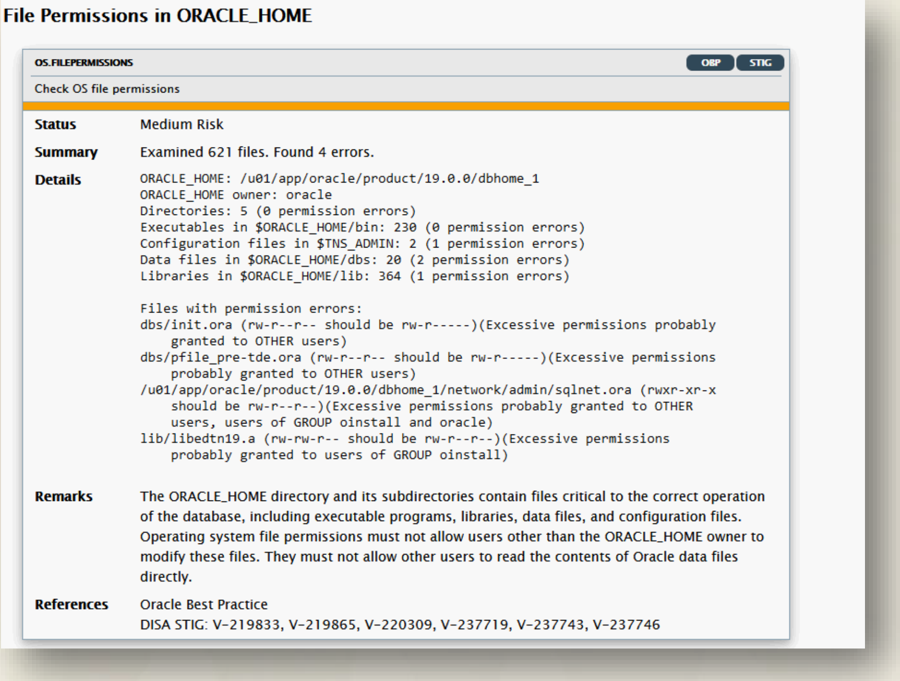
Database Backup

CONF.BACKUP

Ensure regular database backup

Status	High Risk
Summary	No Backup Records found for the last 90 days.
Remarks	You should backup the database regularly. Having a recent backup on a separate media will help you prevent data loss in a system failure and may help you quickly recover from a ransomware attack. Oracle Recovery Manager (RMAN) allows performing backup and recovery tasks on your databases. It is strongly recommended to use Transparent Data Encryption (TDE) or RMAN encrypted backups to ensure that malicious users cannot read backup data. Encrypting data at the source with TDE or RMAN protects local and subsequent offsite backups from the beginning of the backup lifecycle. For continuous data protection and fast recovery against ransomware attacks, refer to Oracle Zero Data Loss Recovery Appliance, which provides immutable backups and deployment in network-isolated Cyber Vault architecture.
References	Oracle Best Practice DISA STIG: V-237720, V-237721, V-237722

操作系统 – 文件权限



File Permissions in ORACLE_HOME

OS.FILEPERMISSIONS

Check OS file permissions

Status Medium Risk

Summary Examined 621 files. Found 4 errors.

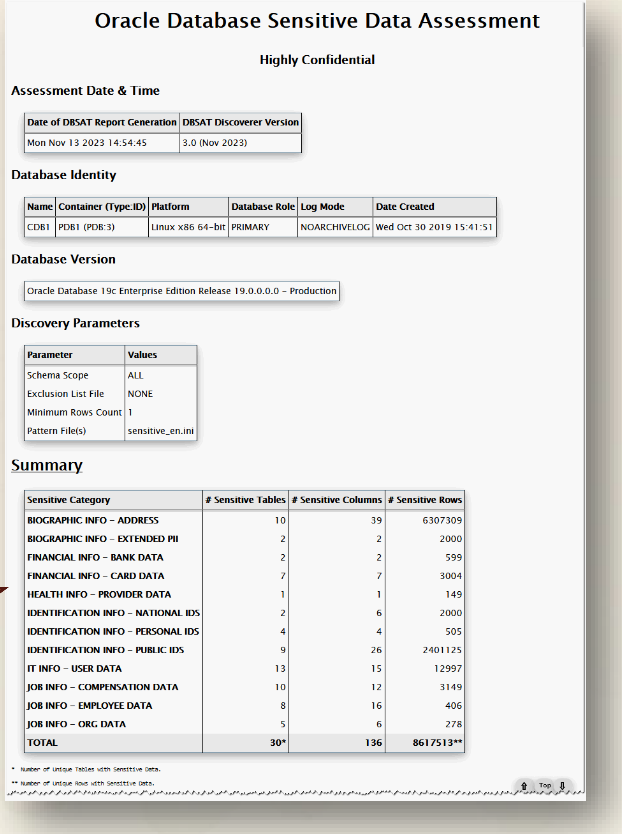
Details

```
ORACLE_HOME: /u01/app/oracle/product/19.0.0/dbhome_1
ORACLE_HOME owner: oracle
Directories: 5 (0 permission errors)
Executables in $ORACLE_HOME/bin: 230 (0 permission errors)
Configuration files in $TNS_ADMIN: 2 (1 permission errors)
Data files in $ORACLE_HOME/dbs: 20 (2 permission errors)
Libraries in $ORACLE_HOME/lib: 364 (1 permission errors)

Files with permission errors:
dbs/init.ora (rw-r--r-- should be rw-r-----)(Excessive permissions probably
    granted to OTHER users)
dbs/pfile_pre-tde.ora (rw-r--r-- should be rw-r-----)(Excessive permissions
    probably granted to OTHER users)
/u01/app/oracle/product/19.0.0/dbhome_1/network/admin/sqlnet.ora (rwxr-xr-x
    should be rw-r--r--)(Excessive permissions probably granted to OTHER
    users, users of GROUP oinstall and oracle)
lib/libedtn19.a (rw-rw-r-- should be rw-r--r--)(Excessive permissions
    probably granted to users of GROUP oinstall)
```

Remarks The ORACLE_HOME directory and its subdirectories contain files critical to the correct operation of the database, including executable programs, libraries, data files, and configuration files. Operating system file permissions must not allow users other than the ORACLE_HOME owner to modify these files. They must not allow other users to read the contents of Oracle data files directly.

References Oracle Best Practice
DISA STIG: V-219833, V-219865, V-220309, V-237719, V-237743, V-237746

敏感数据发现 – 概要



Oracle Database Sensitive Data Assessment

Highly Confidential

Assessment Date & Time

Date of DBSAT Report Generation	DBSAT Discoverer Version
Mon Nov 13 2023 14:54:45	3.0 (Nov 2023)

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Date Created
CDB1	PDB1 (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Oct 30 2019 15:41:51

Database Version

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 – Production

Discovery Parameters

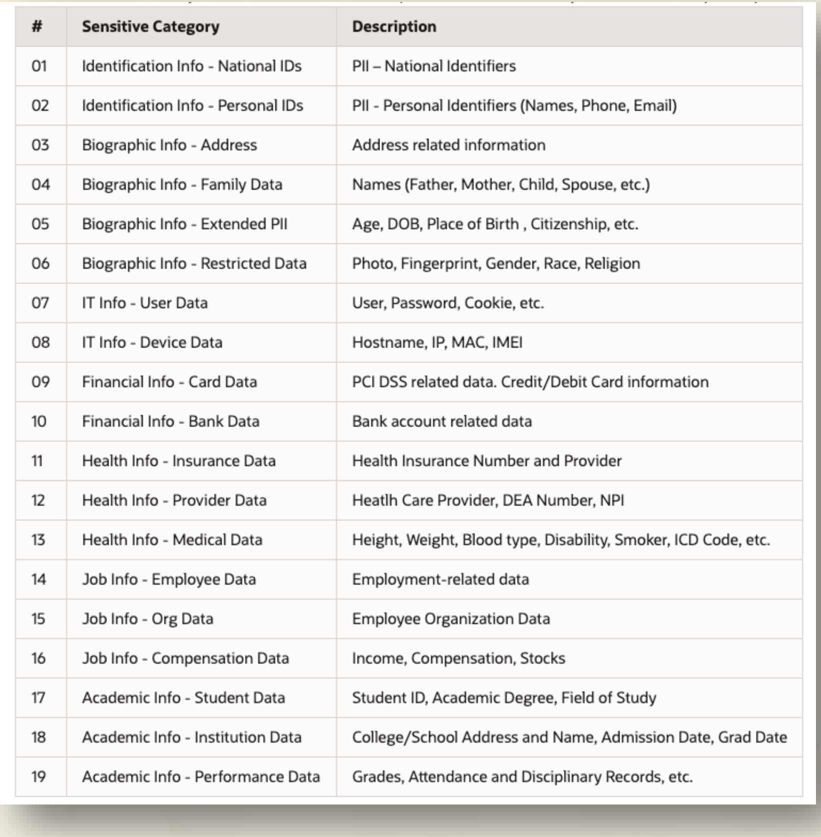
Parameter	Values
Schema Scope	ALL
Exclusion List File	NONE
Minimum Rows Count	1
Pattern File(s)	sensitive_en.ini

Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO – ADDRESS	10	39	6307309
BIOGRAPHIC INFO – EXTENDED PII	2	2	2000
FINANCIAL INFO – BANK DATA	2	2	599
FINANCIAL INFO – CARD DATA	7	7	3004
HEALTH INFO – PROVIDER DATA	1	1	149
IDENTIFICATION INFO – NATIONAL IDS	2	6	2000
IDENTIFICATION INFO – PERSONAL IDS	4	4	505
IDENTIFICATION INFO – PUBLIC IDS	9	26	2401125
IT INFO – USER DATA	13	15	12997
JOB INFO – COMPENSATION DATA	10	12	3149
JOB INFO – EMPLOYEE DATA	8	16	406
JOB INFO – ORG DATA	5	6	278
TOTAL	30*	136	8617513**

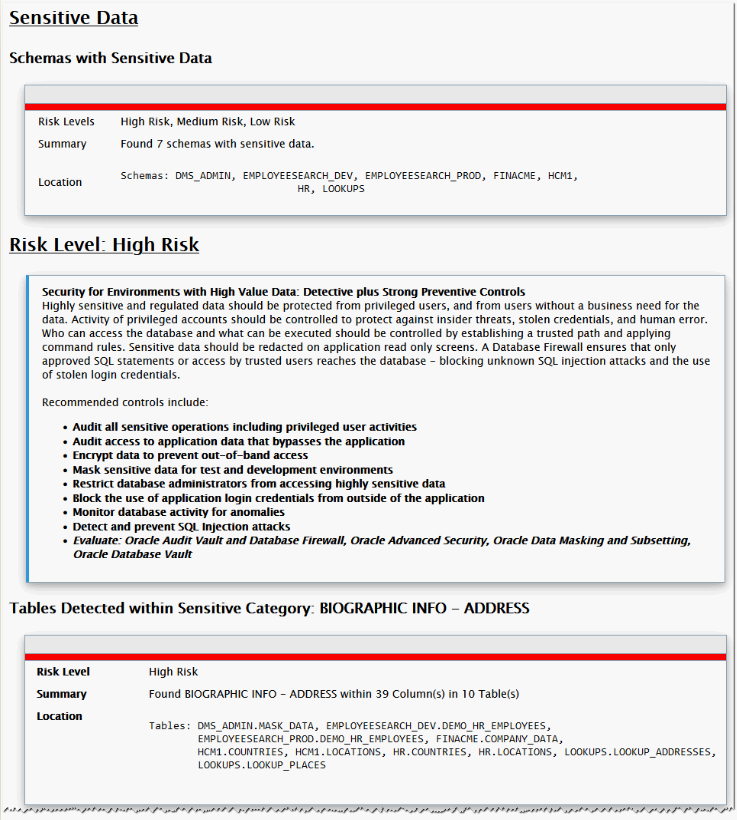
* Number of Unique Tables with Sensitive Data.

** Number of Unique Rows with Sensitive Data.



#	Sensitive Category	Description
01	Identification Info - National IDs	PII – National Identifiers
02	Identification Info - Personal IDs	PII - Personal Identifiers (Names, Phone, Email)
03	Biographic Info - Address	Address related information
04	Biographic Info - Family Data	Names (Father, Mother, Child, Spouse, etc.)
05	Biographic Info - Extended PII	Age, DOB, Place of Birth , Citizenship, etc.
06	Biographic Info - Restricted Data	Photo, Fingerprint, Gender, Race, Religion
07	IT Info - User Data	User, Password, Cookie, etc.
08	IT Info - Device Data	Hostname, IP, MAC, IMEI
09	Financial Info - Card Data	PCI DSS related data. Credit/Debit Card information
10	Financial Info - Bank Data	Bank account related data
11	Health Info - Insurance Data	Health Insurance Number and Provider
12	Health Info - Provider Data	Heatlh Care Provider, DEA Number, NPI
13	Health Info - Medical Data	Height, Weight, Blood type, Disability, Smoker, ICD Code, etc.
14	Job Info - Employee Data	Employment-related data
15	Job Info - Org Data	Employee Organization Data
16	Job Info - Compensation Data	Income, Compensation, Stocks
17	Academic Info - Student Data	Student ID, Academic Degree, Field of Study
18	Academic Info - Institution Data	College/School Address and Name, Admission Date, Grad Date
19	Academic Info - Performance Data	Grades, Attendance and Disciplinary Records, etc.

敏感数据&风险级别



Sensitive Data

Schemas with Sensitive Data

Risk Levels	High Risk, Medium Risk, Low Risk
Summary	Found 7 schemas with sensitive data.
Location	Schemas: DMS_ADMIN, EMPLOYEESEARCH_DEV, EMPLOYEESEARCH_PROD, FINACME, HCM1, HR, LOOKUPS

Risk Level: High Risk

Security for Environments with High Value Data: Detective plus Strong Preventive Controls
Highly sensitive and regulated data should be protected from privileged users, and from users without a business need for the data. Activity of privileged accounts should be controlled to protect against insider threats, stolen credentials, and human error. Who can access the database and what can be executed should be controlled by establishing a trusted path and applying command rules. Sensitive data should be redacted on application read only screens. A Database Firewall ensures that only approved SQL statements or access by trusted users reaches the database – blocking unknown SQL injection attacks and the use of stolen login credentials.

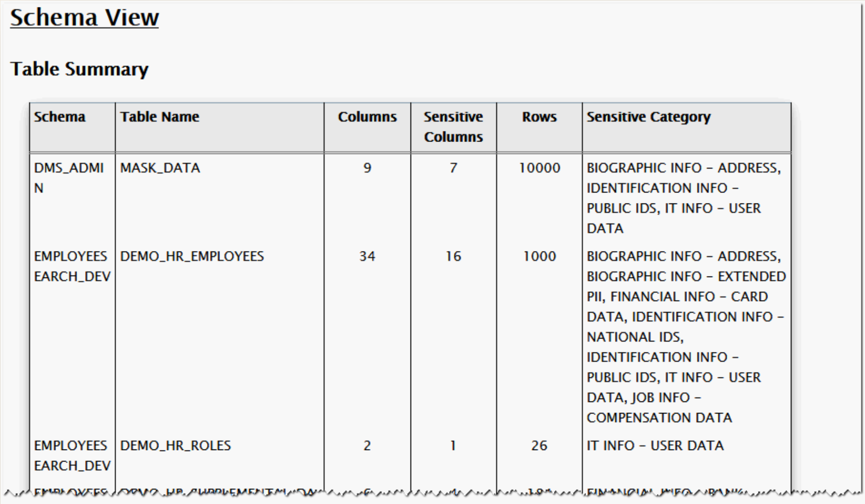
Recommended controls include:

- **Audit all sensitive operations including privileged user activities**
- **Audit access to application data that bypasses the application**
- **Encrypt data to prevent out-of-band access**
- **Mask sensitive data for test and development environments**
- **Restrict database administrators from accessing highly sensitive data**
- **Block the use of application login credentials from outside of the application**
- **Monitor database activity for anomalies**
- **Detect and prevent SQL Injection attacks**
- ***Evaluate: Oracle Audit Vault and Database Firewall, Oracle Advanced Security, Oracle Data Masking and Subsetting, Oracle Database Vault***

Tables Detected within Sensitive Category: BIOGRAPHIC INFO – ADDRESS

Risk Level	High Risk
Summary	Found BIOGRAPHIC INFO – ADDRESS within 39 Column(s) in 10 Table(s)
Location	Tables: DMS_ADMIN.MASK_DATA, EMPLOYEESEARCH_DEV.DEMO_HR_EMPLOYEES, EMPLOYEESEARCH_PROD.DEMO_HR_EMPLOYEES, FINACME.COMPANY_DATA, HCM1.COUNTRIES, HCM1.LOCATIONS, HR.COUNTRIES, HR.LOCATIONS, LOOKUPS.LOOKUP_ADDRESSES, LOOKUPS.LOOKUP_PLACES

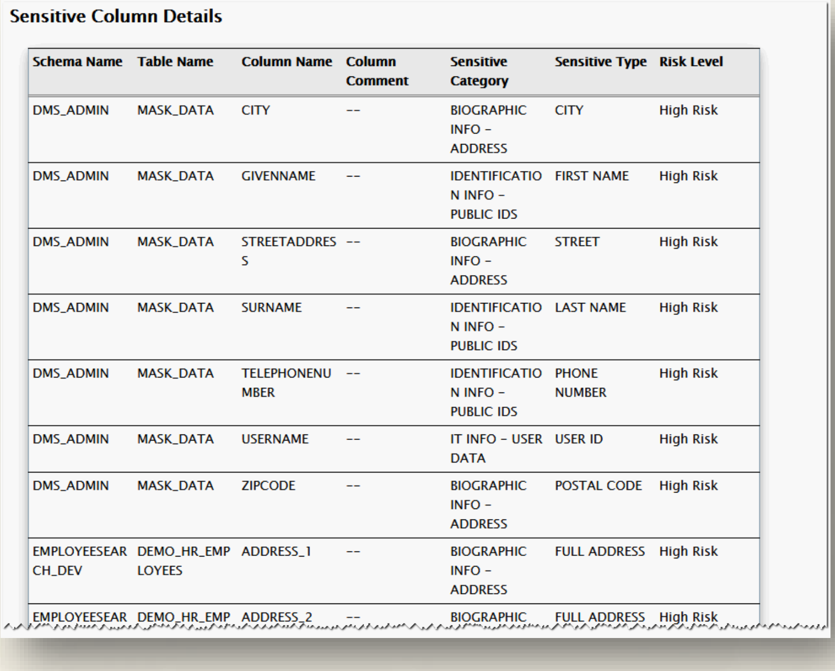
Schema视图&敏感列详细信息



Schema View

Table Summary

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
DMS_ADMIN	MASK_DATA	9	7	10000	BIOGRAPHIC INFO – ADDRESS, IDENTIFICATION INFO – PUBLIC IDS, IT INFO – USER DATA
EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	34	16	1000	BIOGRAPHIC INFO – ADDRESS, BIOGRAPHIC INFO – EXTENDED PII, FINANCIAL INFO – CARD DATA, IDENTIFICATION INFO – NATIONAL IDS, IDENTIFICATION INFO – PUBLIC IDS, IT INFO – USER DATA, JOB INFO – COMPENSATION DATA
EMPLOYEESEARCH_DEV	DEMO_HR_ROLES	2	1	26	IT INFO – USER DATA
EMPLOYEES	[illegible]	[illegible]	[illegible]	[illegible]	FINANCIAL INFO [illegible]



Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
DMS_ADMIN	MASK_DATA	CITY	--	BIOGRAPHIC INFO – ADDRESS	CITY	High Risk
DMS_ADMIN	MASK_DATA	GIVENNAME	--	IDENTIFICATION INFO – PUBLIC IDS	FIRST NAME	High Risk
DMS_ADMIN	MASK_DATA	STREETADDRESS	--	BIOGRAPHIC INFO – ADDRESS	STREET	High Risk
DMS_ADMIN	MASK_DATA	SURNAME	--	IDENTIFICATION INFO – PUBLIC IDS	LAST NAME	High Risk
DMS_ADMIN	MASK_DATA	TELEPHONENUMBER	--	IDENTIFICATION INFO – PUBLIC IDS	PHONE NUMBER	High Risk
DMS_ADMIN	MASK_DATA	USERNAME	--	IT INFO – USER DATA	USER ID	High Risk
DMS_ADMIN	MASK_DATA	ZIPCODE	--	BIOGRAPHIC INFO – ADDRESS	POSTAL CODE	High Risk
EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	ADDRESS_1	--	BIOGRAPHIC INFO – ADDRESS	FULL ADDRESS	High Risk
EMPLOYEESEAR	DEMO_HR_EMP	ADDRESS_2	--	BIOGRAPHIC	FULL ADDRESS	High Risk

为什么以及何时考虑DBSAT?Why and when to consider DBSAT?

- 通过命令行快速获取完整的数据库安全评估报告Get a quick and complete Database Security security assessment report via command line
- 访问Oracle数据库安全优秀实践Get access to Oracle Database security best practices
- 开始发现敏感数据Get started discovering sensitive data
- 加强当前的安全策略/指导方针/加固指南Strengthen your current security policy/guidelines/hardening guides
- 评估少量数据库Assess few databases

如果您认可DBSAT建议的价值，并希望评估大量数据库，请考虑使用Data Safe或AVDF。If you value DBSAT recommendations and want to get them for your entire fleet, consider using Data Safe or Audit Vault and Database Firewall.

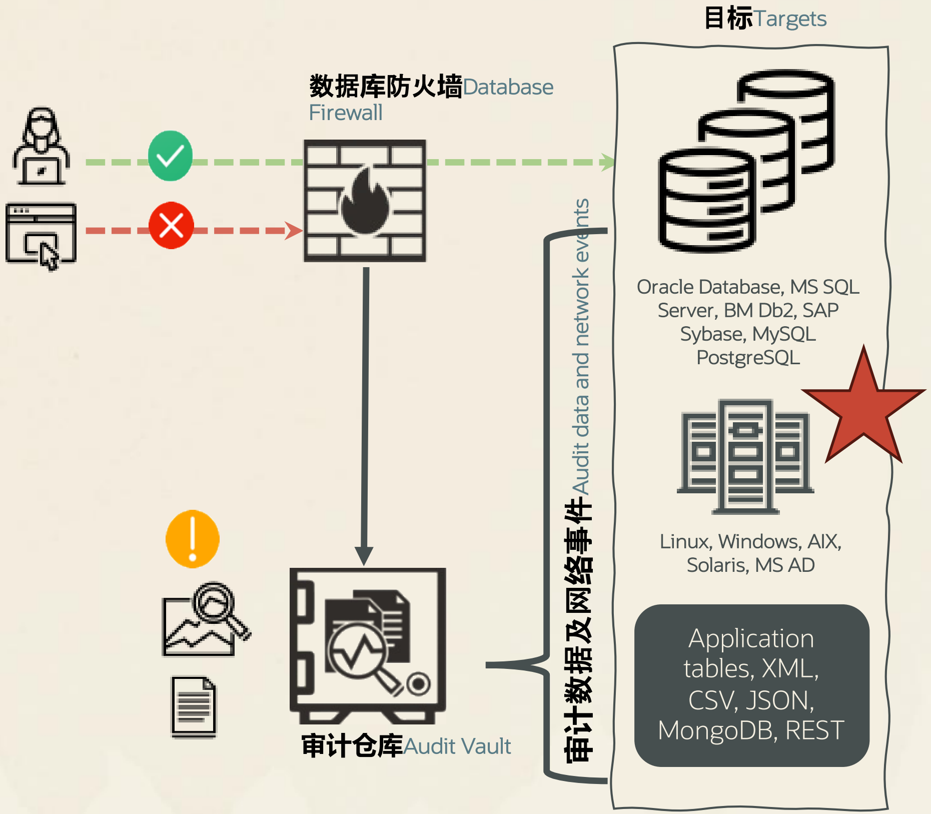
审计仓库和数据库防火墙（AVDF）

Audit Vault and Database Firewall(AVDF)

活动审计，数据库防火墙，数据库安全态势管理

Activity Auditing, Database Firewall, and Database Security Posture Management

Oracle审计仓库和数据库防火墙Oracle Audit Vault and Database Firewall



目标Targets
数据库防火墙Database Firewall
Oracle Database, MS SQL Server, BM Db2, SAP Sybase, MySQL PostgreSQL
Linux, Windows, AIX, Solaris, MS AD
Application tables, XML, CSV, JSON, MongoDB, REST
审计数据及网络事件Audit data and network events
审计仓库Audit Vault

Oracle审计仓库和数据库防火墙（AVDF）是一个完整的数据库活动监控（DAM）解决方案，它结合了原生审计数据和基于网络的SQL流量捕获。Oracle Audit Vault and Database Firewall (AVDF) is a complete Database Activity Monitoring (DAM) solution that combines native audit data with network-based SQL traffic capture.

监视特权用户的活动Monitors privileged user activity

事故发生后，了解发生了的事情Understands what happened after an incident

阻止未经授权的访问Blocks unauthorized access

有关可疑活动的警报Alerts on suspicious activity

简化法规遵从性Simplifies regulatory compliance

AVDF数据库安全态势管理AVDF Database Security Posture Management

安全评估Security Assessment

了解您的安全配置，并确定偏离可接受的安全基线的情况Know your security configuration and identify drift from your accepted security baseline

敏感数据发现Sensitive Data Discovery

知道你的敏感对象是什么，存放在哪里。 Know what your sensitive objects are and where they are stored.

特权用户发现Privileged User Discovery

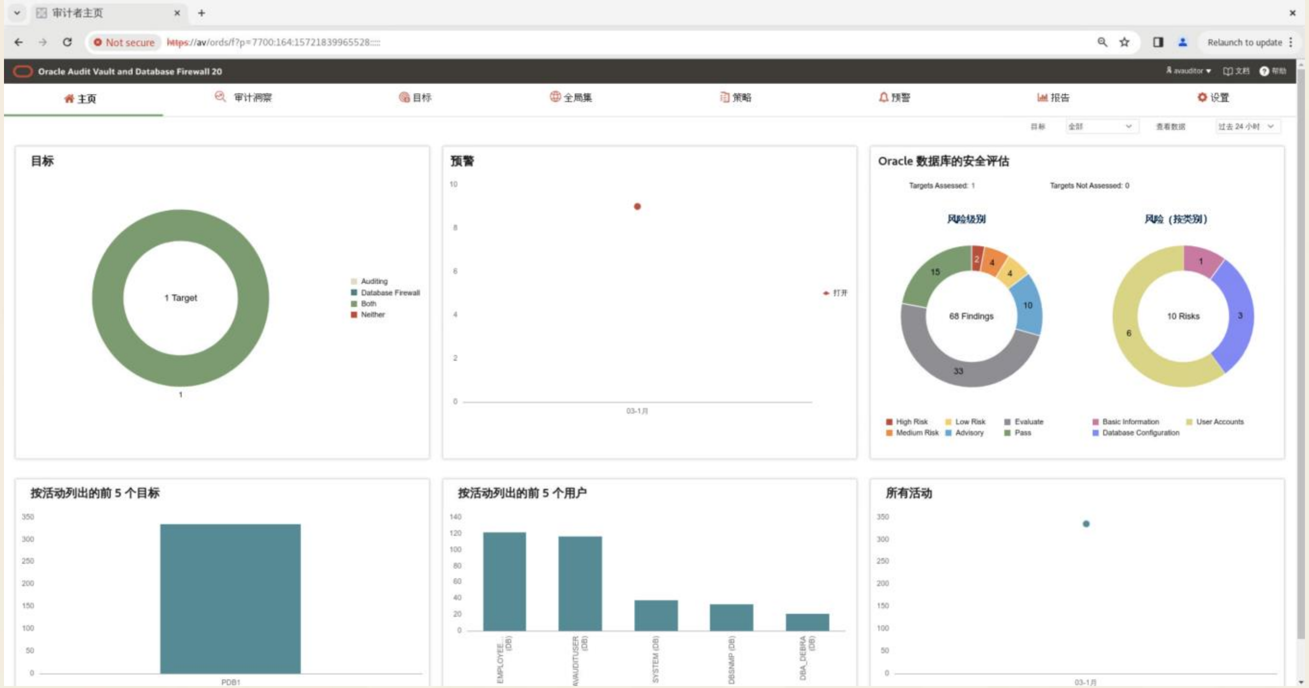
了解您的特权用户是谁以及他们拥有什么权限。 Know who your privileged users are and what permissions they have.

审计洞察Audit Insights

了解数据库用户如何使用您的敏感数据Know how your sensitive data has been used by database users

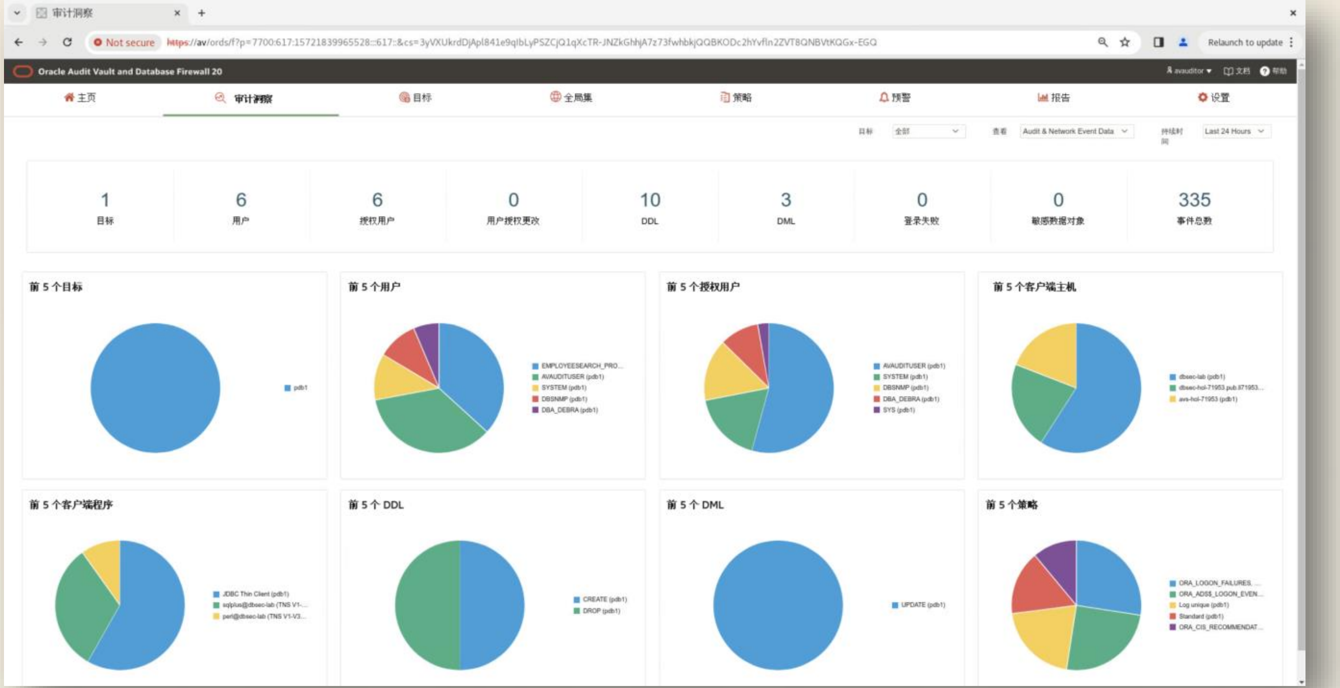
演示DEMO

主页



审计者主页
Not secure
https://av/ords/f?p=7700:164:15721839965528::::
Relaunch to update
Oracle Audit Vault and Database Firewall 20
avauditor
文档
帮助
主页
审计洞察
目标
全局集
策略
预警
报告
设置
目标
全部
查看数据
过去 24 小时
目标
1 Target
1
Auditing
Database Firewall
Both
Neither
预警
10
8
6
4
2
0
03-1月
打开
Oracle 数据库的安全评估
Targets Assessed: 1
Targets Not Assessed: 0
风险级别
2
4
4
10
33
15
68 Findings
High Risk
Medium Risk
Low Risk
Advisory
Evaluate
Pass
风险（按类别）
1
3
6
10 Risks
Basic Information
Database Configuration
User Accounts
按活动列出的前 5 个目标
350
300
250
200
150
100
50
0
PDB1
按活动列出的前 5 个用户
140
120
100
80
60
40
20
0
EMPLOYEE (DB)
AVAUDITUSER (DB)
SYSTEM (DB)
DBSNMP (DB)
DBA_DEBRA (DB)
所有活动
350
300
250
200
150
100
50
0
03-1月

审计洞察


审计洞察
Not secure
https://av/ords/f?p=7700:617:15721839965528::617::&cs=3yVXUkrdDjApl841e9qIbLyPSZCjQ1qXcTR-JNZkGhhjA7z73fwhbkjQQBKODc2hYvfln2ZVT8QNBVtKQGx-EGQ
Relaunch to update
Oracle Audit Vault and Database Firewall 20
avauditor
文档
帮助
主页
审计洞察
目标
全局集
策略
预警
报告
设置

目标 全部　查看 Audit & Network Event Data　持续时间 Last 24 Hours

1	6	6	0	10	3	0	0	335
目标	用户	授权用户	用户授权更改	DDL	DML	登录失败	敏感数据对象	事件总数

前 5 个目标

前 5 个用户

前 5 个授权用户

前 5 个客户端主机

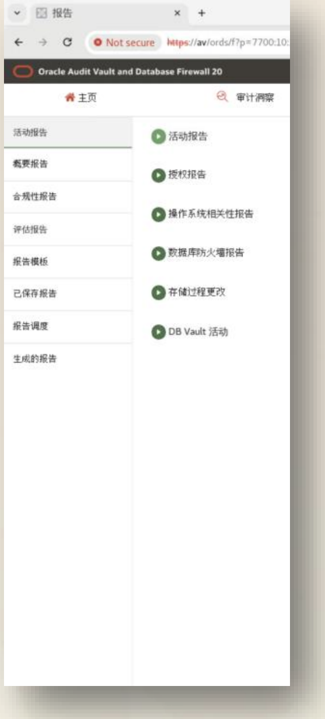
前 5 个客户端程序

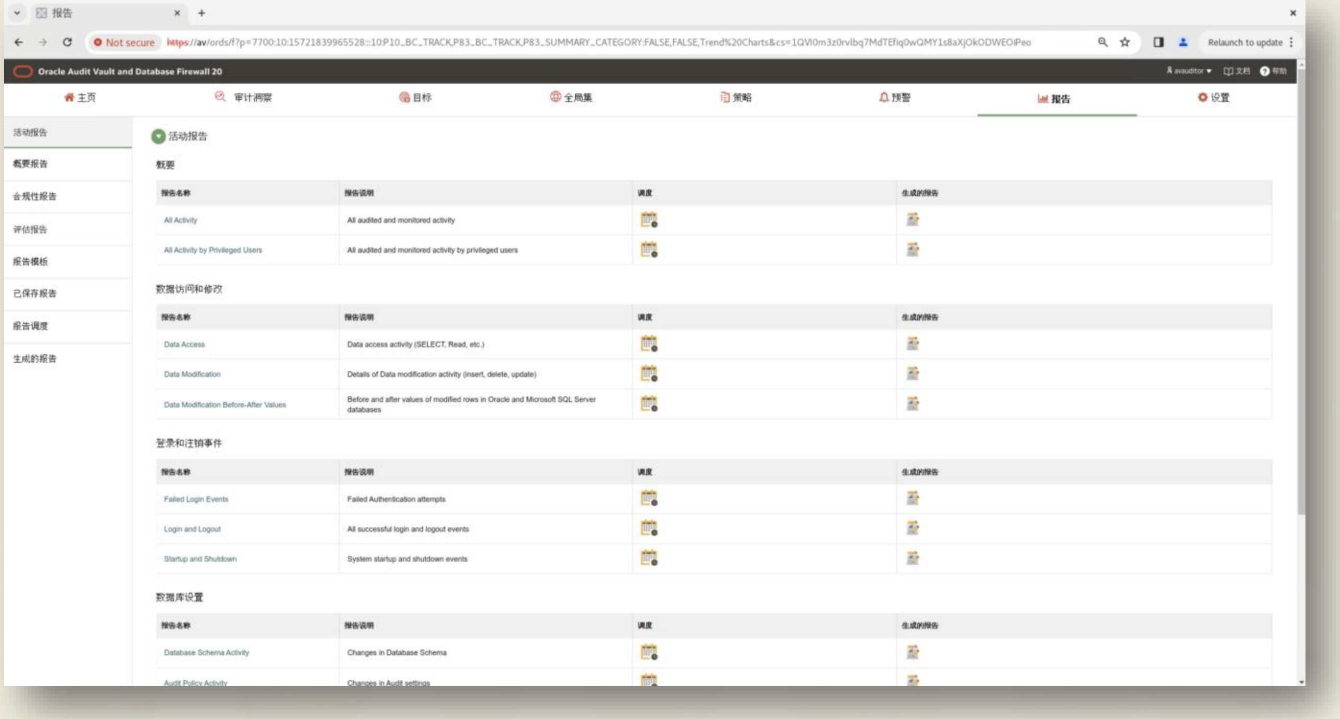
前 5 个 DDL

前 5 个 DML

前 5 个策略

报告




报告
Not secure
https://av/ords/f?p=7700:10:15721839965528::10:P10_BC_TRACK,P83_BC_TRACK,P83_SUMMARY_CATEGORY:FALSE,FALSE,Trend%20Charts&cs=1QVI0m3z0rvlbq7MdTEfiq0wQMY1s8aXjOkODWEOiPeo
Relaunch to update
Oracle Audit Vault and Database Firewall 20
avauditor
文档
帮助
主页
审计洞察
目标
全局集
策略
预警
报告
设置
活动报告
概要报告
合规性报告
评估报告
报告模板
已保存报告
报告调度
生成的报告

活动报告

概要

报告名称	报告说明	调度	生成的报告
All Activity	All audited and monitored activity	📅	📄
All Activity by Privileged Users	All audited and monitored activity by privileged users	📅	📄

数据访问和修改

报告名称	报告说明	调度	生成的报告
Data Access	Data access activity (SELECT, Read, etc.)	📅	📄
Data Modification	Details of Data modification activity (insert, delete, update)	📅	📄
Data Modification Before-After Values	Before and after values of modified rows in Oracle and Microsoft SQL Server databases	📅	📄

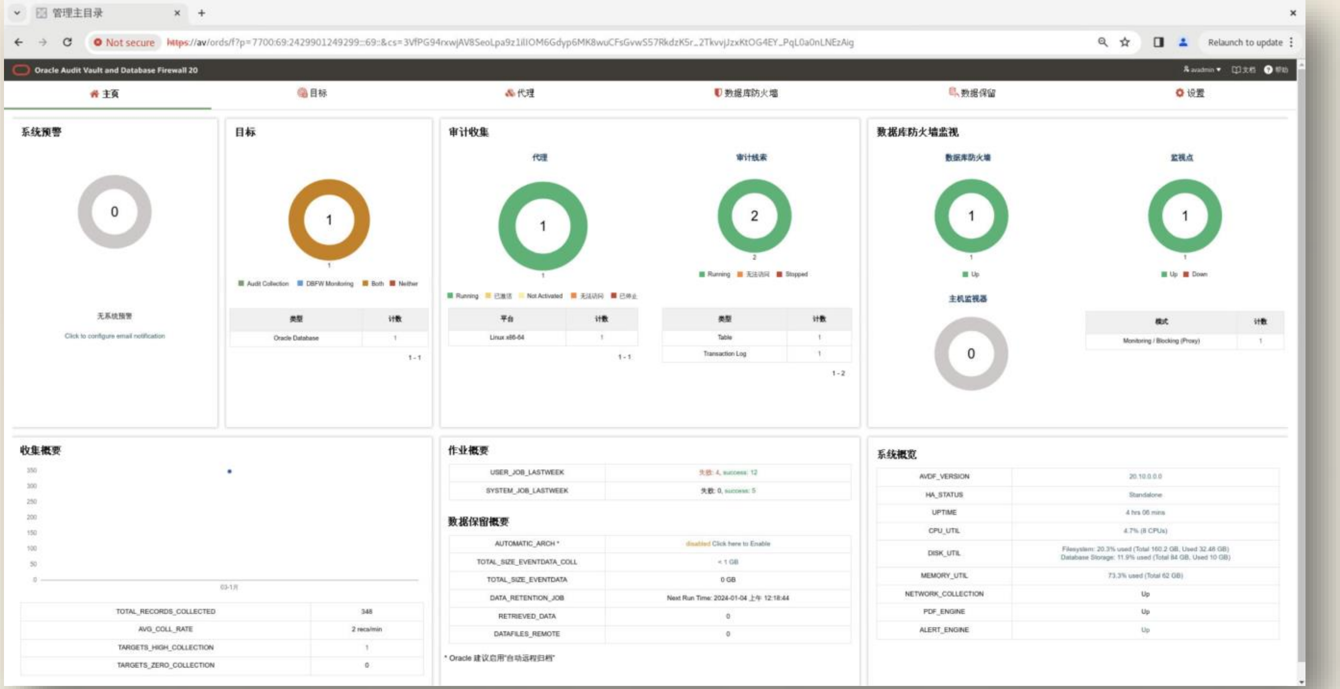
登录和注销事件

报告名称	报告说明	调度	生成的报告
Failed Login Events	Failed Authentication attempts	📅	📄
Login and Logout	All successful login and logout events	📅	📄
Startup and Shutdown	System startup and shutdown events	📅	📄

数据库设置

报告名称	报告说明	调度	生成的报告
Database Schema Activity	Changes in Database Schema	📅	📄
Audit Policy Activity	Changes in Audit settings	📅	📄

权责分离



类型	计数
Oracle Database	1

1 - 1

平台	计数
Linux x86-64	1

1 - 1

类型	计数
Table	1
Transaction Log	1

1 - 2

模式	计数
Monitoring / Blocking (Proxy)	1

TOTAL_RECORDS_COLLECTED	348
AVG_COLL_RATE	2 recs/min
TARGETS_HIGH_COLLECTION	1
TARGETS_ZERO_COLLECTION	0

USER_JOB_LASTWEEK	失败: 4, success: 12
SYSTEM_JOB_LASTWEEK	失败: 0, success: 5

AUTOMATIC_ARCH *	disabled Click here to Enable
TOTAL_SIZE_EVENTDATA_COLL	< 1 GB
TOTAL_SIZE_EVENTDATA	0 GB
DATA_RETENTION_JOB	Next Run Time: 2024-01-04 上午 12:18:44
RETRIEVED_DATA	0
DATAFILES_REMOTE	0

* Oracle 建议启用"自动远程归档"

AVDF_VERSION	20.10.0.0.0
HA_STATUS	Standalone
UPTIME	4 hrs 06 mins
CPU_UTIL	4.7% (8 CPUs)
DISK_UTIL	Filesystem: 20.3% used (Total 160.2 GB, Used 32.48 GB) Database Storage: 11.9% used (Total 84 GB, Used 10 GB)
MEMORY_UTIL	73.3% used (Total 62 GB)
NETWORK_COLLECTION	Up
PDF_ENGINE	Up
ALERT_ENGINE	Up

深入了解Oracle审计仓库与数据库防火墙（AVDF）

ORACLE
甲骨文

深入了解Oracle审计仓库与数据库防火墙(AVDF)

数据安全实战演练系列(二)

钟远

- 资深数据安全专家
- 10年以上系统安全运维和管理库管理经验
- 电信行业背景，在智能运维与数据安全架构方面经验丰富

内容简介

深入了解Oracle审计仓库和数据库防火墙(AVDF)，理解AVDF的原理，架构，功能，以及如何部署使用等.通过现场DEMO演示掌握AVDF的使用，主要包括：

- 如何做用户权限审计
- 如何做敏感数据审计
- 如何查看审计关键表值的前/后变化
- 如何创建审计告警策略
- 如何拦截SQL语句注入

B站专家系列课程

为什么以及何时考虑AVDF?Why and when to consider AVDF?

- 不仅仅需要评估Go beyond assessment
- 为所有Oracle数据库获得大规模的简化和集中的安全配置Get a fleet-wide simplified and centralized security configuration for all Oracle Databases
- 公司/法规要求禁止您在任何云中存储审计记录，或者希望控制审计记录所在的基础设施
  Have corporate/regulatory requirements that forbid you from storing audit records in any cloud, or want control over the infrastructure where your audit records are

如果您希望对数据库进行大规模的安全态势管理以及活动监控，那么AVDF就是您的首选工具。

If you want to have a fleet-wide security posture management of your databases along with activity monitoring, then AVDF is your tool of choice.

数据安全Data Safe

数据库安全云服务，为云上和本地Oracle数据库提供统一的控制台

Database Security cloud service with a unified console for the Oracle Database in-cloud and on-premises

Oracle数据安全Oracle Data Safe

统一的数据库安全控制中心Unified database security control center

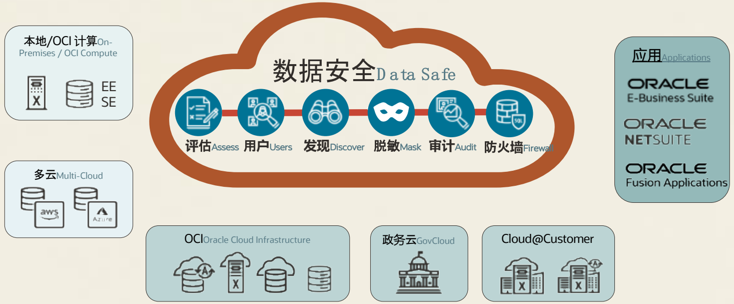
- 安全配置评估Security configuration assessment
- 用户风险评估User risk assessment
- 用户活动审计User activity auditing
- 敏感数据发现Sensitive data discovery
- 数据脱敏Data masking

对所有数据库（本地&云）进行深度防御Defense in depth across your database fleet – on-premises and in the cloud

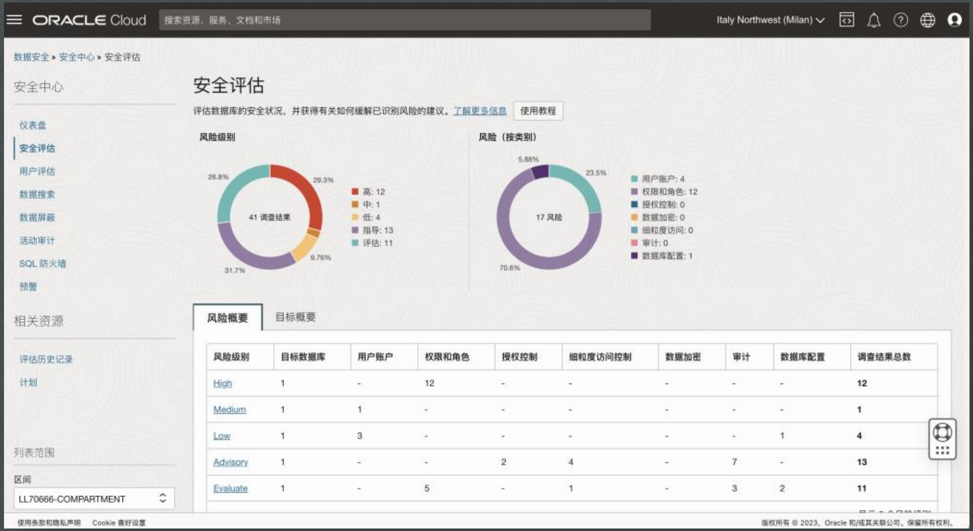
- 节省时间，降低安全风险Saves time and mitigates security risks
- 不需要特殊的安全专业知识No special security expertise needed

包含在所有数据库服务中Included with all database services

快速简易地注册自治数据库Quick and easy to register Autonomous Databases



数据库安全评估Database Security Assessment



数据安全 » 安全中心 » 安全评估

安全中心

- 仪表盘
- 安全评估
- 用户评估
- 数据搜索
- 数据屏蔽
- 活动审计
- SQL 防火墙
- 预警

相关资源

- 评估历史记录
- 计划

列表范围

区间

LL70666-COMPARTMENT

安全评估

评估数据库的安全状况，并获得有关如何缓解已识别风险的建议。了解更多信息 使用教程

风险级别

- 🟥 高: 12
- 🟧 中: 1
- 🟨 低: 4
- 🟪 指导: 13
- 🟦 评估: 11

风险（按类别）

- 🟦 用户账户: 4
- 🟪 权限和角色: 12
- 🟦 授权控制: 0
- 🟧 数据加密: 0
- 🟦 细粒度访问: 0
- 🟥 审计: 0
- 🟪 数据库配置: 1

风险概要 | 目标概要

风险级别	目标数据库	用户账户	权限和角色	授权控制	细粒度访问控制	数据加密	审计	数据库配置	调查结果总数
High	1	-	12	-	-	-	-	-	**12**
Medium	1	1	-	-	-	-	-	-	**1**
Low	1	3	-	-	-	-	-	1	**4**
Advisory	1	-	-	2	4	-	7	-	**13**
Evaluate	1	-	5	-	1	-	3	2	**11**

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

包括自治数据库特定的检查和建议

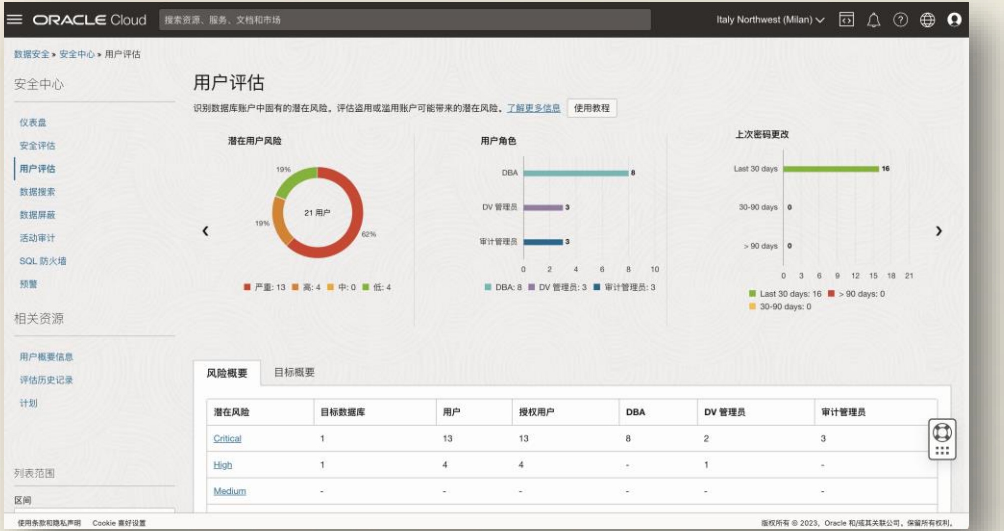
Including Autonomous Databases specific checks and recommendations

检查数据库配置，分析用户角色和权限，并确定正在使用(重要的是没有使用)哪些安全控制。

Checks database configuration, analyzes user roles and privileges and identifies which security controls are (and importantly are NOT) in use.

- 全面的评估Comprehensive assessment
- 识别偏离基线的漂移Identify drift from baseline
- 可操作报告(CIS、STIG和EU GDPR)Actionable reports (CIS, STIG, and EU GDPR)

用户风险评估User Risk Assessment



用户评估

识别数据库账户中固有的潜在风险。评估盗用或滥用账户可能带来的潜在风险。了解更多信息 使用教程

潜在风险	目标数据库	用户	授权用户	DBA	DV 管理员	审计管理员
Critical	1	13	13	8	2	3
High	1	4	4	-	1	-
Medium	-	-	-	-	-	-

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

深入了解数据库帐户的详细信息—包括查看帐户授予的角色、系统特权和审计活动

Drill-down for details on database accounts – including viewing granted roles, system privileges, and audited activity by the account

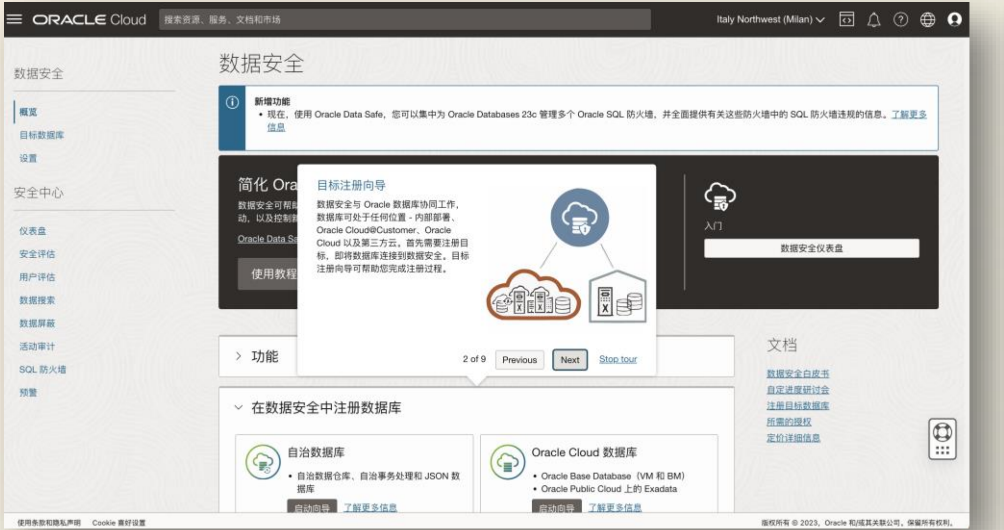
评估数据库并突出显示可能构成风险的帐户

Assesses the database and highlights accounts that could pose a risk

- 识别权限过大的用户Identify over-privileged users
- 识别有风险的用户ProfileIdentify risky user profiles
- 评估静态和动态ProfileEvaluate static and dynamic profile
- 识别偏离基线的漂移Identify drift from baseline
- 用可操作的信息降低风险Reduce risk with actionable information

演示DEMO

目标注册



ORACLE Cloud 搜索资源、服务、文档和市场 Italy Northwest (Milan)

数据安全

- 概览
- 目标数据库
- 设置

安全中心

- 仪表盘
- 安全评估
- 用户评估
- 数据搜索
- 数据屏蔽
- 活动审计
- SQL 防火墙
- 预警

数据安全

新增功能

- 现在，使用 Oracle Data Safe，您可以集中为 Oracle Databases 23c 管理多个 Oracle SQL 防火墙，并全面提供有关这些防火墙中的 SQL 防火墙违规的信息。了解更多信息

简化 Ora

数据安全可帮助
动，以及控制

Oracle Data Sa

使用教程

目标注册向导

数据安全与 Oracle 数据库协同工作，数据库可处于任何位置 - 内部部署、Oracle Cloud@Customer、Oracle Cloud 以及第三方云。首先需要注册目标，即将数据库连接到数据安全。目标注册向导可帮助您完成注册过程。

2 of 9 Previous Next Stop tour

入门

数据安全仪表盘

› 功能

⌄ 在数据安全中注册数据库

自治数据库

- 自治数据仓库、自治事务处理和 JSON 数据库

启动向导 了解更多信息

Oracle Cloud 数据库

- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

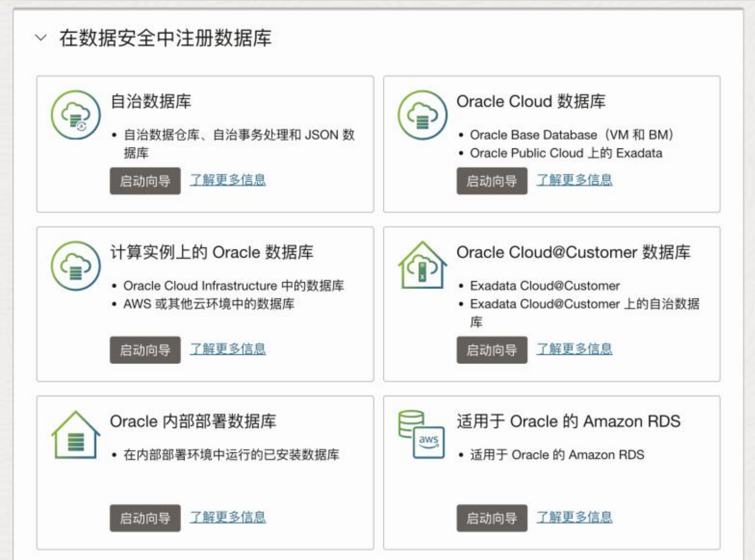
启动向导 了解更多信息

文档

- 数据安全白皮书
- 自定进度研讨会
- 注册目标数据库
- 所需的授权
- 定价详细信息

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。



⌄ 在数据安全中注册数据库

自治数据库

- 自治数据仓库、自治事务处理和 JSON 数据库

启动向导 了解更多信息

Oracle Cloud 数据库

- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

启动向导 了解更多信息

计算实例上的 Oracle 数据库

- Oracle Cloud Infrastructure 中的数据库
- AWS 或其他云环境中的数据库

启动向导 了解更多信息

Oracle Cloud@Customer 数据库

- Exadata Cloud@Customer
- Exadata Cloud@Customer 上的自治数据库

启动向导 了解更多信息

Oracle 内部部署数据库

- 在内部部署环境中运行的已安装数据库

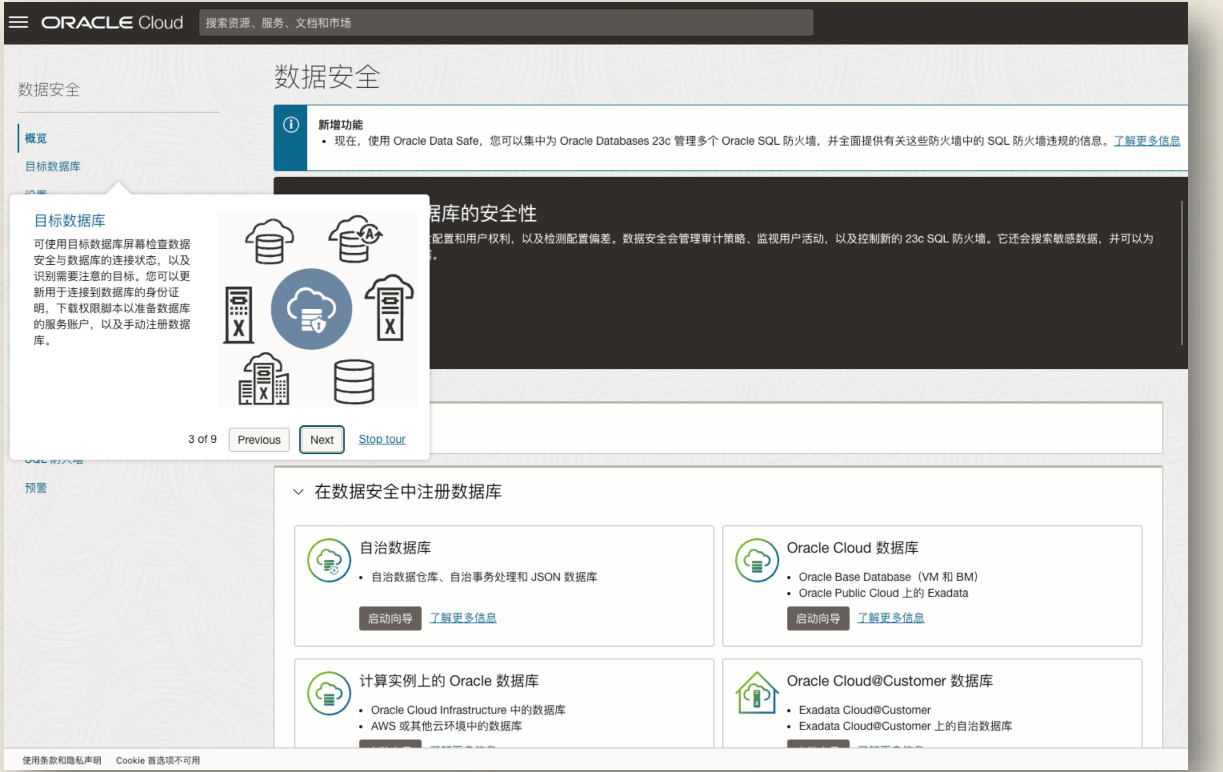
启动向导 了解更多信息

适用于 Oracle 的 Amazon RDS

- 适用于 Oracle 的 Amazon RDS

启动向导 了解更多信息

目标数据库



数据安全

- 概览
- 目标数据库
- 设置
- SQL 防火墙
- 预警

数据安全

新增功能

- 现在，使用 Oracle Data Safe，您可以集中为 Oracle Databases 23c 管理多个 Oracle SQL 防火墙，并全面提供有关这些防火墙中的 SQL 防火墙违规的信息。了解更多信息

据库的安全性

配置和用户权利，以及检测配置偏差。数据安全会管理审计策略、监视用户活动，以及控制新的 23c SQL 防火墙。它还会搜索敏感数据，并可以为

。

目标数据库

可使用目标数据库屏幕检查数据安全与数据库的连接状态，以及识别需要注意的目标。您可以更新用于连接到数据库的身份证明，下载权限脚本以准备数据库的服务账户，以及手动注册数据库。

在数据安全中注册数据库

自治数据库

- 自治数据仓库、自治事务处理和 JSON 数据库

Oracle Cloud 数据库

- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

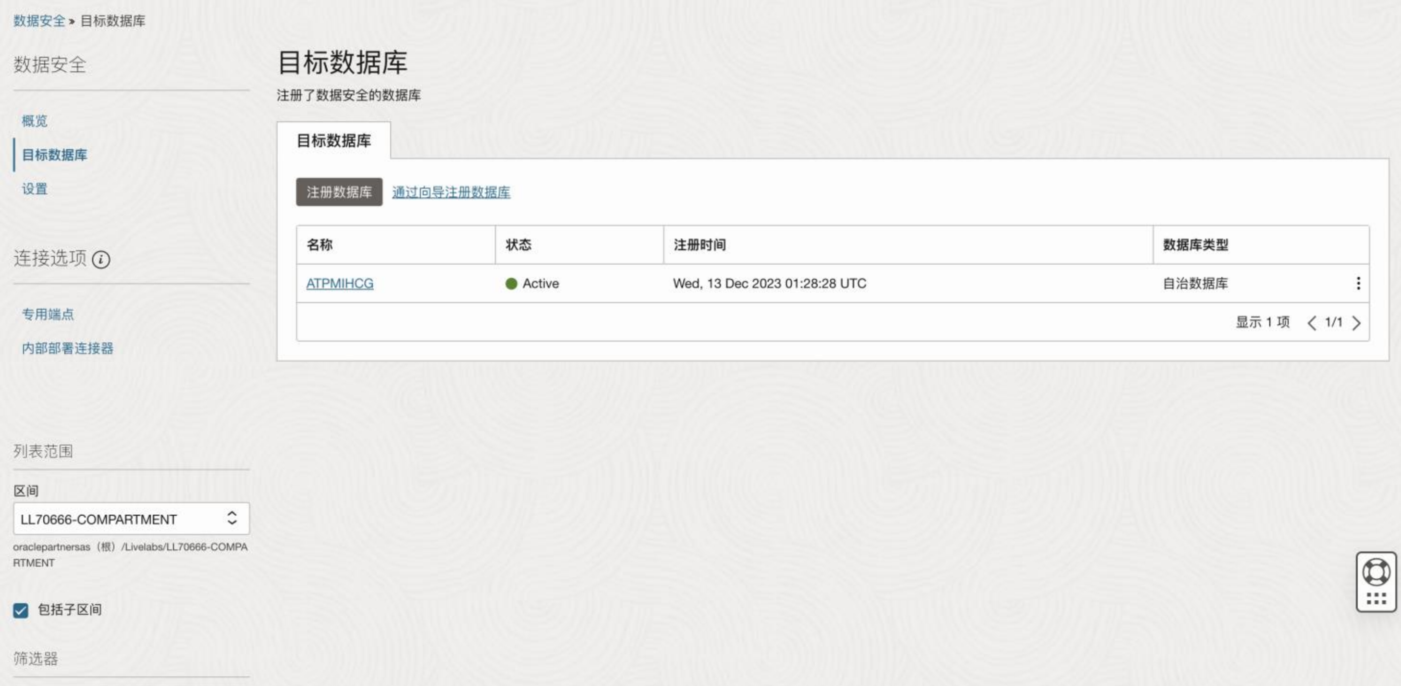
计算实例上的 Oracle 数据库

- Oracle Cloud Infrastructure 中的数据库
- AWS 或其他云环境中的数据库

Oracle Cloud@Customer 数据库

- Exadata Cloud@Customer
- Exadata Cloud@Customer 上的自治数据库

目标数据库



数据安全 » 目标数据库

数据安全

- 概览
- 目标数据库
- 设置

连接选项 ⓘ

- 专用端点
- 内部部署连接器

列表范围

区间

LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

☑ 包括子区间

筛选器

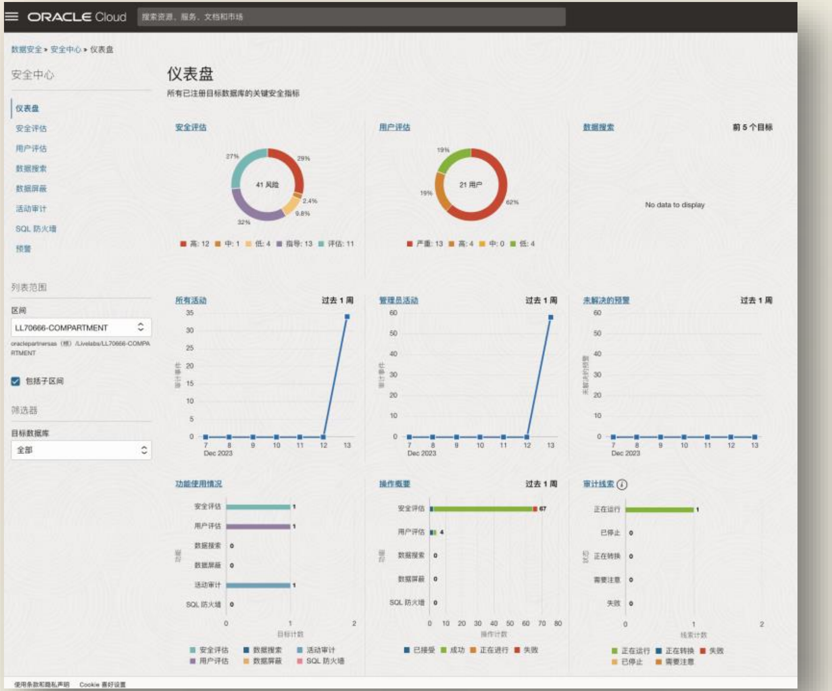
目标数据库

注册了数据安全的数据库

名称	状态	注册时间	数据库类型
ATPMIHCG	● Active	Wed, 13 Dec 2023 01:28:28 UTC	自治数据库

显示 1 项 < 1/1 >

安全中心 – 仪表盘



ORACLE Cloud　搜索资源、服务、文档和市场

数据安全 ▸ 安全中心 ▸ 仪表盘

安全中心

- 仪表盘
- 安全评估
- 用户评估
- 数据搜索
- 数据屏蔽
- 活动审计
- SQL 防火墙
- 预警

列表范围

区间

LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

☑ 包括子区间

筛选器

目标数据库

全部

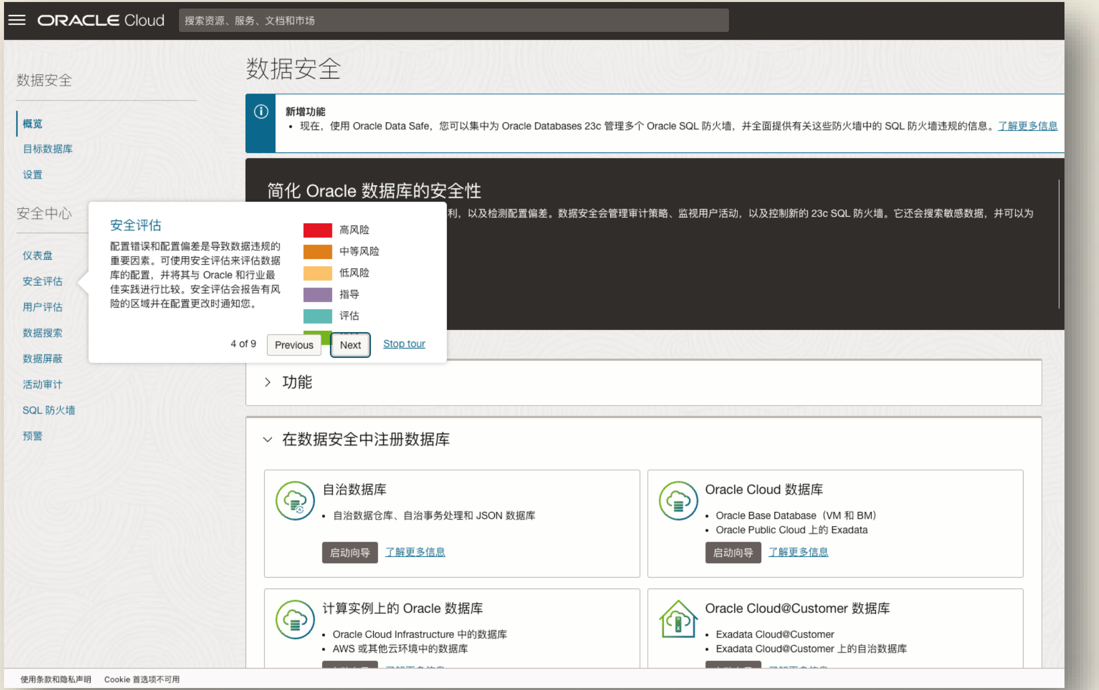
仪表盘

所有已注册目标数据库的关键安全指标

No data to display

使用条款和隐私声明　Cookie 喜好设置

安全中心 – 安全评估



数据安全

新增功能

- 现在，使用 Oracle Data Safe，您可以集中为 Oracle Databases 23c 管理多个 Oracle SQL 防火墙，并全面提供有关这些防火墙中的 SQL 防火墙违规的信息。了解更多信息

简化 Oracle 数据库的安全性

利，以及检测配置偏差。数据安全会管理审计策略、监视用户活动，以及控制新的 23c SQL 防火墙。它还会搜索敏感数据，并可以为

安全评估

配置错误和配置偏差是导致数据违规的重要因素。可使用安全评估来评估数据库的配置，并将其与 Oracle 和行业最佳实践进行比较。安全评估会报告有风险的区域并在配置更改时通知您。

🟥 高风险
🟧 中等风险
🟨 低风险
🟪 指导
🟦 评估

› 功能

⌄ 在数据安全中注册数据库

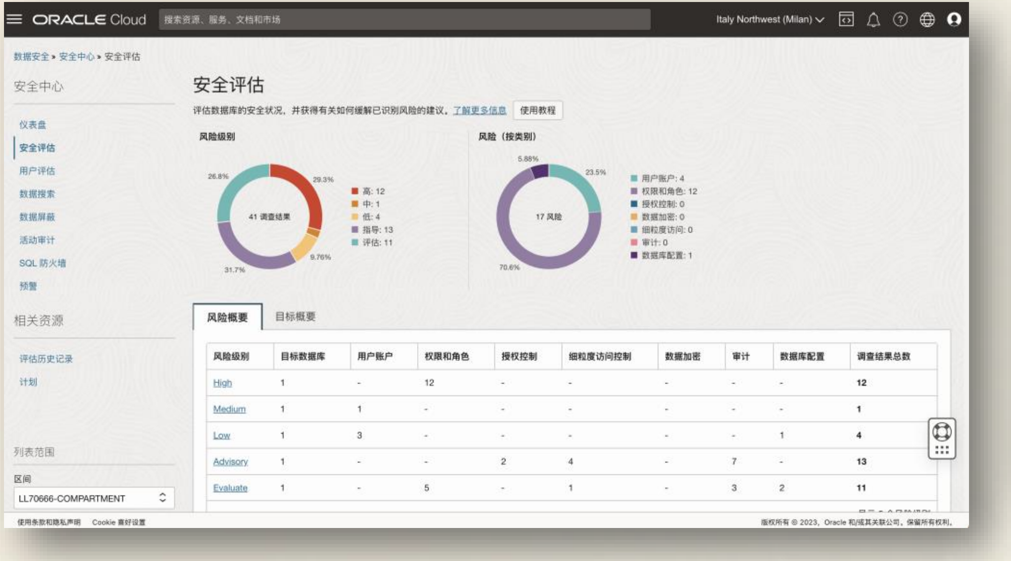
自治数据库
- 自治数据仓库、自治事务处理和 JSON 数据库

Oracle Cloud 数据库
- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

计算实例上的 Oracle 数据库
- Oracle Cloud Infrastructure 中的数据库
- AWS 或其他云环境中的数据库

Oracle Cloud@Customer 数据库
- Exadata Cloud@Customer
- Exadata Cloud@Customer 上的自治数据库

安全中心 – 安全评估

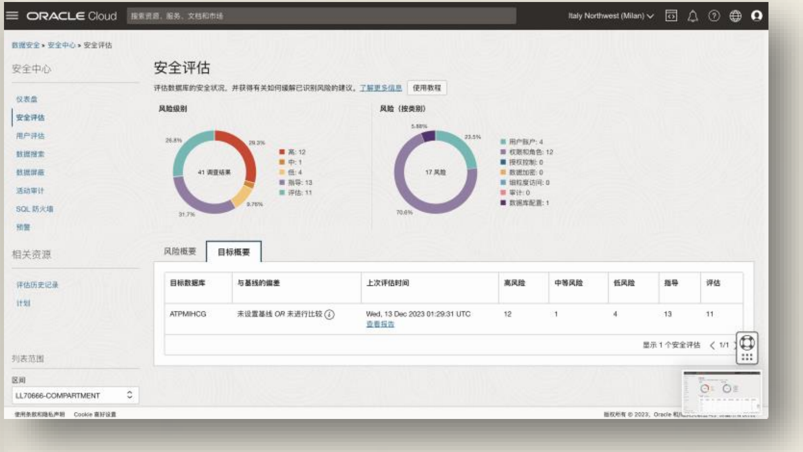


安全评估

评估数据库的安全状况，并获得有关如何缓解已识别风险的建议。了解更多信息 使用教程

风险级别	目标数据库	用户账户	权限和角色	授权控制	细粒度访问控制	数据加密	审计	数据库配置	调查结果总数
High	1	-	12	-	-	-	-	-	**12**
Medium	1	1	-	-	-	-	-	-	**1**
Low	1	3	-	-	-	-	-	1	**4**
Advisory	1	-	-	2	4	-	7	-	**13**
Evaluate	1	-	5	-	1	-	3	2	**11**

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。



安全评估

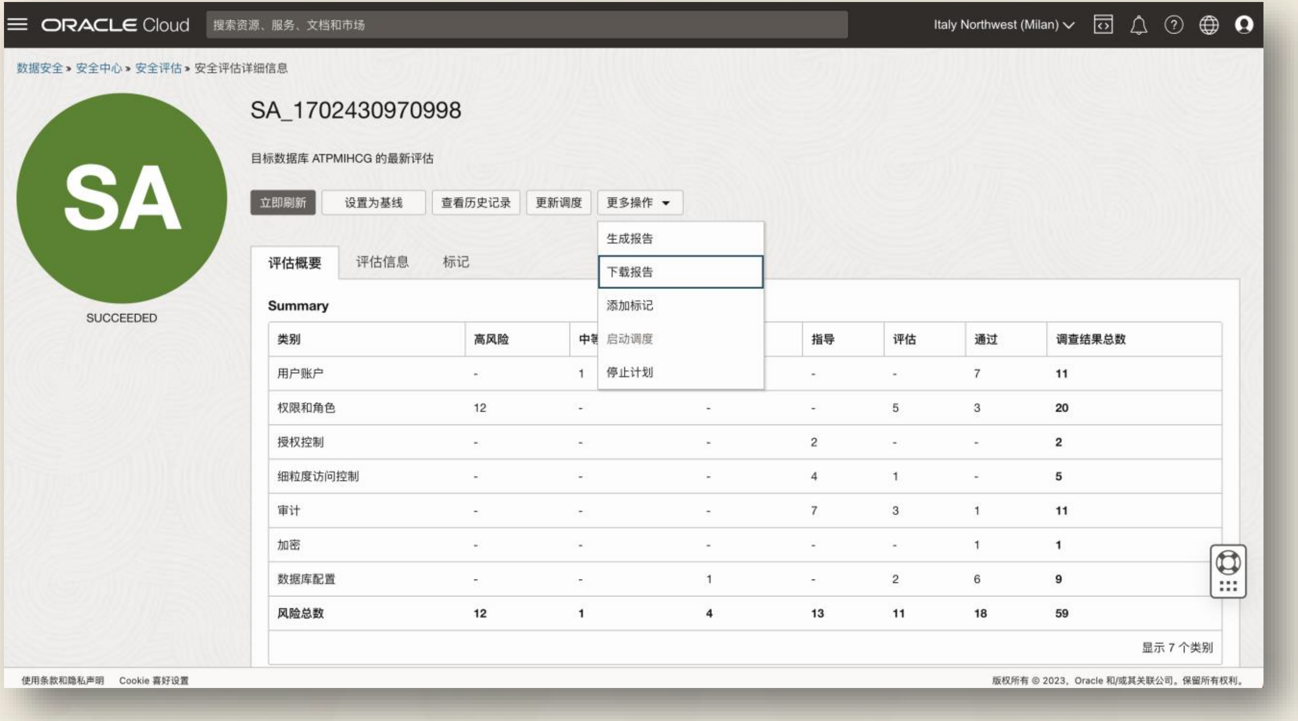
评估数据库的安全状况，并获得有关如何缓解已识别风险的建议。了解更多信息 使用教程

目标数据库	与基线的偏差	上次评估时间	高风险	中等风险	低风险	指导	评估
ATPMIHCG	未设置基线 OR 未进行比较 ⓘ	Wed, 13 Dec 2023 01:29:31 UTC 查看报告	12	1	4	13	11

显示 1 个安全评估 ‹ 1/1 ›

版权所有 © 2023，Oracle 和...

安全中心 – 安全评估 – 评估报告



SA_1702430970998

目标数据库 ATPMIHCG 的最新评估

Summary

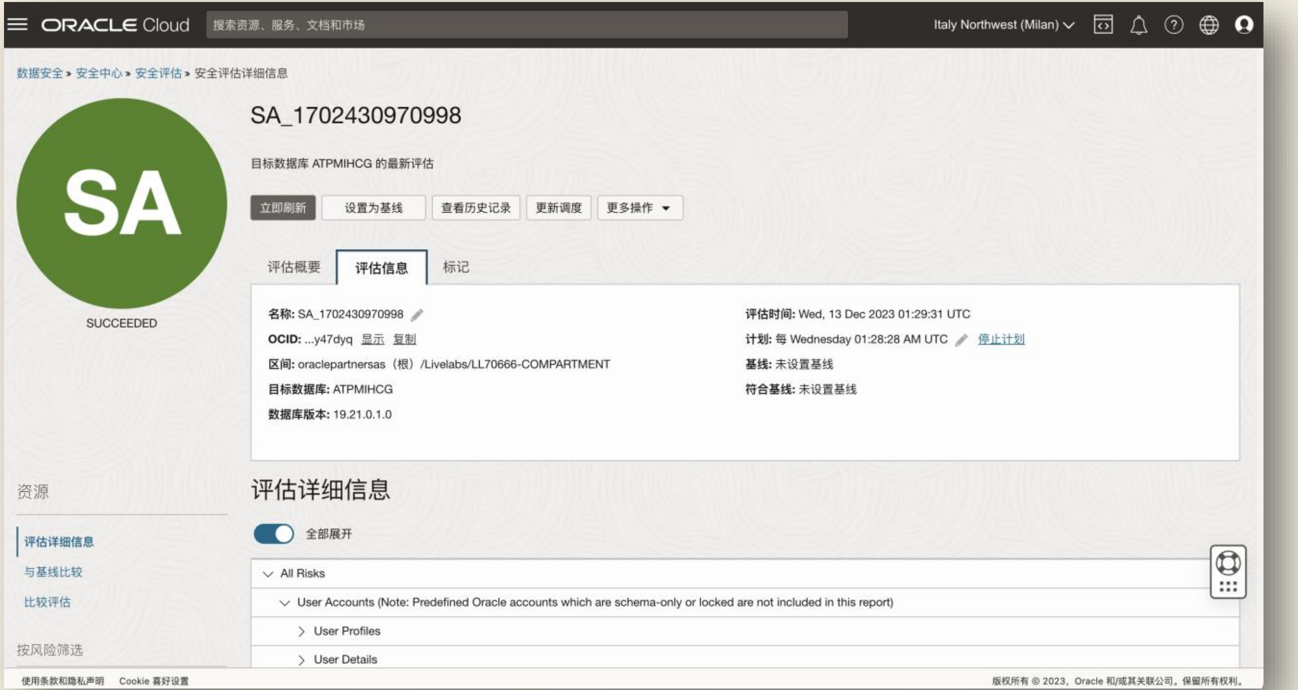
类别	高风险	中等		指导	评估	通过	调查结果总数
用户账户	-	1		-	-	7	**11**
权限和角色	12	-	-	-	5	3	**20**
授权控制	-	-	-	2	-	-	**2**
细粒度访问控制	-	-	-	4	1	-	**5**
审计	-	-	-	7	3	1	**11**
加密	-	-	-	-	-	1	**1**
数据库配置	-	-	1	-	2	6	**9**
风险总数	**12**	**1**	**4**	**13**	**11**	**18**	**59**

显示 7 个类别

使用条款和隐私声明　Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 安全评估 – 评估报告



SUCCEEDED

SA_1702430970998

目标数据库 ATPMIHCG 的最新评估

名称: SA_1702430970998

OCID: ...y47dyq 显示 复制

区间: oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

目标数据库: ATPMIHCG

数据库版本: 19.21.0.1.0

评估时间: Wed, 13 Dec 2023 01:29:31 UTC

计划: 每 Wednesday 01:28:28 AM UTC 停止计划

基线: 未设置基线

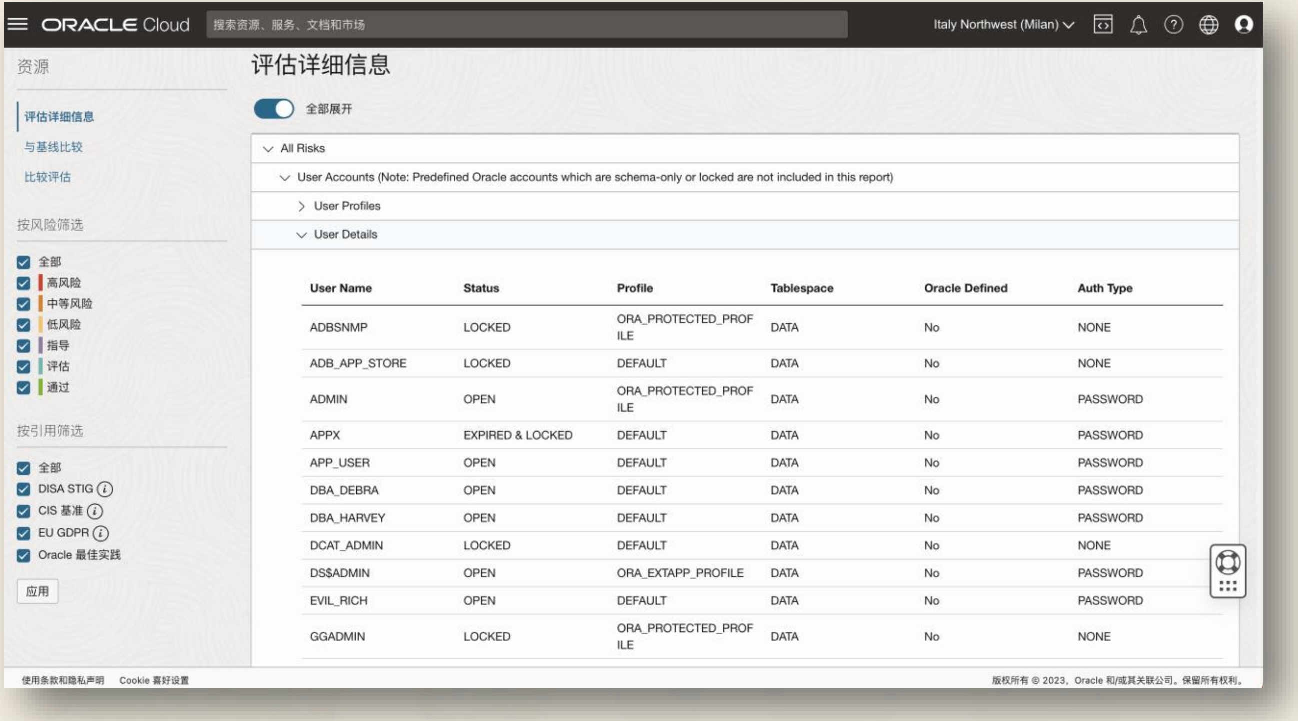
符合基线: 未设置基线

评估详细信息

全部展开

- All Risks
  - User Accounts (Note: Predefined Oracle accounts which are schema-only or locked are not included in this report)
    - User Profiles
    - User Details

安全中心 – 安全评估 – 评估报告



资源

- 评估详细信息
- 与基线比较
- 比较评估

按风险筛选

☑ 全部
☑ 高风险
☑ 中等风险
☑ 低风险
☑ 指导
☑ 评估
☑ 通过

按引用筛选

☑ 全部
☑ DISA STIG ⓘ
☑ CIS 基准 ⓘ
☑ EU GDPR ⓘ
☑ Oracle 最佳实践

应用

评估详细信息

● 全部展开

All Risks

User Accounts (Note: Predefined Oracle accounts which are schema-only or locked are not included in this report)

User Profiles

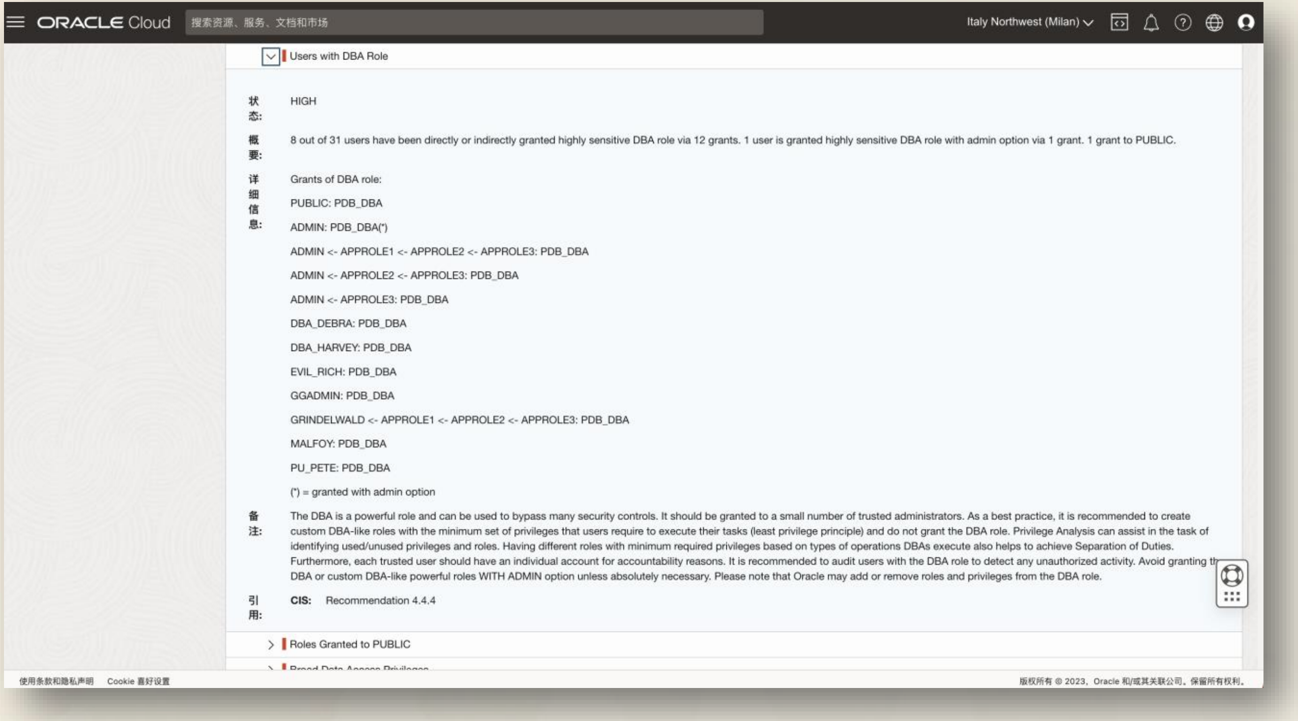
User Details

User Name	Status	Profile	Tablespace	Oracle Defined	Auth Type
ADBSNMP	LOCKED	ORA_PROTECTED_PROFILE	DATA	No	NONE
ADB_APP_STORE	LOCKED	DEFAULT	DATA	No	NONE
ADMIN	OPEN	ORA_PROTECTED_PROFILE	DATA	No	PASSWORD
APPX	EXPIRED & LOCKED	DEFAULT	DATA	No	PASSWORD
APP_USER	OPEN	DEFAULT	DATA	No	PASSWORD
DBA_DEBRA	OPEN	DEFAULT	DATA	No	PASSWORD
DBA_HARVEY	OPEN	DEFAULT	DATA	No	PASSWORD
DCAT_ADMIN	LOCKED	DEFAULT	DATA	No	NONE
DS$ADMIN	OPEN	ORA_EXTAPP_PROFILE	DATA	No	PASSWORD
EVIL_RICH	OPEN	DEFAULT	DATA	No	PASSWORD
GGADMIN	LOCKED	ORA_PROTECTED_PROFILE	DATA	No	NONE

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 安全评估 – 评估报告



Users with DBA Role

状态: HIGH

概要: 8 out of 31 users have been directly or indirectly granted highly sensitive DBA role via 12 grants. 1 user is granted highly sensitive DBA role with admin option via 1 grant. 1 grant to PUBLIC.

详细信息:

```
Grants of DBA role:
PUBLIC: PDB_DBA
ADMIN: PDB_DBA(*)
ADMIN <- APPROLE1 <- APPROLE2 <- APPROLE3: PDB_DBA
ADMIN <- APPROLE2 <- APPROLE3: PDB_DBA
ADMIN <- APPROLE3: PDB_DBA
DBA_DEBRA: PDB_DBA
DBA_HARVEY: PDB_DBA
EVIL_RICH: PDB_DBA
GGADMIN: PDB_DBA
GRINDELWALD <- APPROLE1 <- APPROLE2 <- APPROLE3: PDB_DBA
MALFOY: PDB_DBA
PU_PETE: PDB_DBA
(*) = granted with admin option
```

备注: The DBA is a powerful role and can be used to bypass many security controls. It should be granted to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with the minimum set of privileges that users require to execute their tasks (least privilege principle) and do not grant the DBA role. Privilege Analysis can assist in the task of identifying used/unused privileges and roles. Having different roles with minimum required privileges based on types of operations DBAs execute also helps to achieve Separation of Duties. Furthermore, each trusted user should have an individual account for accountability reasons. It is recommended to audit users with the DBA role to detect any unauthorized activity. Avoid granting th DBA or custom DBA-like powerful roles WITH ADMIN option unless absolutely necessary. Please note that Oracle may add or remove roles and privileges from the DBA role.

引用: **CIS:** Recommendation 4.4.4

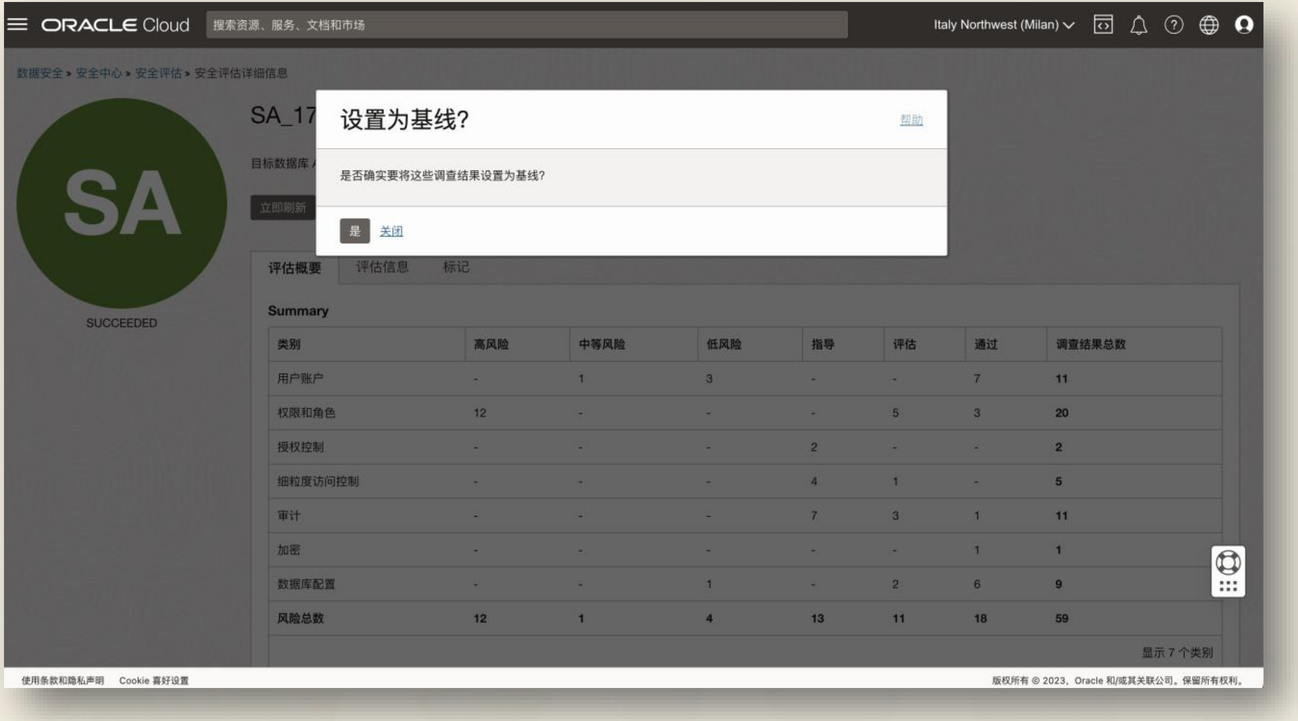
› Roles Granted to PUBLIC

› Broad Data Access Privileges

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 安全评估 – 评估报告 – 基线



设置为基线?

是否确实要将这些调查结果设置为基线?

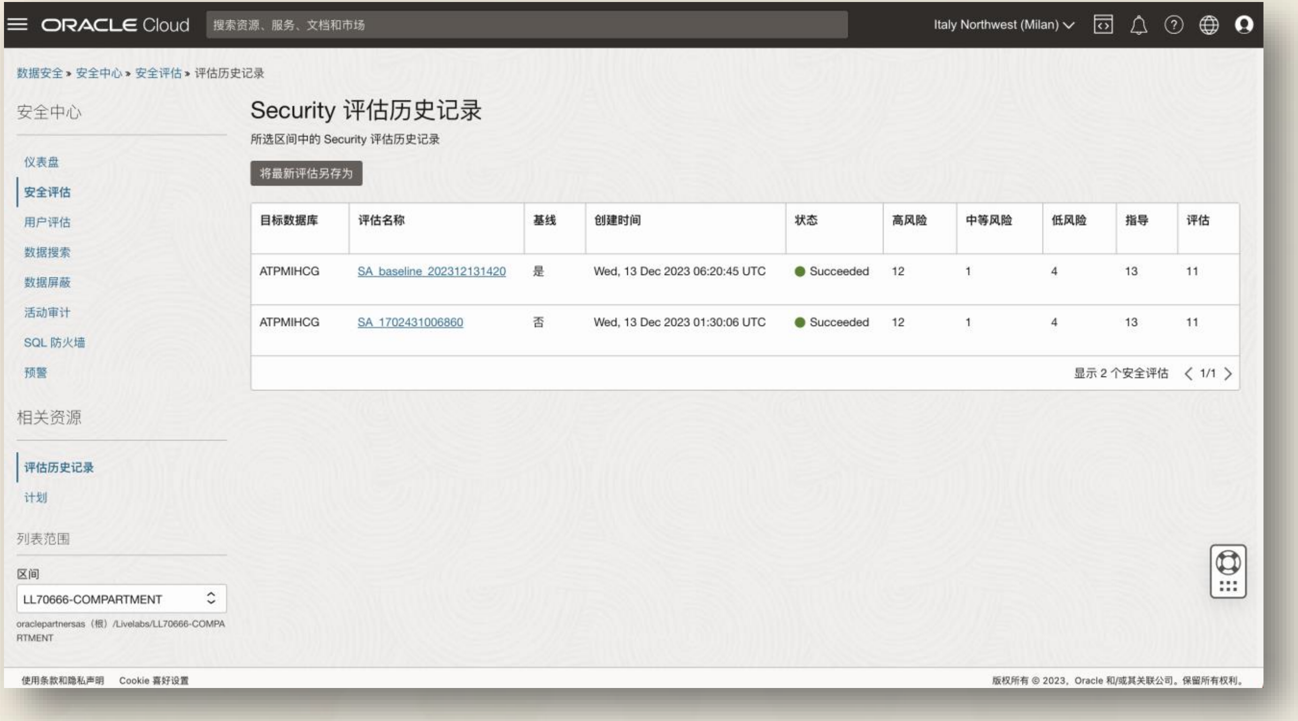
Summary

类别	高风险	中等风险	低风险	指导	评估	通过	调查结果总数
用户账户	-	1	3	-	-	7	**11**
权限和角色	12	-	-	-	5	3	**20**
授权控制	-	-	-	2	-	-	**2**
细粒度访问控制	-	-	-	4	1	-	**5**
审计	-	-	-	7	3	1	**11**
加密	-	-	-	-	-	1	**1**
数据库配置	-	-	1	-	2	6	**9**
风险总数	**12**	**1**	**4**	**13**	**11**	**18**	**59**

显示 7 个类别

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 安全评估 – 评估报告 – 基线



数据安全 » 安全中心 » 安全评估 » 评估历史记录

区间: LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

Security 评估历史记录

所选区间中的 Security 评估历史记录

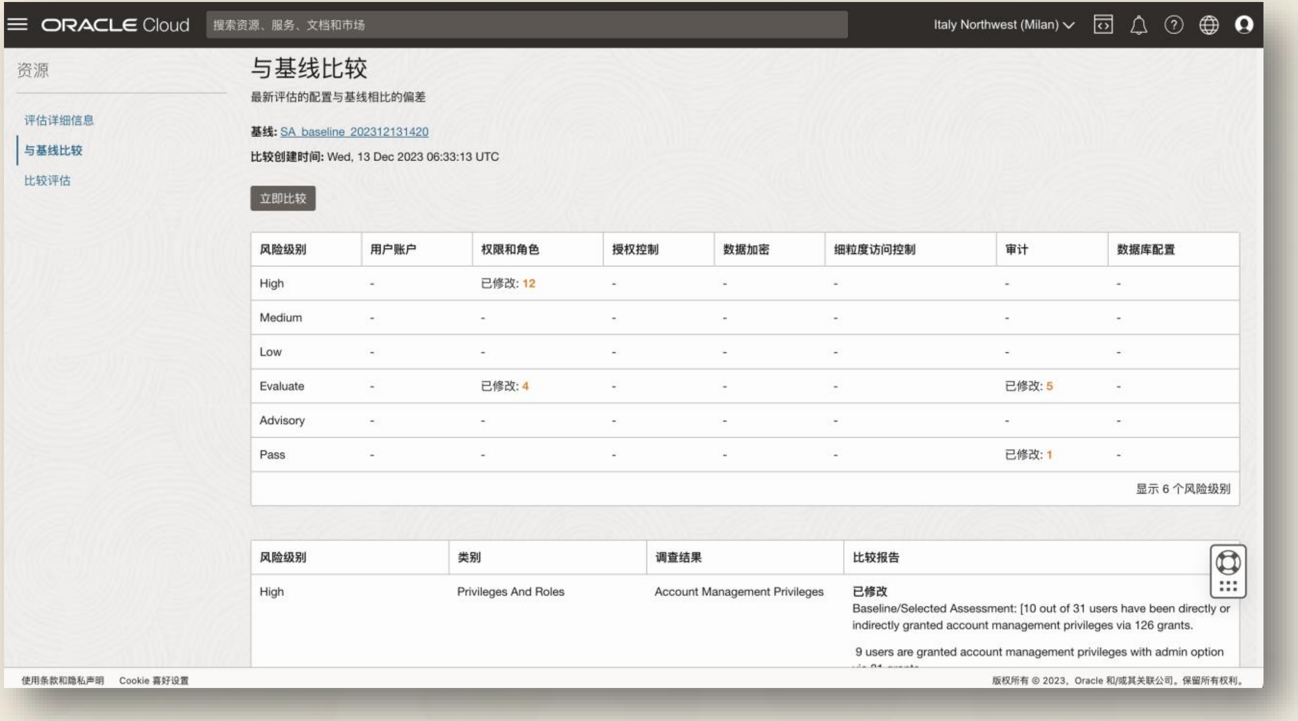
将最新评估另存为

目标数据库	评估名称	基线	创建时间	状态	高风险	中等风险	低风险	指导	评估
ATPMIHCG	SA_baseline_202312131420	是	Wed, 13 Dec 2023 06:20:45 UTC	● Succeeded	12	1	4	13	11
ATPMIHCG	SA_1702431006860	否	Wed, 13 Dec 2023 01:30:06 UTC	● Succeeded	12	1	4	13	11

显示 2 个安全评估 ‹ 1/1 ›

使用条款和隐私声明　Cookie 喜好设置
版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 安全评估 – 评估报告 – 基线



与基线比较

最新评估的配置与基线相比的偏差

基线: SA_baseline_202312131420

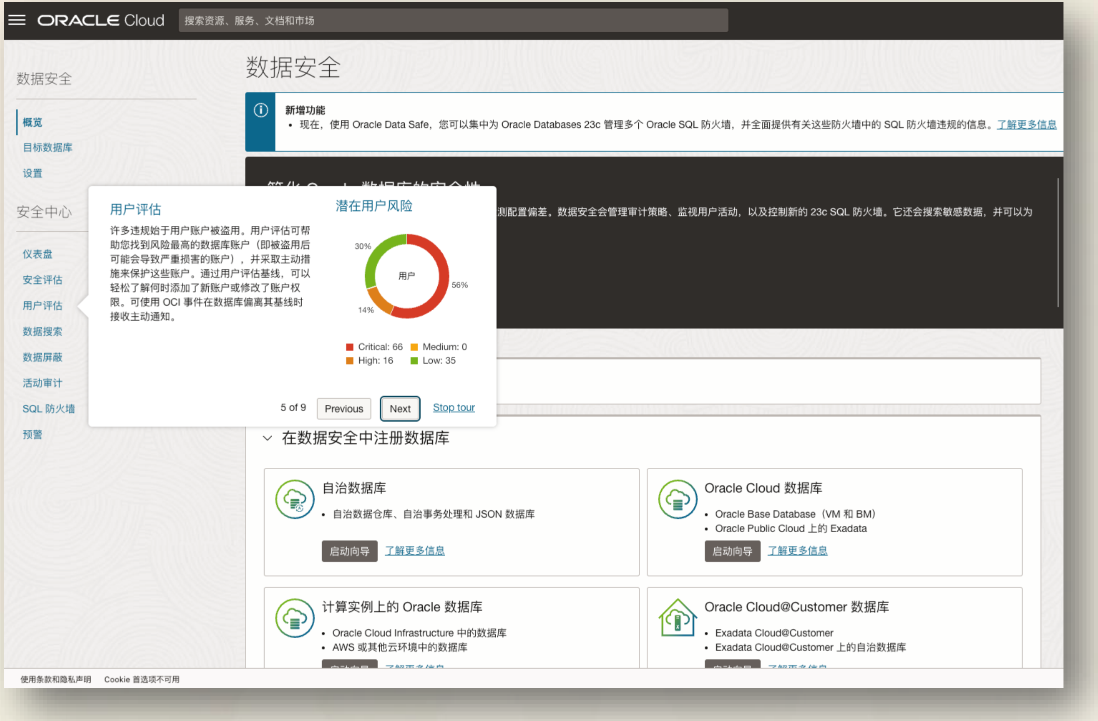
比较创建时间: Wed, 13 Dec 2023 06:33:13 UTC

风险级别	用户账户	权限和角色	授权控制	数据加密	细粒度访问控制	审计	数据库配置
High	-	已修改: 12	-	-	-	-	-
Medium	-	-	-	-	-	-	-
Low	-	-	-	-	-	-	-
Evaluate	-	已修改: 4	-	-	-	已修改: 5	-
Advisory	-	-	-	-	-	-	-
Pass	-	-	-	-	-	已修改: 1	-

显示 6 个风险级别

风险级别	类别	调查结果	比较报告
High	Privileges And Roles	Account Management Privileges	**已修改** Baseline/Selected Assessment: [10 out of 31 users have been directly or indirectly granted account management privileges via 126 grants. 9 users are granted account management privileges with admin option

安全中心 – 用户评估



数据安全

数据安全

安全中心

新增功能

- 现在，使用 Oracle Data Safe，您可以集中为 Oracle Databases 23c 管理多个 Oracle SQL 防火墙，并全面提供有关这些防火墙中的 SQL 防火墙违规的信息。了解更多信息

测配置偏差。数据安全会管理审计策略、监视用户活动，以及控制新的 23c SQL 防火墙。它还会搜索敏感数据，并可以为

用户评估

许多违规始于用户账户被盗用。用户评估可帮助您找到风险最高的数据库账户（即被盗用后可能会导致严重损害的账户），并采取主动措施来保护这些账户。通过用户评估基线，可以轻松了解何时添加了新账户或修改了账户权限。可使用 OCI 事件在数据库偏离其基线时接收主动通知。

潜在用户风险

在数据安全中注册数据库

自治数据库

- 自治数据仓库、自治事务处理和 JSON 数据库

Oracle Cloud 数据库

- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

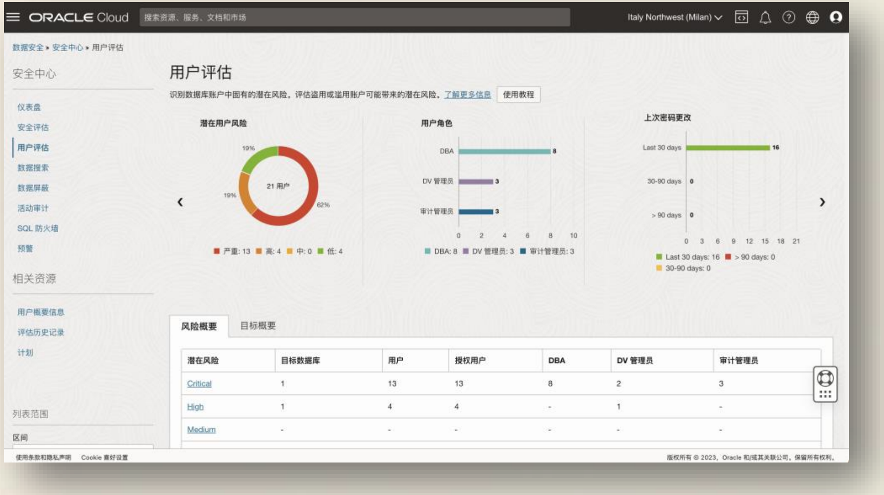
计算实例上的 Oracle 数据库

- Oracle Cloud Infrastructure 中的数据库
- AWS 或其他云环境中的数据库

Oracle Cloud@Customer 数据库

- Exadata Cloud@Customer
- Exadata Cloud@Customer 上的自治数据库

安全中心 – 用户评估

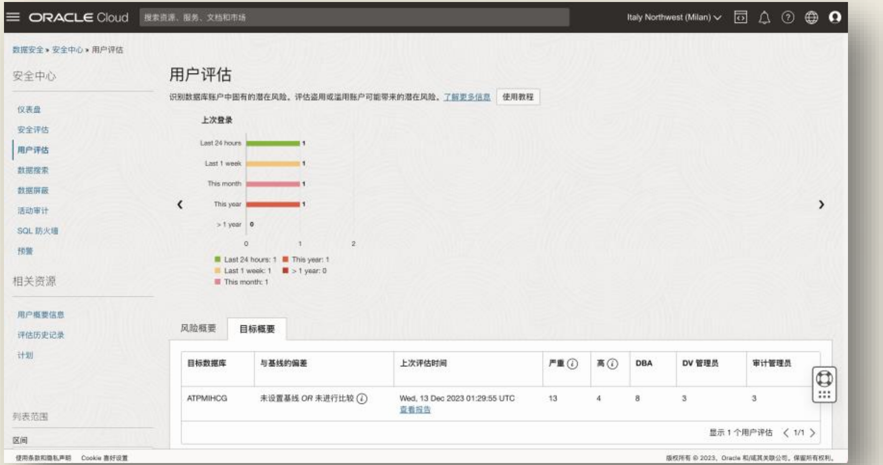


用户评估

识别数据库账户中固有的潜在风险。评估盗用或滥用账户可能带来的潜在风险。了解更多信息 使用教程

潜在风险	目标数据库	用户	授权用户	DBA	DV 管理员	审计管理员
Critical	1	13	13	8	2	3
High	1	4	4	-	1	-
Medium	-	-	-	-	-	-

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。



用户评估

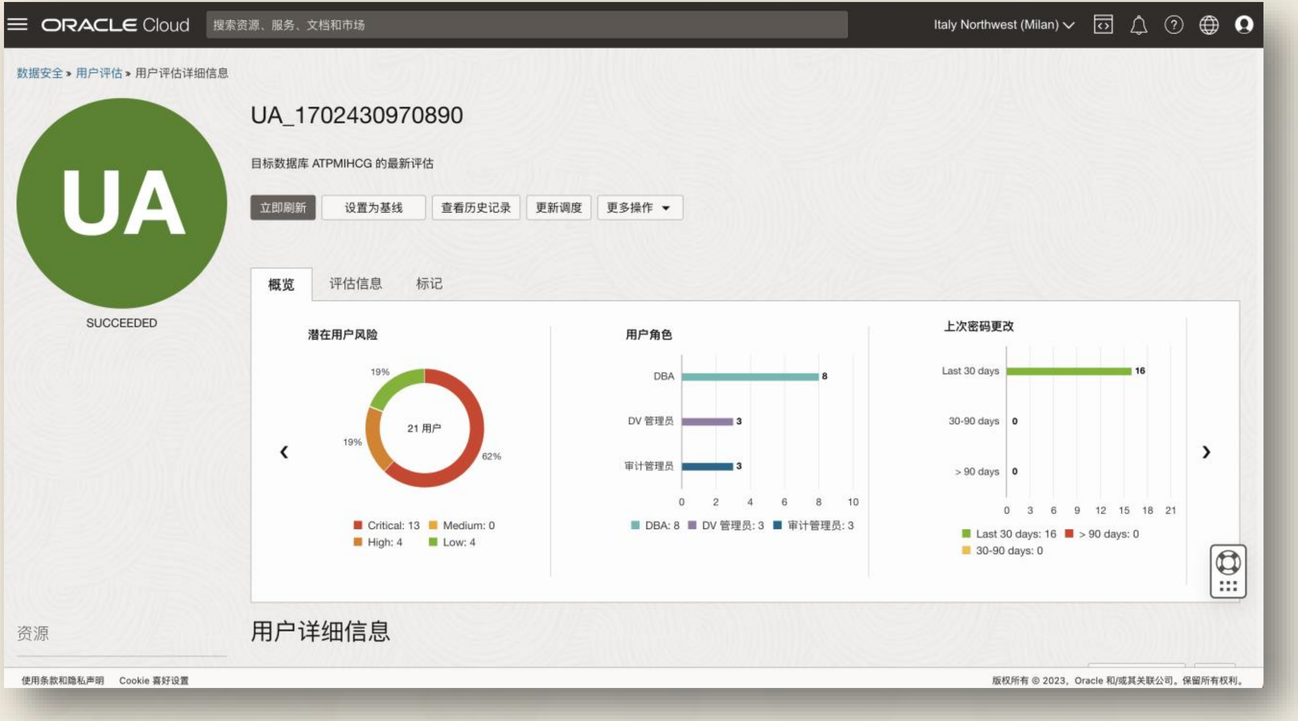
识别数据库账户中固有的潜在风险。评估盗用或滥用账户可能带来的潜在风险。了解更多信息 使用教程

目标数据库	与基线的偏差	上次评估时间	严重 ⓘ	高 ⓘ	DBA	DV 管理员	审计管理员
ATPMIHCG	未设置基线 *OR* 未进行比较 ⓘ	Wed, 13 Dec 2023 01:29:55 UTC 查看报告	13	4	8	3	3

显示 1 个用户评估 〈 1/1 〉

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 用户评估 – 报告



数据安全 » 用户评估 » 用户评估详细信息

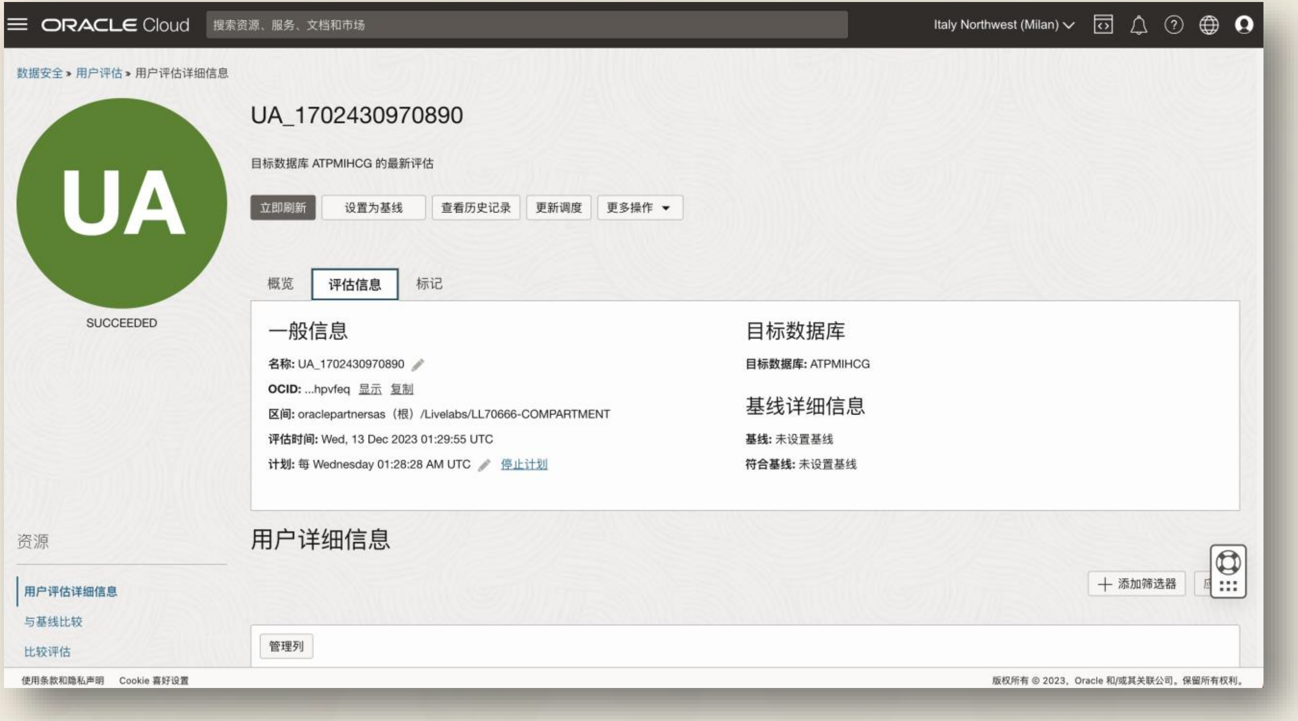
UA_1702430970890

目标数据库 ATPMIHCG 的最新评估

SUCCEEDED

用户详细信息

安全中心 – 用户评估 – 报告



数据安全 » 用户评估 » 用户评估详细信息

UA_1702430970890

目标数据库 ATPMIHCG 的最新评估

一般信息

名称: UA_1702430970890

OCID: ...hpvfeq 显示 复制

区间: oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

评估时间: Wed, 13 Dec 2023 01:29:55 UTC

计划: 每 Wednesday 01:28:28 AM UTC 停止计划

目标数据库

目标数据库: ATPMIHCG

基线详细信息

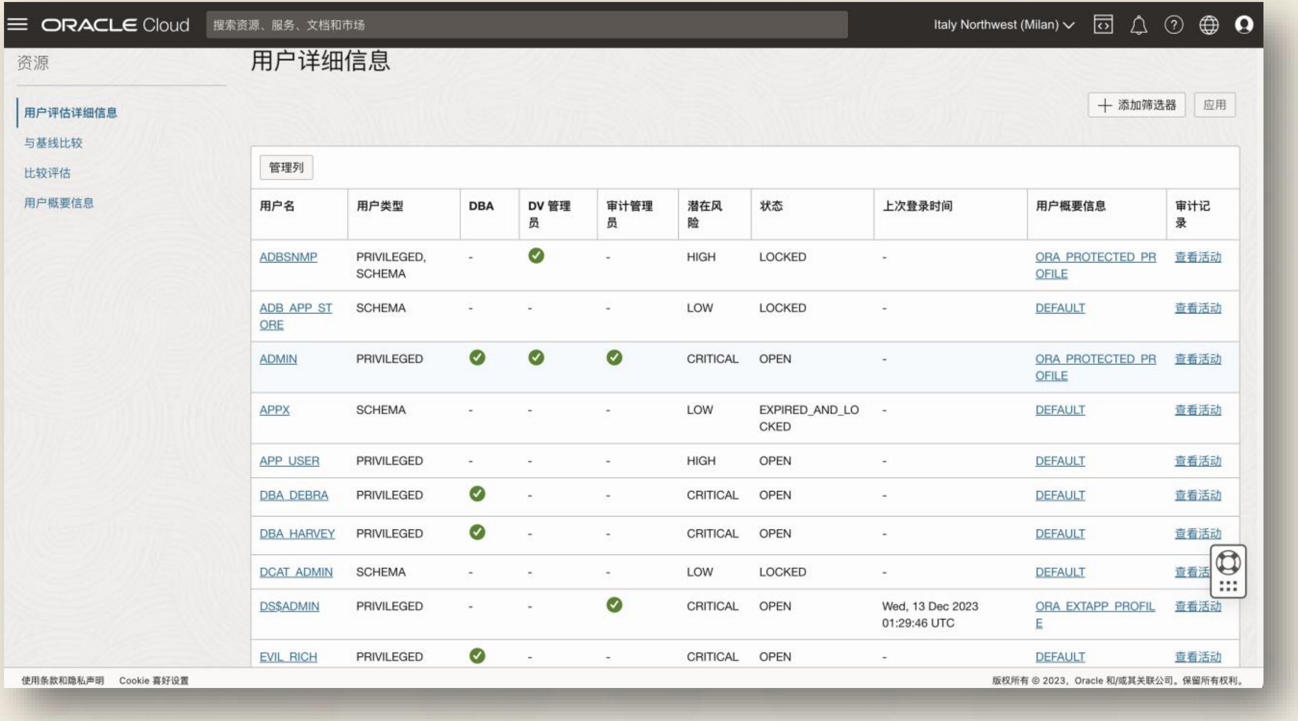
基线: 未设置基线

符合基线: 未设置基线

用户详细信息

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 用户评估 – 报告



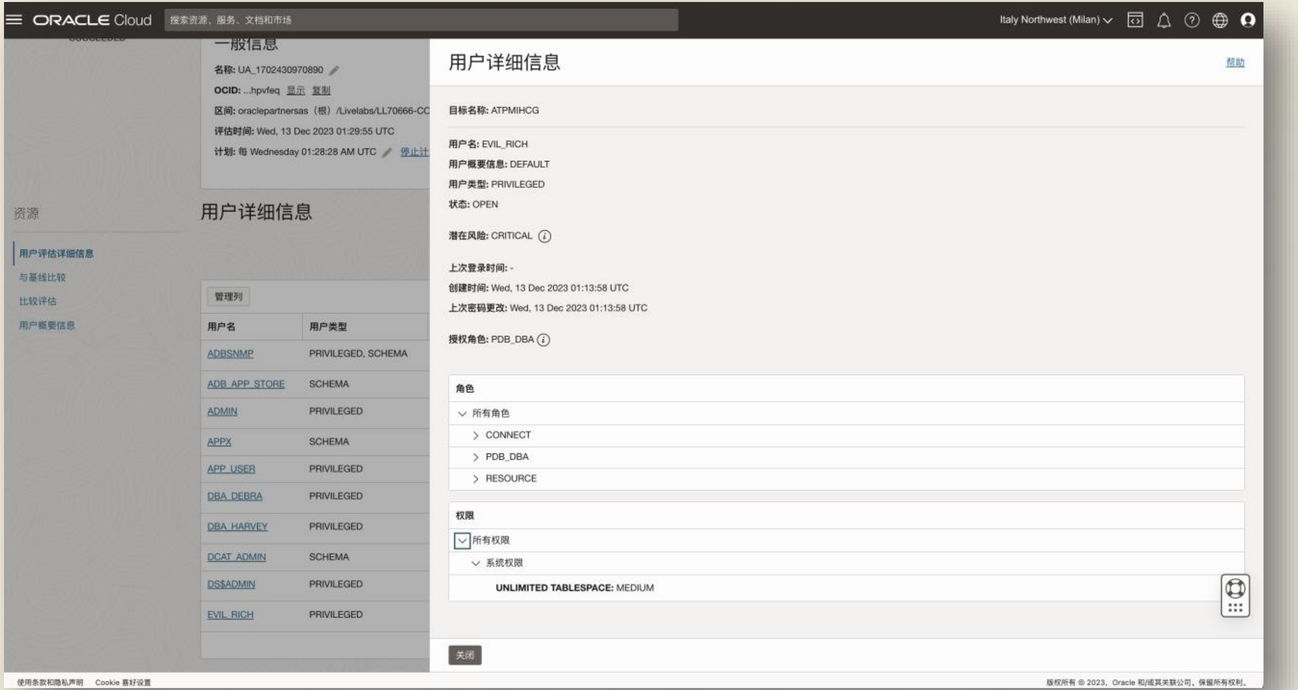
用户详细信息

用户名	用户类型	DBA	DV 管理员	审计管理员	潜在风险	状态	上次登录时间	用户概要信息	审计记录
ADBSNMP	PRIVILEGED, SCHEMA	-	✓	-	HIGH	LOCKED	-	ORA_PROTECTED_PROFILE	查看活动
ADB_APP_STORE	SCHEMA	-	-	-	LOW	LOCKED	-	DEFAULT	查看活动
ADMIN	PRIVILEGED	✓	✓	✓	CRITICAL	OPEN	-	ORA_PROTECTED_PROFILE	查看活动
APPX	SCHEMA	-	-	-	LOW	EXPIRED_AND_LOCKED	-	DEFAULT	查看活动
APP_USER	PRIVILEGED	-	-	-	HIGH	OPEN	-	DEFAULT	查看活动
DBA_DEBRA	PRIVILEGED	✓	-	-	CRITICAL	OPEN	-	DEFAULT	查看活动
DBA_HARVEY	PRIVILEGED	✓	-	-	CRITICAL	OPEN	-	DEFAULT	查看活动
DCAT_ADMIN	SCHEMA	-	-	-	LOW	LOCKED	-	DEFAULT	查看活
DS$ADMIN	PRIVILEGED	-	-	✓	CRITICAL	OPEN	Wed, 13 Dec 2023 01:29:46 UTC	ORA_EXTAPP_PROFILE	查看活动
EVIL_RICH	PRIVILEGED	✓	-	-	CRITICAL	OPEN	-	DEFAULT	查看活动

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 用户评估 – 报告



一般信息

名称: UA_1702430970890

OCID: ...hpvfeq 显示 复制

区间: oraclepartnersas（根）/Livelabs/LL70666-CC

评估时间: Wed, 13 Dec 2023 01:29:55 UTC

计划: 每 Wednesday 01:28:28 AM UTC 停止计

用户详细信息

用户名	用户类型
ADBSNMP	PRIVILEGED, SCHEMA
ADB_APP_STORE	SCHEMA
ADMIN	PRIVILEGED
APPX	SCHEMA
APP_USER	PRIVILEGED
DBA_DEBRA	PRIVILEGED
DBA_HARVEY	PRIVILEGED
DCAT_ADMIN	SCHEMA
DS$ADMIN	PRIVILEGED
EVIL_RICH	PRIVILEGED

用户详细信息

目标名称: ATPMIHCG

用户名: EVIL_RICH
用户概要信息: DEFAULT
用户类型: PRIVILEGED
状态: OPEN

潜在风险: CRITICAL

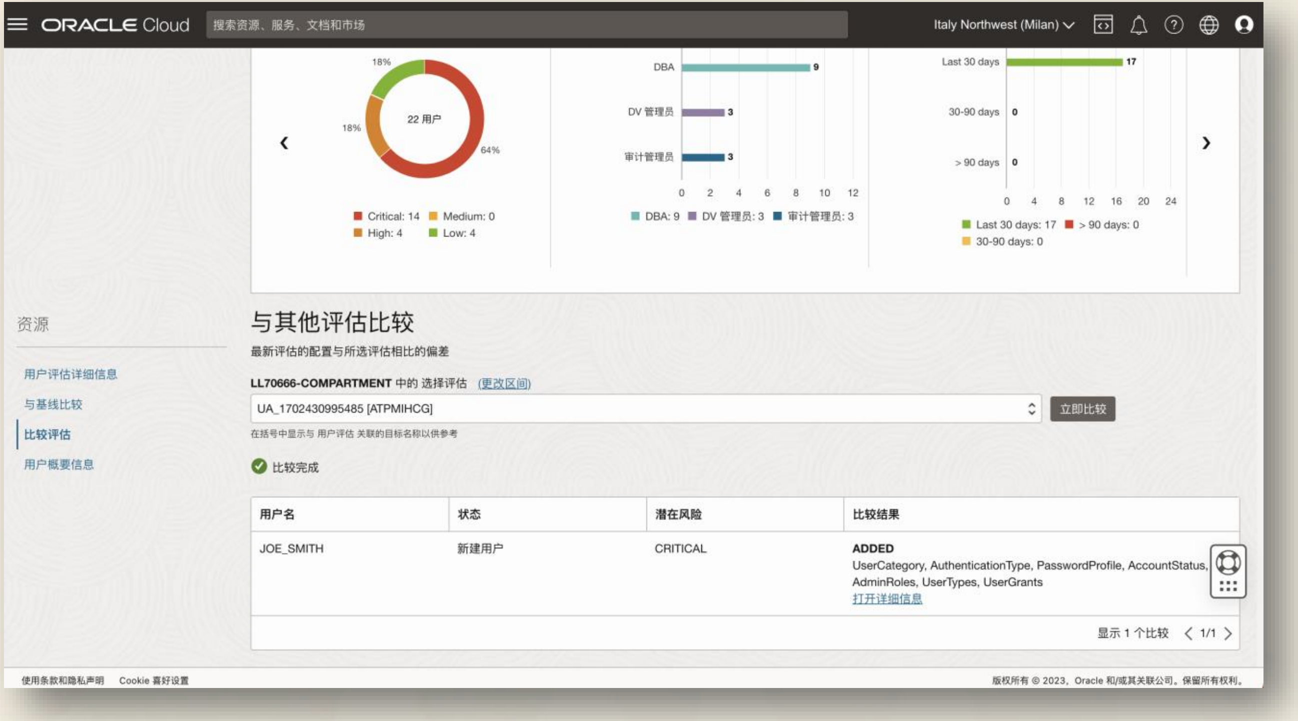
上次登录时间: -
创建时间: Wed, 13 Dec 2023 01:13:58 UTC
上次密码更改: Wed, 13 Dec 2023 01:13:58 UTC

授权角色: PDB_DBA

角色
- 所有角色
  - CONNECT
  - PDB_DBA
  - RESOURCE

权限
- 所有权限
  - 系统权限
    - **UNLIMITED TABLESPACE:** MEDIUM

安全中心 – 用户评估 – 比较评估



与其他评估比较

最新评估的配置与所选评估相比的偏差

LL70666-COMPARTMENT 中的 选择评估 (更改区间)

UA_1702430995485 [ATPMIHCG]

立即比较

在括号中显示与 用户评估 关联的目标名称以供参考

✓ 比较完成

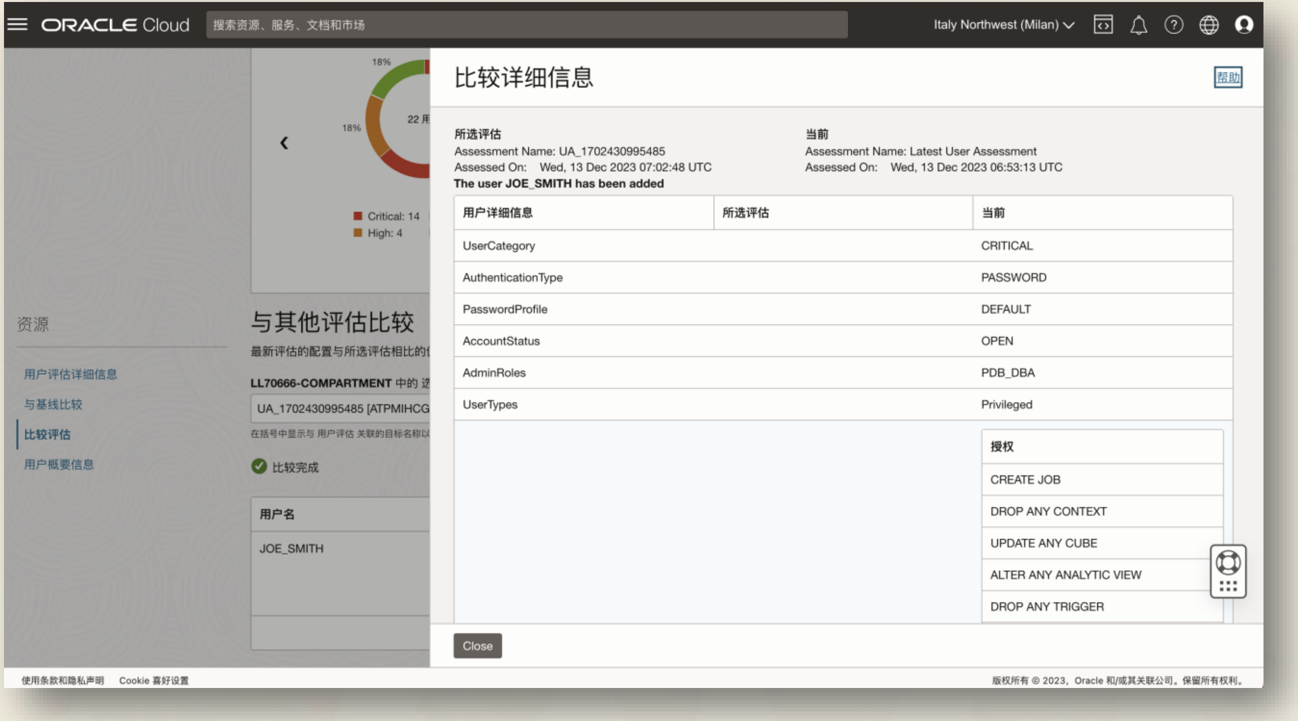
用户名	状态	潜在风险	比较结果
JOE_SMITH	新建用户	CRITICAL	**ADDED** UserCategory, AuthenticationType, PasswordProfile, AccountStatus, AdminRoles, UserTypes, UserGrants 打开详细信息

显示 1 个比较 ‹ 1/1 ›

使用条款和隐私声明 Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 用户评估 – 比较评估



比较详细信息

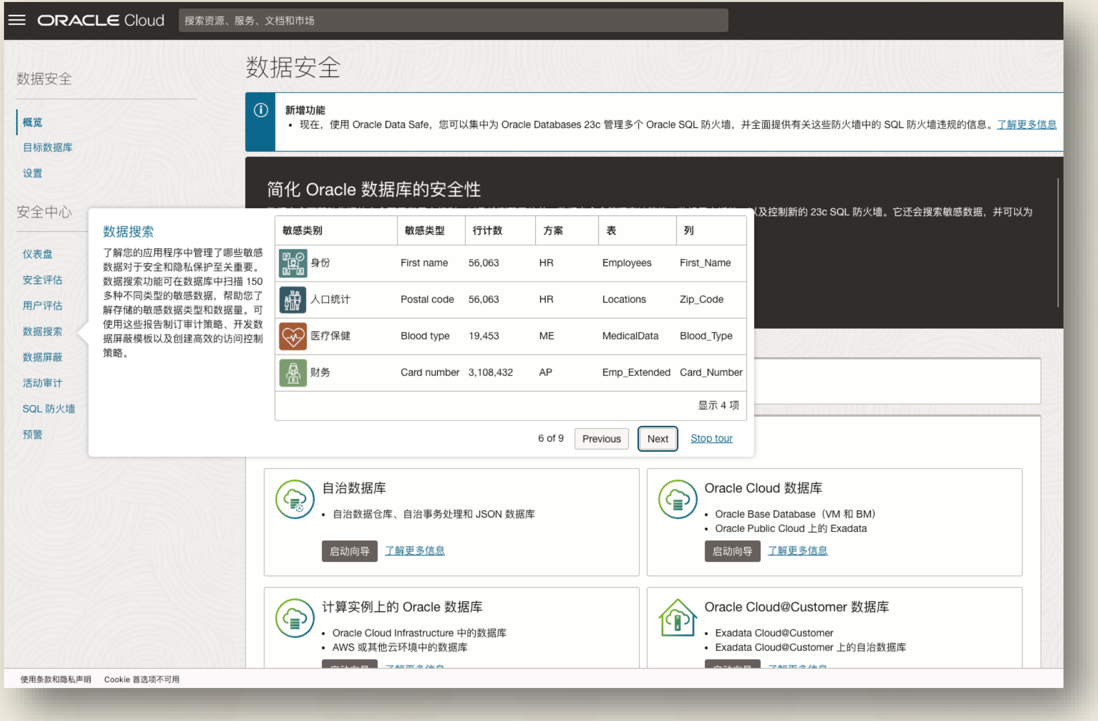
所选评估
Assessment Name: UA_1702430995485
Assessed On: Wed, 13 Dec 2023 07:02:48 UTC

当前
Assessment Name: Latest User Assessment
Assessed On: Wed, 13 Dec 2023 06:53:13 UTC

The user JOE_SMITH has been added

用户详细信息	所选评估	当前
UserCategory		CRITICAL
AuthenticationType		PASSWORD
PasswordProfile		DEFAULT
AccountStatus		OPEN
AdminRoles		PDB_DBA
UserTypes		Privileged
		授权 CREATE JOB DROP ANY CONTEXT UPDATE ANY CUBE ALTER ANY ANALYTIC VIEW DROP ANY TRIGGER

安全中心 – 数据搜索



数据安全

新增功能

- 现在，使用 Oracle Data Safe，您可以集中为 Oracle Databases 23c 管理多个 Oracle SQL 防火墙，并全面提供有关这些防火墙中的 SQL 防火墙违规的信息。了解更多信息

简化 Oracle 数据库的安全性

以及控制新的 23c SQL 防火墙。它还会搜索敏感数据，并可以为

数据搜索

了解您的应用程序中管理了哪些敏感数据对于安全和隐私保护至关重要。数据搜索功能可在数据库中扫描 150 多种不同类型的敏感数据，帮助您了解存储的敏感数据类型和数据量。可使用这些报告制订审计策略、开发数据屏蔽模板以及创建高效的访问控制策略。

敏感类别	敏感类型	行计数	方案	表	列
身份	First name	56,063	HR	Employees	First_Name
人口统计	Postal code	56,063	HR	Locations	Zip_Code
医疗保健	Blood type	19,453	ME	MedicalData	Blood_Type
财务	Card number	3,108,432	AP	Emp_Extended	Card_Number

显示 4 项

自治数据库

- 自治数据仓库、自治事务处理和 JSON 数据库

Oracle Cloud 数据库

- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

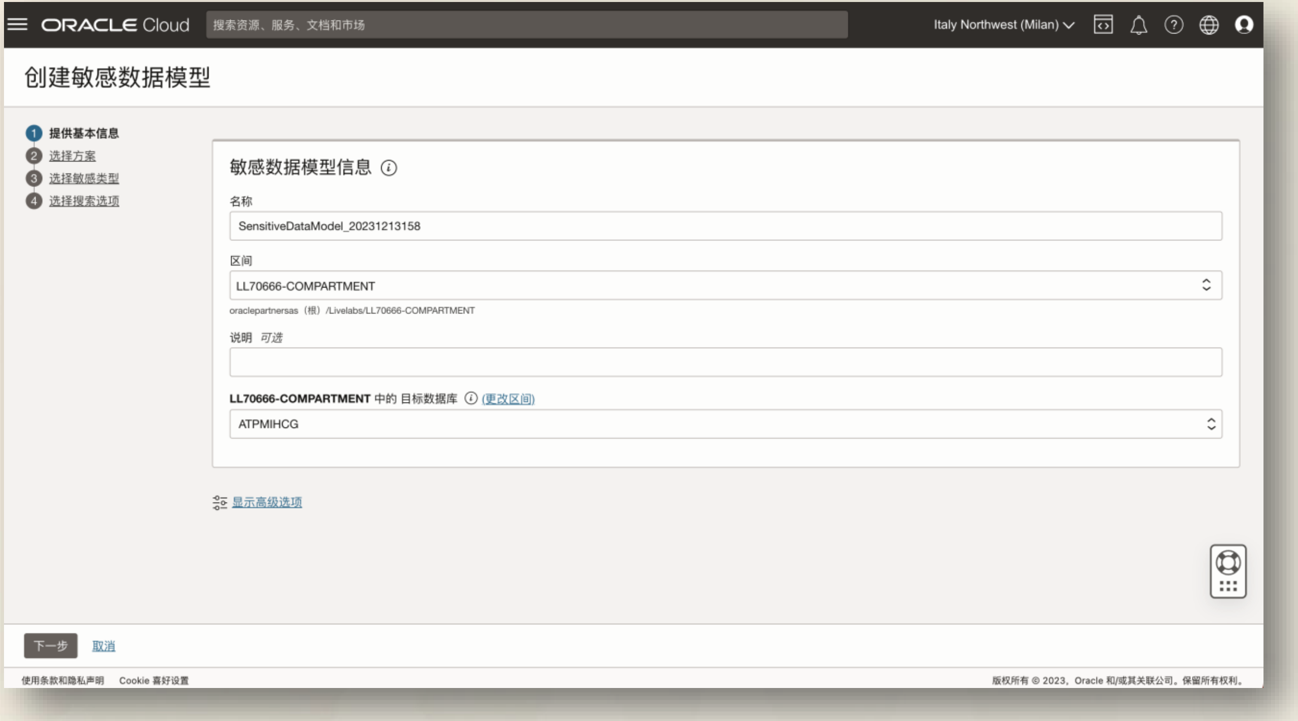
计算实例上的 Oracle 数据库

- Oracle Cloud Infrastructure 中的数据库
- AWS 或其他云环境中的数据库

Oracle Cloud@Customer 数据库

- Exadata Cloud@Customer
- Exadata Cloud@Customer 上的自治数据库

安全中心 – 数据搜索 – 创建敏感数据模型（SDM）



创建敏感数据模型

1. 提供基本信息
2. 选择方案
3. 选择敏感类型
4. 选择搜索选项

敏感数据模型信息

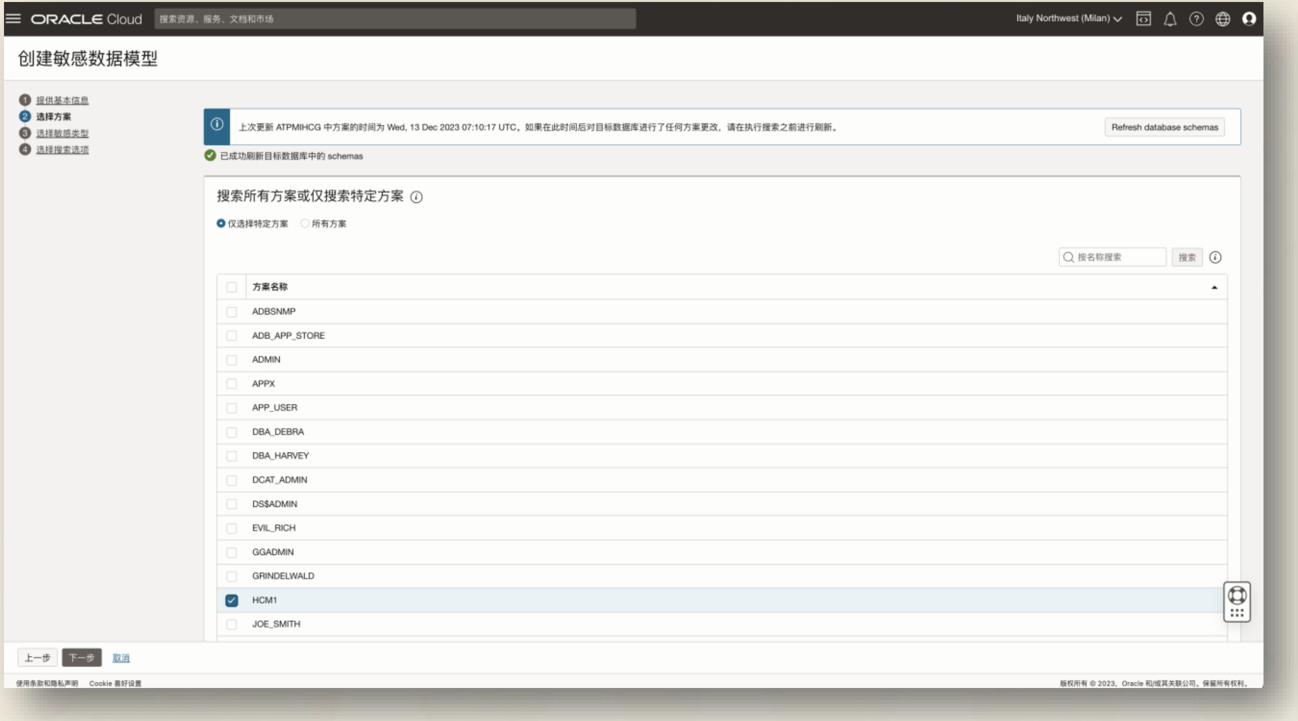
名称
SensitiveDataModel_20231213158

区间
LL70666-COMPARTMENT
oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

说明 可选

LL70666-COMPARTMENT 中的 目标数据库 (更改区间)
ATPMIHCG

安全中心 – 数据搜索 – 创建敏感数据模型（SDM）



创建敏感数据模型

1. 提供基本信息
2. 选择方案
3. 选择敏感类型
4. 选择搜索选项

上次更新 ATPMIHCG 中方案的时间为 Wed, 13 Dec 2023 07:10:17 UTC。如果在此时间后对目标数据库进行了任何方案更改，请在执行搜索之前进行刷新。 Refresh database schemas

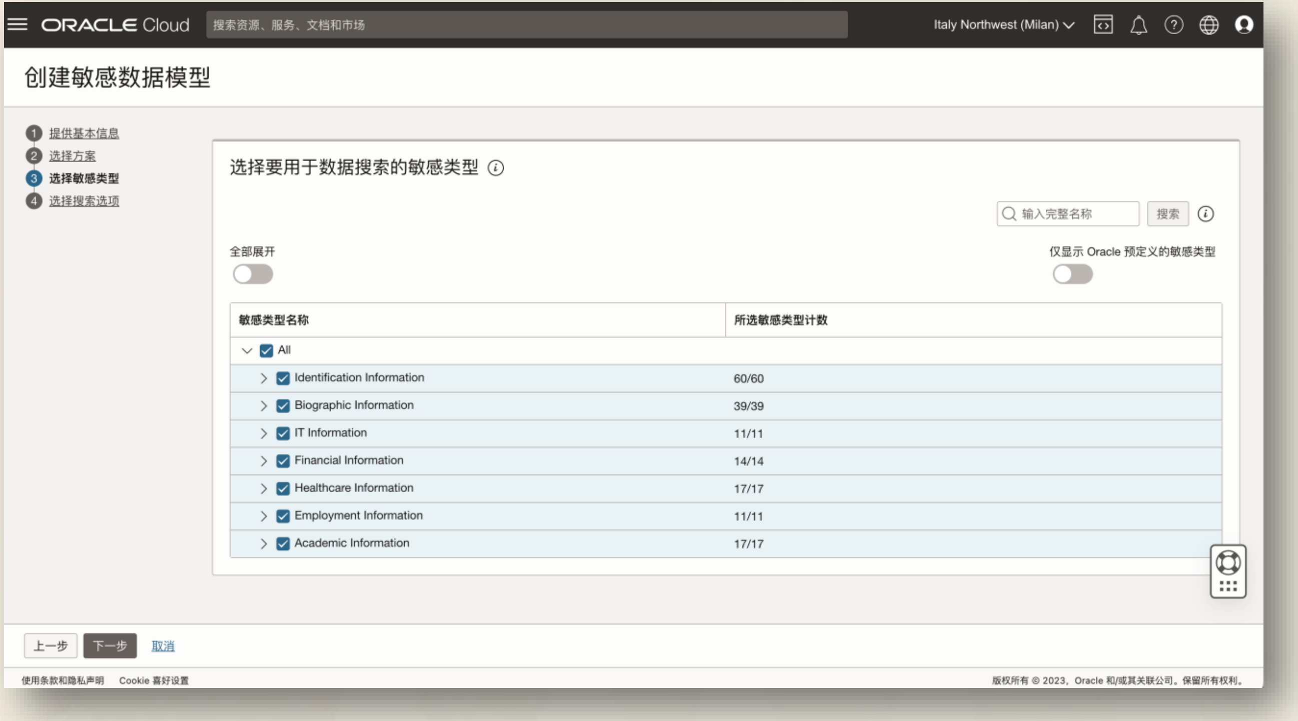
已成功刷新目标数据库中的 schemas

搜索所有方案或仅搜索特定方案

● 仅选择特定方案 ○ 所有方案

□	方案名称
□	ADBSNMP
□	ADB_APP_STORE
□	ADMIN
□	APPX
□	APP_USER
□	DBA_DEBRA
□	DBA_HARVEY
□	DCAT_ADMIN
□	DS$ADMIN
□	EVIL_RICH
□	GGADMIN
□	GRINDELWALD
☑	HCM1
□	JOE_SMITH

安全中心 – 数据搜索 – 创建敏感数据模型（SDM）



创建敏感数据模型

1. 提供基本信息
2. 选择方案
3. 选择敏感类型
4. 选择搜索选项

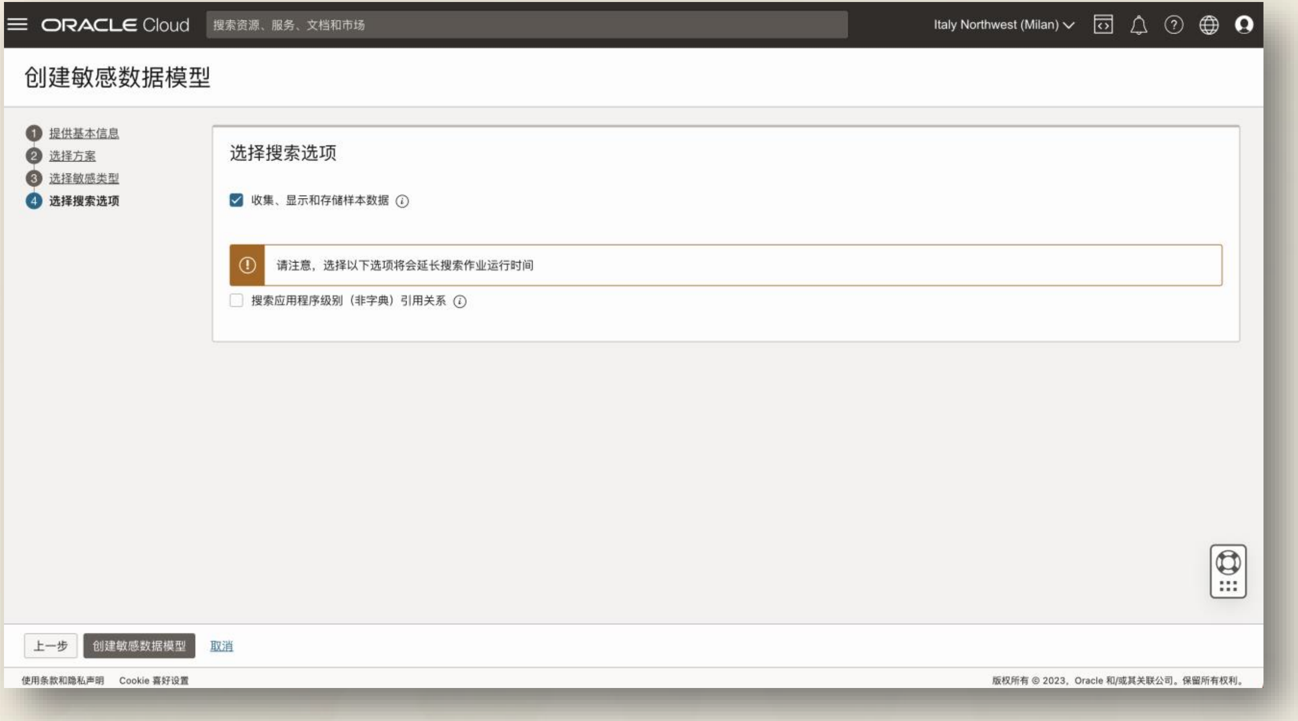
选择要用于数据搜索的敏感类型

全部展开 ○

仅显示 Oracle 预定义的敏感类型 ○

敏感类型名称	所选敏感类型计数
☑ All	
☑ Identification Information	60/60
☑ Biographic Information	39/39
☑ IT Information	11/11
☑ Financial Information	14/14
☑ Healthcare Information	17/17
☑ Employment Information	11/11
☑ Academic Information	17/17

安全中心 – 数据搜索 – 创建敏感数据模型（SDM）



创建敏感数据模型

1. 提供基本信息
2. 选择方案
3. 选择敏感类型
4. 选择搜索选项

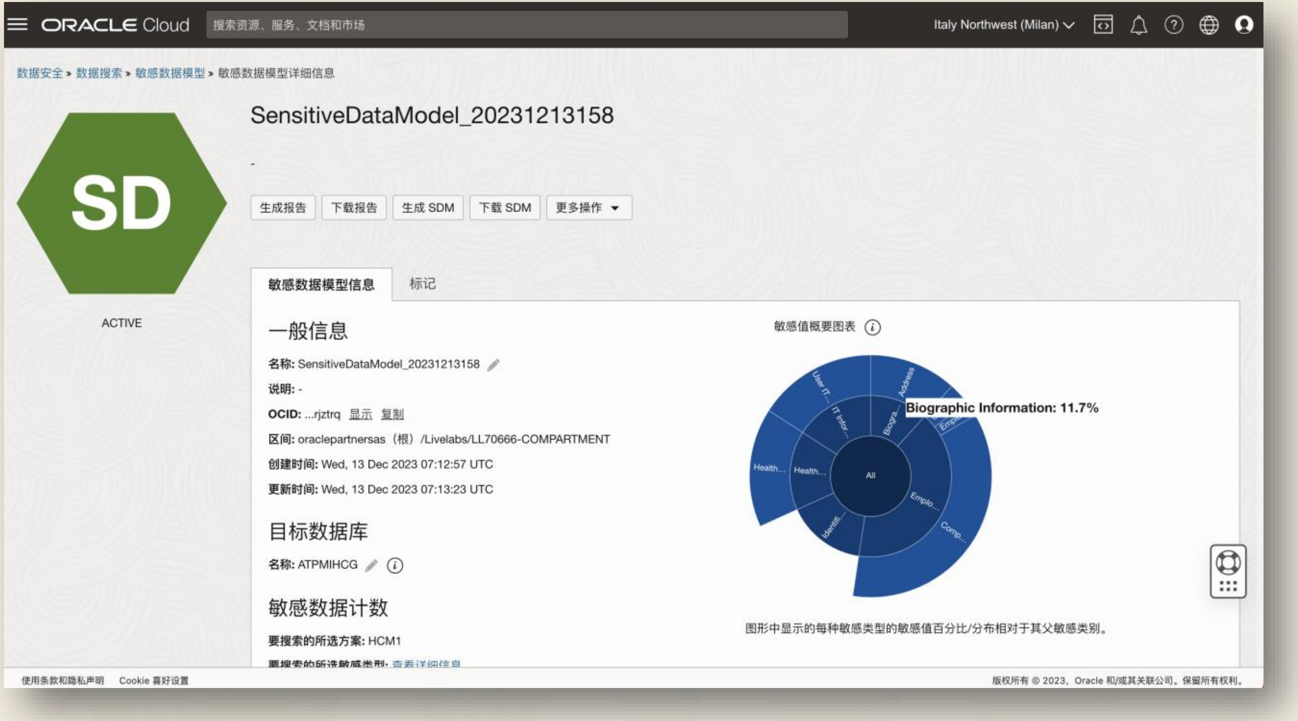
选择搜索选项

☑ 收集、显示和存储样本数据

请注意，选择以下选项将会延长搜索作业运行时间

□ 搜索应用程序级别（非字典）引用关系

安全中心 – 数据搜索 – 创建敏感数据模型（SDM)



数据安全 » 数据搜索 » 敏感数据模型 » 敏感数据模型详细信息

SensitiveDataModel_20231213158

-

一般信息

名称: SensitiveDataModel_20231213158

说明: -

OCID: ...rjztrq 显示 复制

区间: oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

创建时间: Wed, 13 Dec 2023 07:12:57 UTC

更新时间: Wed, 13 Dec 2023 07:13:23 UTC

目标数据库

名称: ATPMIHCG

敏感数据计数

要搜索的所选方案: HCM1

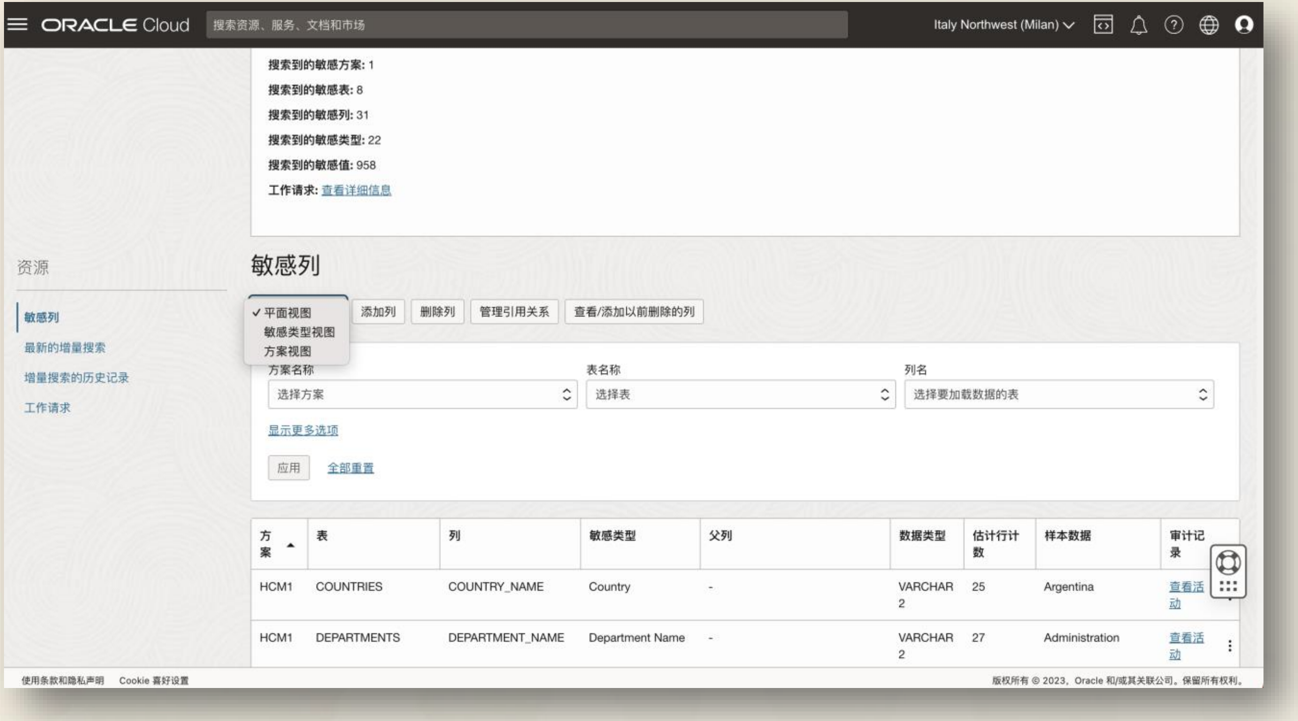
要搜索的所选敏感类型: 查看详细信息

图形中显示的每种敏感类型的敏感值百分比/分布相对于其父敏感类别。

使用条款和隐私声明　Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 数据搜索 – 报告



搜索到的敏感方案: 1

搜索到的敏感表: 8

搜索到的敏感列: 31

搜索到的敏感类型: 22

搜索到的敏感值: 958

工作请求: 查看详细信息

敏感列

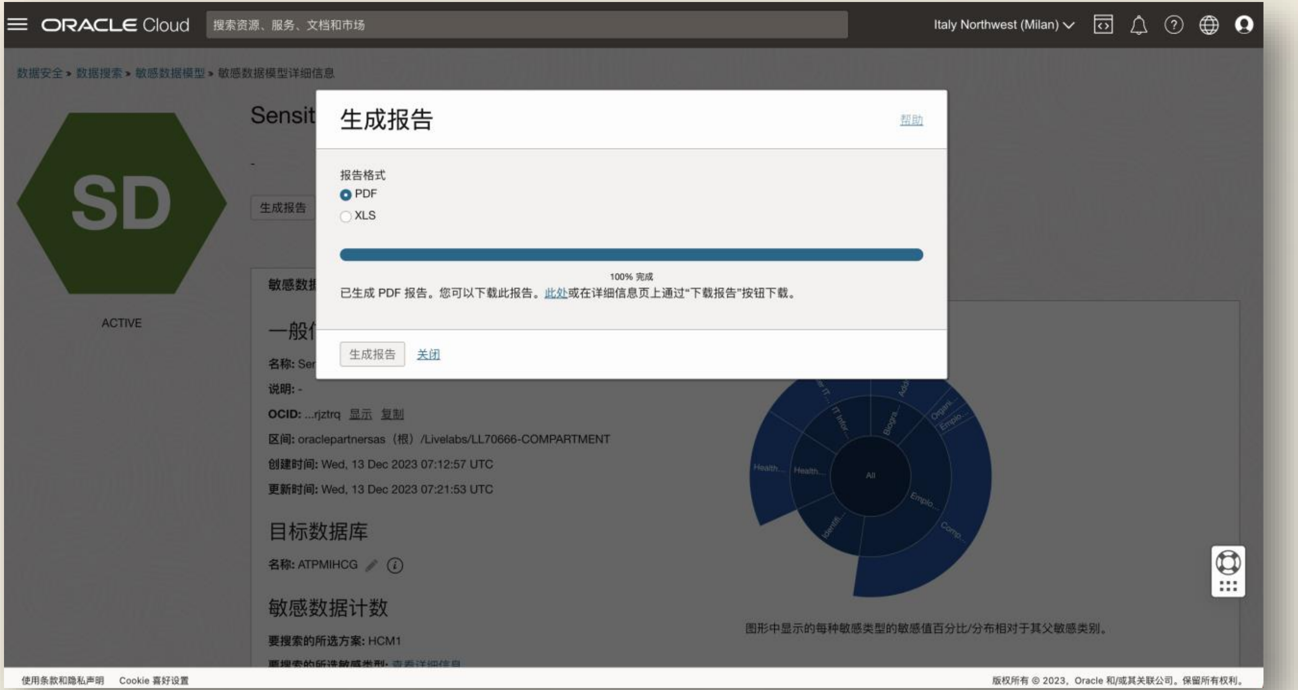
方案名称: 选择方案

表名称: 选择表

列名: 选择要加载数据的表

方案	表	列	敏感类型	父列	数据类型	估计行计数	样本数据	审计记录
HCM1	COUNTRIES	COUNTRY_NAME	Country	-	VARCHAR2	25	Argentina	查看活动
HCM1	DEPARTMENTS	DEPARTMENT_NAME	Department Name	-	VARCHAR2	27	Administration	查看活动

安全中心 – 数据搜索 – 报告



数据安全 » 数据搜索 » 敏感数据模型 » 敏感数据模型详细信息

生成报告

报告格式

● PDF

○ XLS

100% 完成

已生成 PDF 报告。您可以下载此报告。此处或在详细信息页上通过“下载报告”按钮下载。

名称: Ser

说明: -

OCID: ...rjztrq 显示 复制

区间: oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

创建时间: Wed, 13 Dec 2023 07:12:57 UTC

更新时间: Wed, 13 Dec 2023 07:21:53 UTC

目标数据库

名称: ATPMIHCG

敏感数据计数

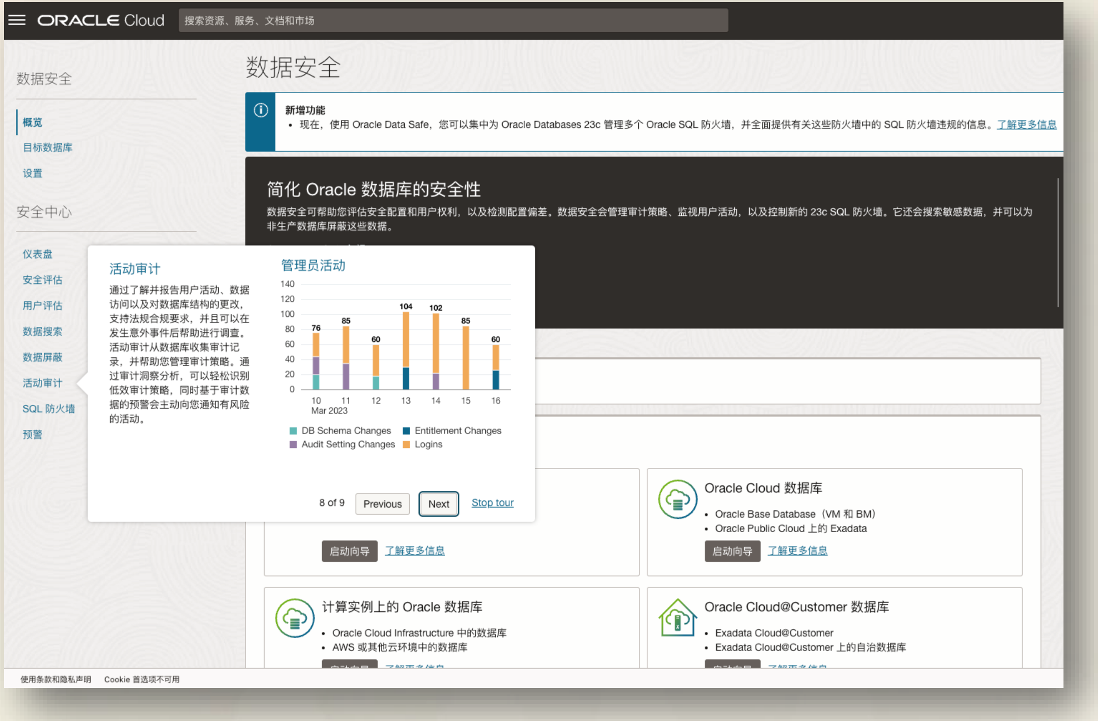
要搜索的所选方案: HCM1

要搜索的所选敏感类别: 查看详细信息

图形中显示的每种敏感类型的敏感值百分比/分布相对于其父敏感类别。

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 活动审计



数据安全

新增功能

- 现在，使用 Oracle Data Safe，您可以集中为 Oracle Databases 23c 管理多个 Oracle SQL 防火墙，并全面提供有关这些防火墙中的 SQL 防火墙违规的信息。了解更多信息

简化 Oracle 数据库的安全性

数据安全可帮助您评估安全配置和用户权利，以及检测配置偏差。数据安全会管理审计策略、监视用户活动，以及控制新的 23c SQL 防火墙。它还会搜索敏感数据，并可以为非生产数据库屏蔽这些数据。

活动审计

通过了解并报告用户活动、数据访问以及对数据库结构的更改，支持法规合规要求，并且可以在发生意外事件后帮助进行调查。活动审计从数据库收集审计记录，并帮助您管理审计策略。通过审计洞察分析，可以轻松识别低效审计策略，同时基于审计数据的预警会主动向您通知有风险的活动。

管理员活动

Oracle Cloud 数据库

- Oracle Base Database（VM 和 BM）
- Oracle Public Cloud 上的 Exadata

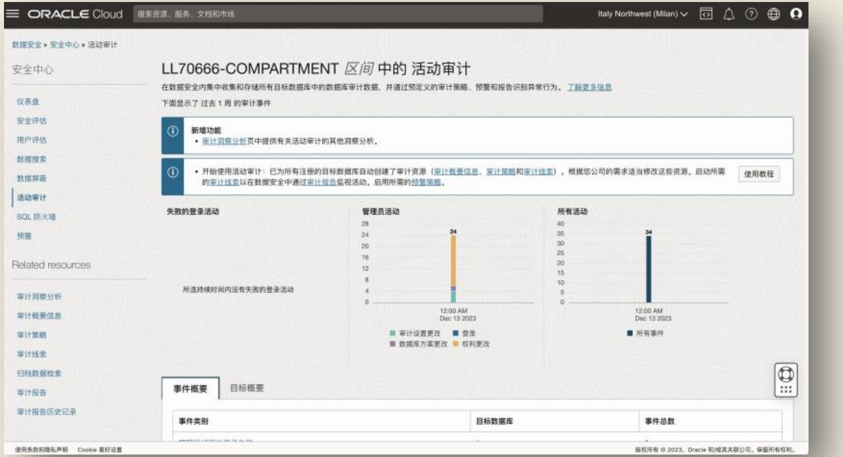
计算实例上的 Oracle 数据库

- Oracle Cloud Infrastructure 中的数据库
- AWS 或其他云环境中的数据库

Oracle Cloud@Customer 数据库

- Exadata Cloud@Customer
- Exadata Cloud@Customer 上的自治数据库

安全中心 – 活动审计



LL70666-COMPARTMENT *区间* 中的 活动审计

在数据安全内集中收集和存储所有目标数据库中的数据库审计数据，并通过预定义的审计策略、预警和报告识别异常行为。 了解更多信息

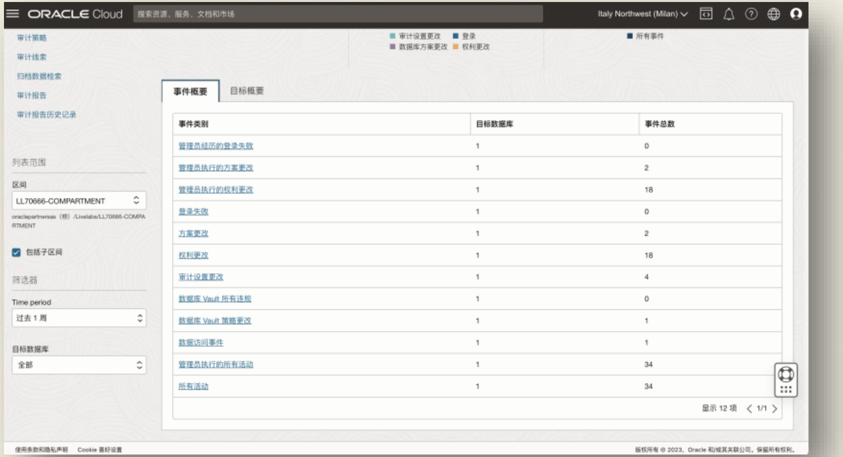
下面显示了 过去 1 周 的审计事件

新增功能
- 审计洞察分析页中提供有关活动审计的其他洞察分析。

- 开始使用活动审计：已为所有注册的目标数据库自动创建了审计资源（审计概要信息、审计策略和审计线索）。根据您公司的需求适当修改这些资源。启动所需的审计线索以在数据安全中通过审计报告监视活动。启用所需的预警策略。

所选持续时间内没有失败的登录活动

事件类别	目标数据库	事件总数



区间: LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

☑ 包括子区间

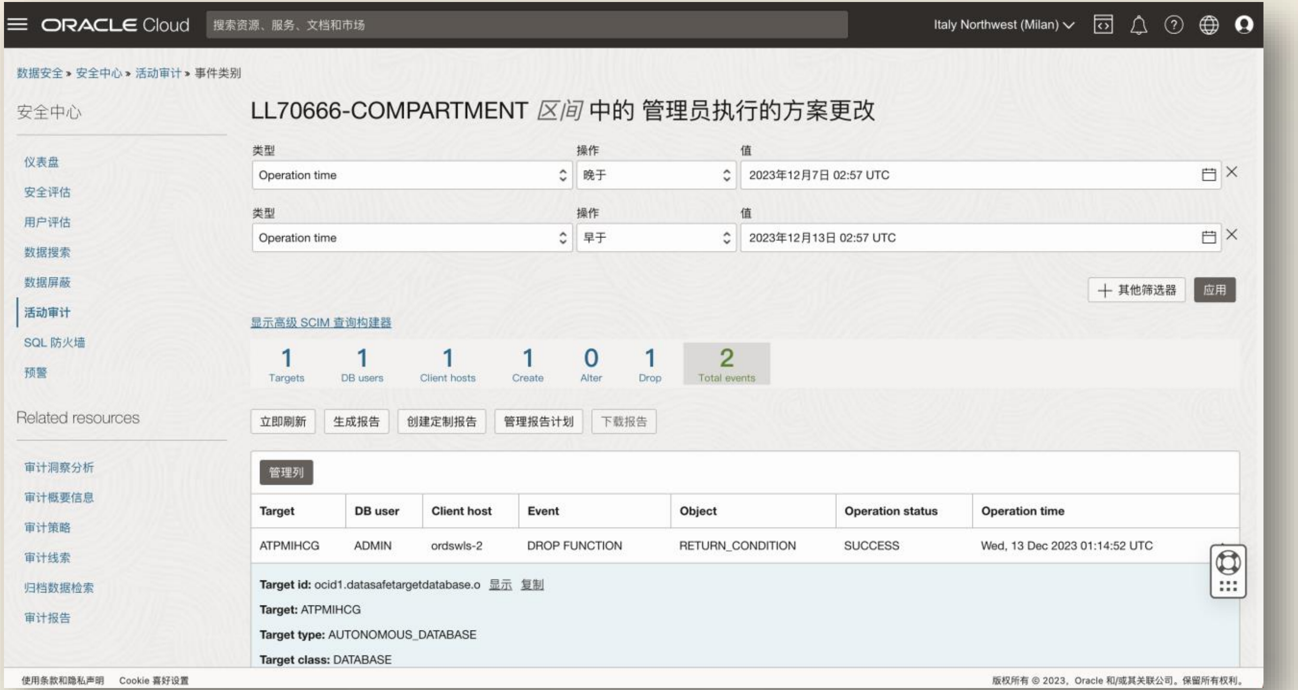
Time period: 过去 1 周

目标数据库: 全部

事件类别	目标数据库	事件总数
管理员经历的登录失败	1	0
管理员执行的方案更改	1	2
管理员执行的权利更改	1	18
登录失败	1	0
方案更改	1	2
权利更改	1	18
审计设置更改	1	4
数据库 Vault 所有违规	1	0
数据库 Vault 策略更改	1	1
数据访问事件	1	1
管理员执行的所有活动	1	34
所有活动	1	34

显示 12 项 ‹ 1/1 ›

安全中心 – 活动审计



数据安全 » 安全中心 » 活动审计 » 事件类别

安全中心

- 仪表盘
- 安全评估
- 用户评估
- 数据搜索
- 数据屏蔽
- 活动审计
- SQL 防火墙
- 预警

Related resources

- 审计洞察分析
- 审计概要信息
- 审计策略
- 审计线索
- 归档数据检索
- 审计报告

LL70666-COMPARTMENT *区间* 中的 管理员执行的方案更改

类型	操作	值
Operation time	晚于	2023年12月7日 02:57 UTC
Operation time	早于	2023年12月13日 02:57 UTC

显示高级 SCIM 查询构建器

Targets	DB users	Client hosts	Create	Alter	Drop	Total events
1	1	1	1	0	1	2

Target	DB user	Client host	Event	Object	Operation status	Operation time
ATPMIHCG	ADMIN	ordswls-2	DROP FUNCTION	RETURN_CONDITION	SUCCESS	Wed, 13 Dec 2023 01:14:52 UTC

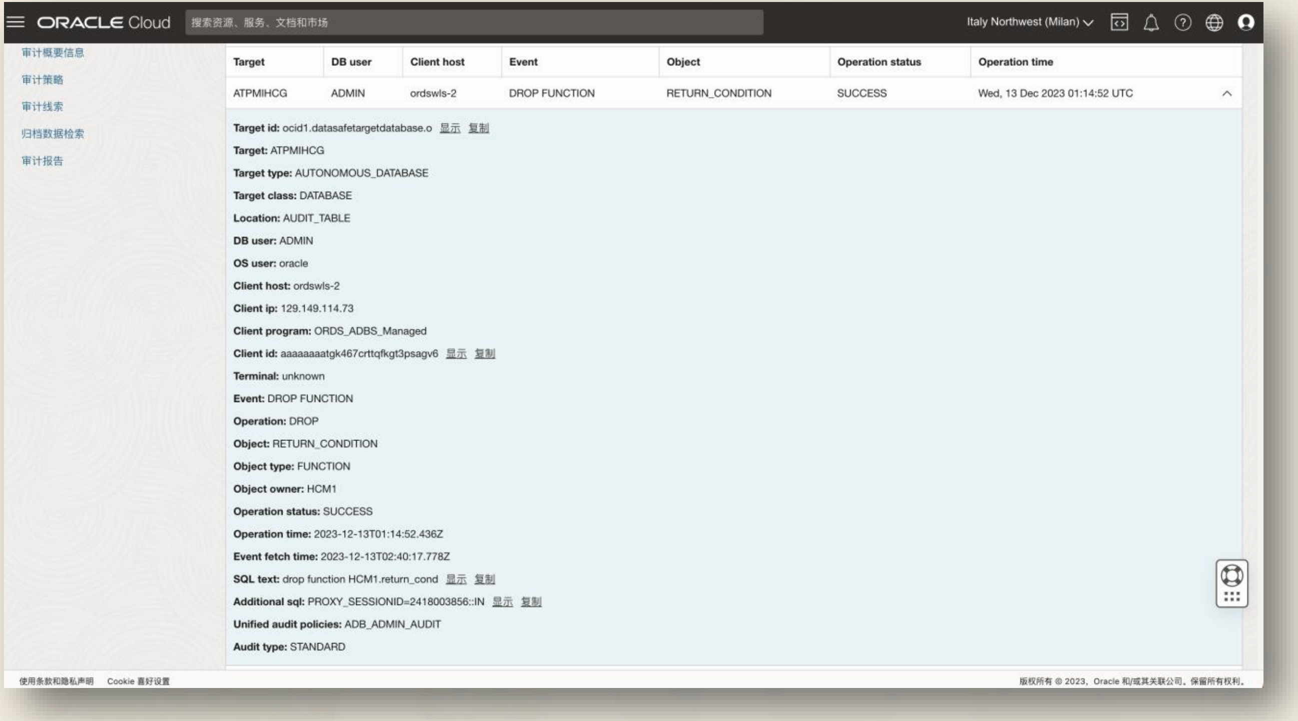
Target id: ocid1.datasafetargetdatabase.o 显示 复制

Target: ATPMIHCG

Target type: AUTONOMOUS_DATABASE

Target class: DATABASE

安全中心 – 活动审计



Target	DB user	Client host	Event	Object	Operation status	Operation time
ATPMIHCG	ADMIN	ordswls-2	DROP FUNCTION	RETURN_CONDITION	SUCCESS	Wed, 13 Dec 2023 01:14:52 UTC

Target id: ocid1.datasafetargetdatabase.o 显示 复制

Target: ATPMIHCG

Target type: AUTONOMOUS_DATABASE

Target class: DATABASE

Location: AUDIT_TABLE

DB user: ADMIN

OS user: oracle

Client host: ordswls-2

Client ip: 129.149.114.73

Client program: ORDS_ADBS_Managed

Client id: aaaaaaaatgk467crttqfkgt3psagv6 显示 复制

Terminal: unknown

Event: DROP FUNCTION

Operation: DROP

Object: RETURN_CONDITION

Object type: FUNCTION

Object owner: HCM1

Operation status: SUCCESS

Operation time: 2023-12-13T01:14:52.436Z

Event fetch time: 2023-12-13T02:40:17.778Z

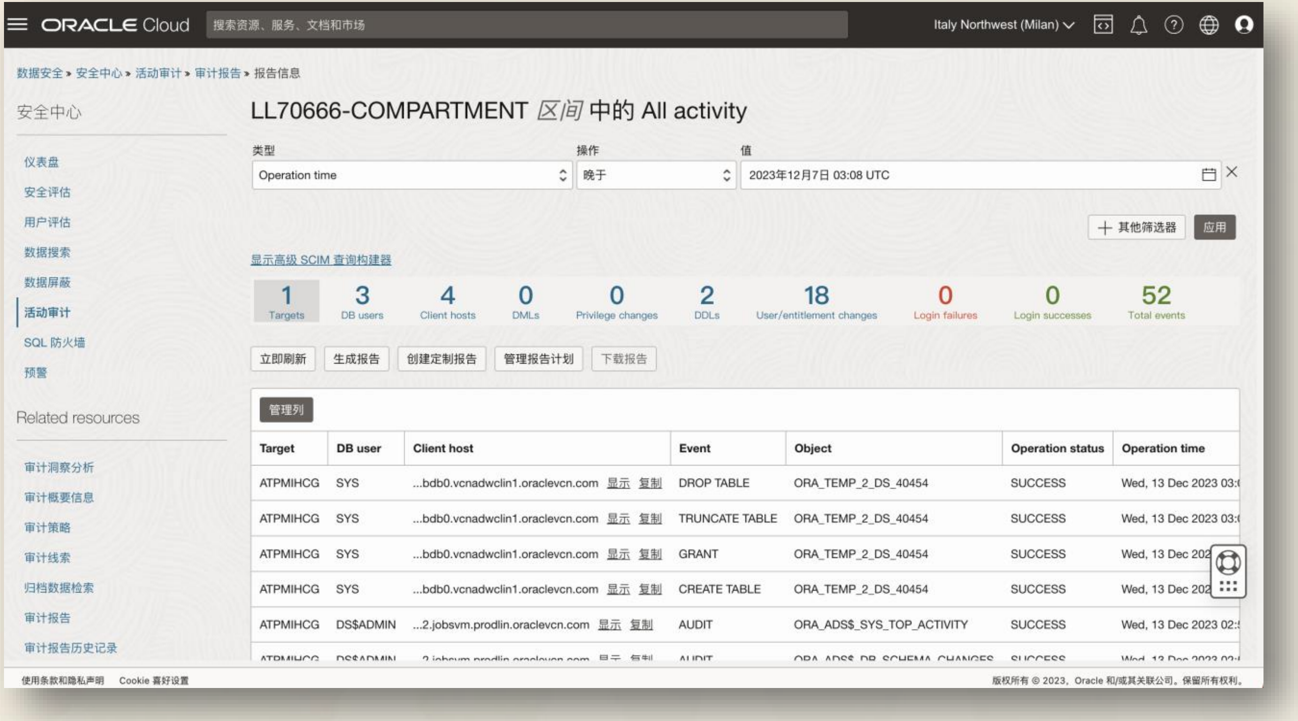
SQL text: drop function HCM1.return_cond 显示 复制

Additional sql: PROXY_SESSIONID=2418003856::IN 显示 复制

Unified audit policies: ADB_ADMIN_AUDIT

Audit type: STANDARD

安全中心 – 活动审计 – 审计报告



数据安全 » 安全中心 » 活动审计 » 审计报告 » 报告信息

LL70666-COMPARTMENT *区间* 中的 All activity

类型: Operation time

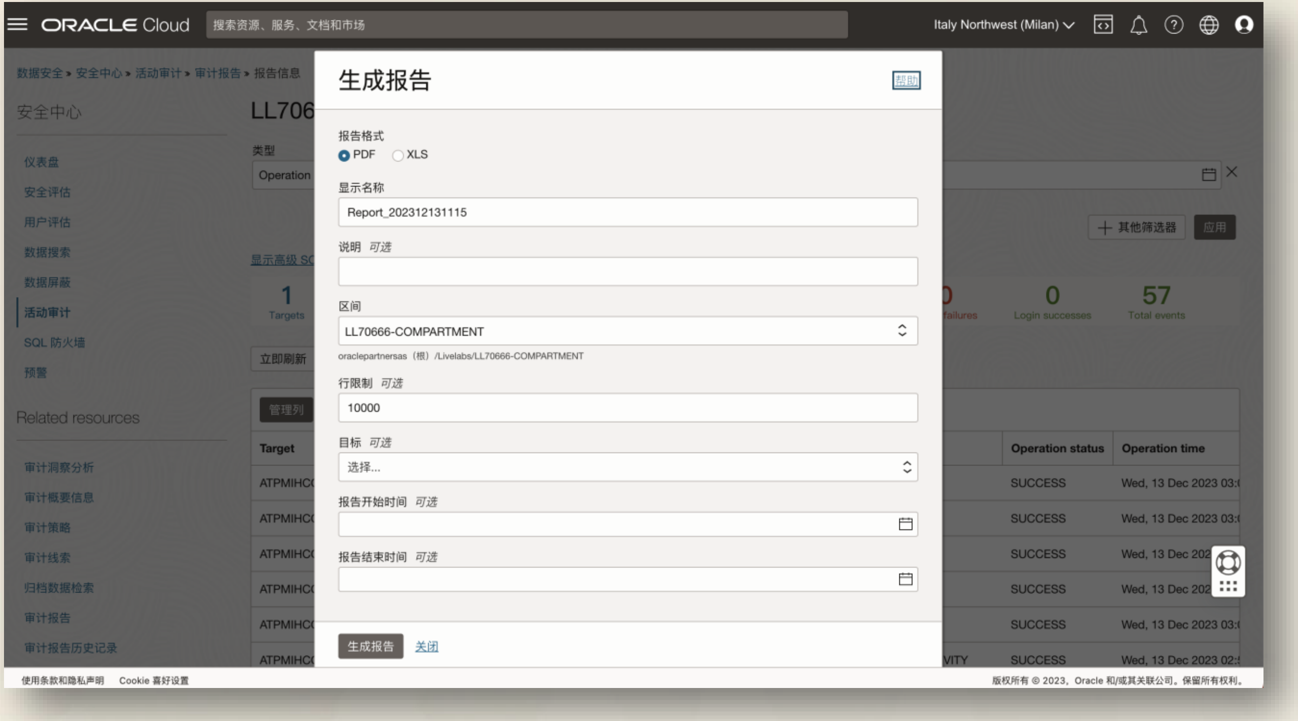
操作: 晚于

值: 2023年12月7日 03:08 UTC

1	3	4	0	0	2	18	0	0	52
Targets	DB users	Client hosts	DMLs	Privilege changes	DDLs	User/entitlement changes	Login failures	Login successes	Total events

Target	DB user	Client host	Event	Object	Operation status	Operation time
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	DROP TABLE	ORA_TEMP_2_DS_40454	SUCCESS	Wed, 13 Dec 2023 03:
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	TRUNCATE TABLE	ORA_TEMP_2_DS_40454	SUCCESS	Wed, 13 Dec 2023 03:
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	GRANT	ORA_TEMP_2_DS_40454	SUCCESS	Wed, 13 Dec 202
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	CREATE TABLE	ORA_TEMP_2_DS_40454	SUCCESS	Wed, 13 Dec 202
ATPMIHCG	DS$ADMIN	...2.jobsvm.prodlin.oraclevcn.com 显示 复制	AUDIT	ORA_ADS$_SYS_TOP_ACTIVITY	SUCCESS	Wed, 13 Dec 2023 02:
ATPMIHCG	DS$ADMIN	...2.jobsvm.prodlin.oraclevcn.com 显示 复制	AUDIT	ORA_ADS$_DB_SCHEMA_CHANGES	SUCCESS	Wed, 13 Dec 2023 02:

安全中心 – 活动审计 – 审计报告 – 生成报告



Target	Operation status	Operation time
ATPMIHC	SUCCESS	Wed, 13 Dec 2023 03:
ATPMIHC	SUCCESS	Wed, 13 Dec 2023 03:
ATPMIHC	SUCCESS	Wed, 13 Dec 202
ATPMIHC	SUCCESS	Wed, 13 Dec 202
ATPMIHC	SUCCESS	Wed, 13 Dec 2023 03:
ATPMIHC	SUCCESS	Wed, 13 Dec 2023 02:

生成报告

帮助

报告格式

● PDF ○ XLS

显示名称

Report_202312131115

说明 *可选*

区间

LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

行限制 *可选*

10000

目标 *可选*

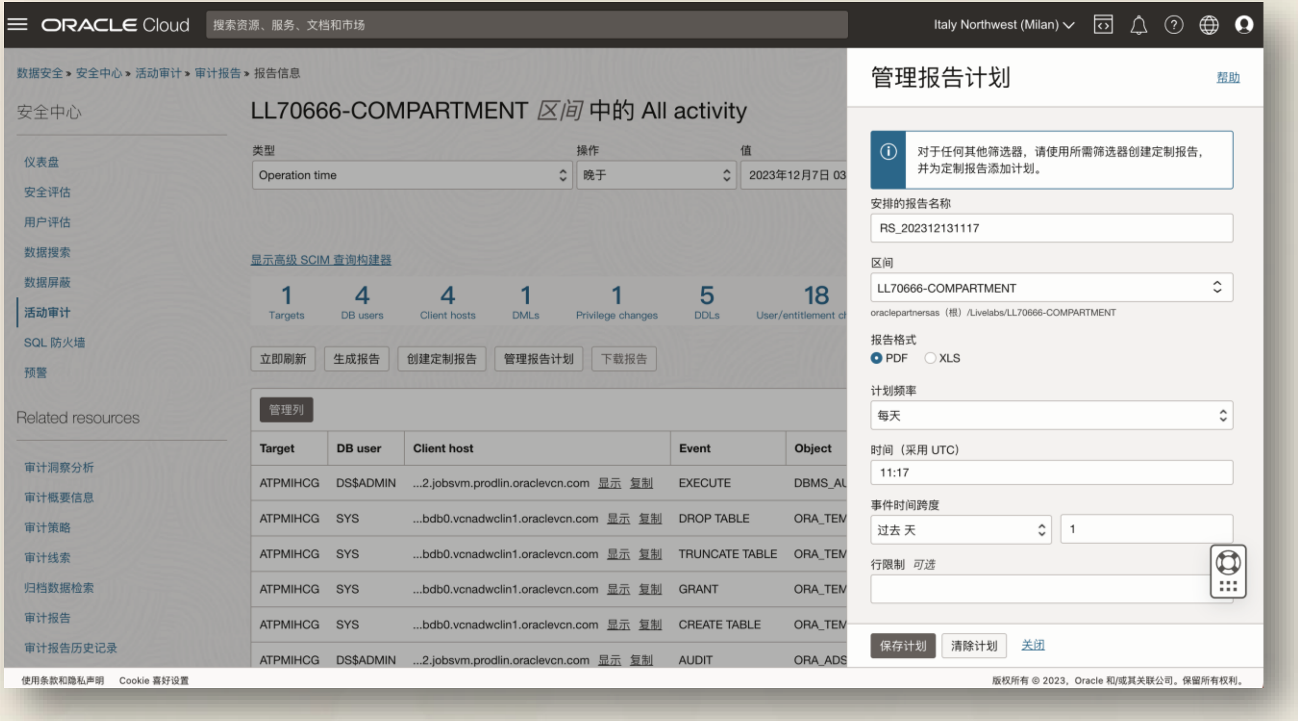
选择...

报告开始时间 *可选*

报告结束时间 *可选*

生成报告 关闭

安全中心 – 活动审计 – 审计报告 – 管理报告计划



数据安全 » 安全中心 » 活动审计 » 审计报告 » 报告信息

安全中心

- 仪表盘
- 安全评估
- 用户评估
- 数据搜索
- 数据屏蔽
- 活动审计
- SQL 防火墙
- 预警

Related resources

- 审计洞察分析
- 审计概要信息
- 审计策略
- 审计线索
- 归档数据检索
- 审计报告
- 审计报告历史记录

LL70666-COMPARTMENT *区间* 中的 All activity

类型	操作	值
Operation time	晚于	2023年12月7日 03

显示高级 SCIM 查询构建器

1	4	4	1	1	5	18
Targets	DB users	Client hosts	DMLs	Privilege changes	DDLs	User/entitlement ch

立即刷新 | 生成报告 | 创建定制报告 | 管理报告计划 | 下载报告

管理列

Target	DB user	Client host	Event	Object
ATPMIHCG	DS$ADMIN	...2.jobsvm.prodlin.oraclevcn.com 显示 复制	EXECUTE	DBMS_AU
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	DROP TABLE	ORA_TEM
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	TRUNCATE TABLE	ORA_TEM
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	GRANT	ORA_TEM
ATPMIHCG	SYS	...bdb0.vcnadwclin1.oraclevcn.com 显示 复制	CREATE TABLE	ORA_TEM
ATPMIHCG	DS$ADMIN	...2.jobsvm.prodlin.oraclevcn.com 显示 复制	AUDIT	ORA_ADS

管理报告计划

帮助

ⓘ 对于任何其他筛选器，请使用所需筛选器创建定制报告，并为定制报告添加计划。

安排的报告名称: RS_202312131117

区间: LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

报告格式: ● PDF ○ XLS

计划频率: 每天

时间（采用 UTC）: 11:17

事件时间跨度: 过去 天 1

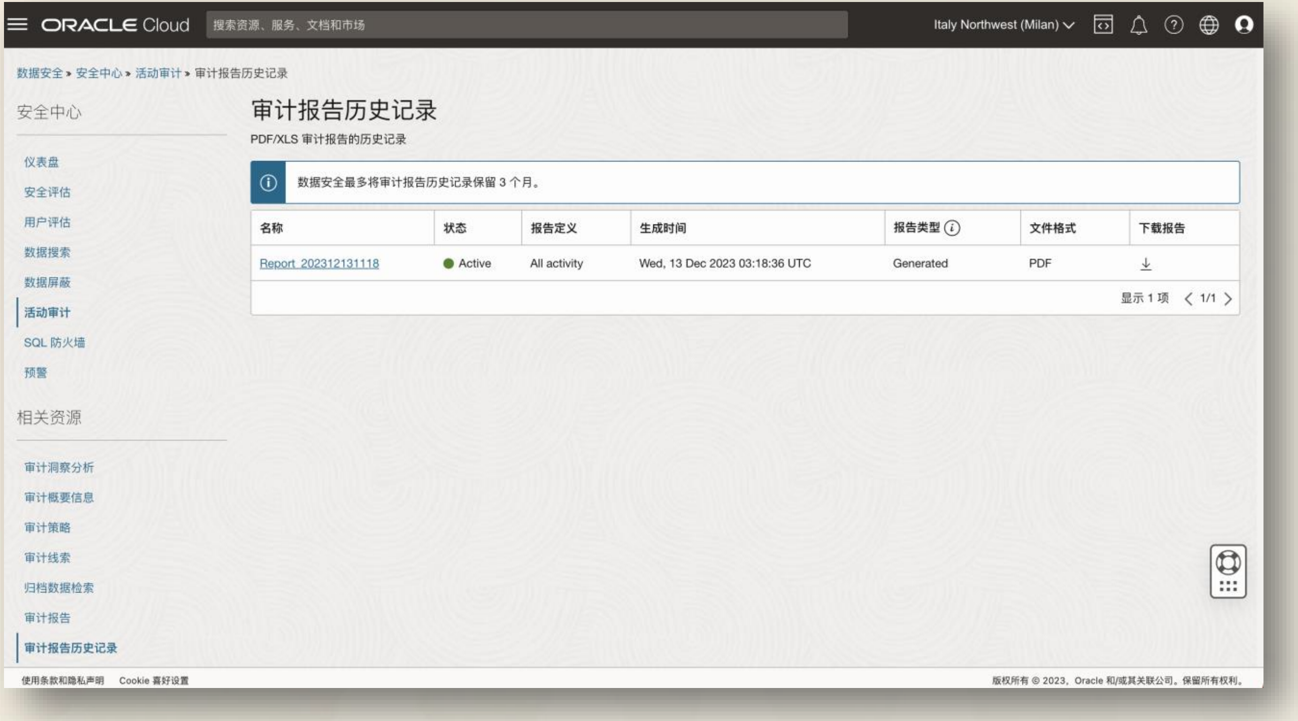
行限制 *可选*

保存计划 | 清除计划 | 关闭

使用条款和隐私声明　Cookie 喜好设置

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 活动审计 – 审计报告历史记录



审计报告历史记录

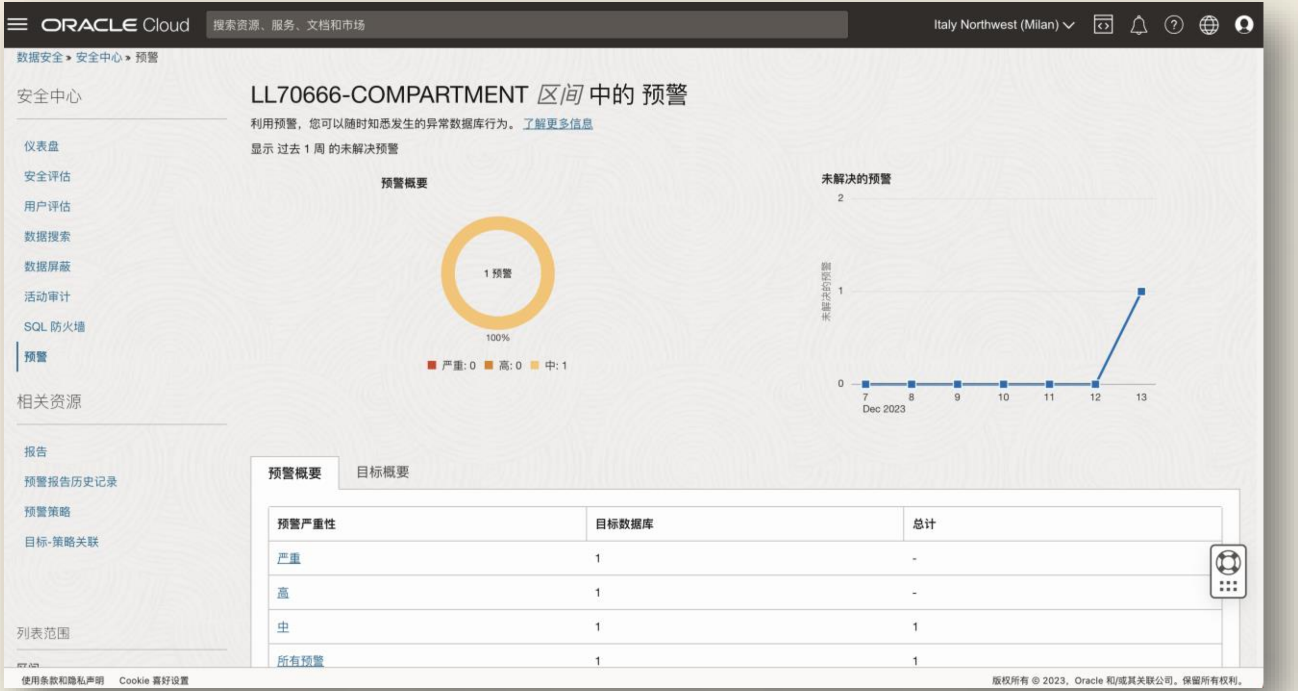
PDF/XLS 审计报告的历史记录

ⓘ 数据安全最多将审计报告历史记录保留 3 个月。

名称	状态	报告定义	生成时间	报告类型 ⓘ	文件格式	下载报告
Report_202312131118	● Active	All activity	Wed, 13 Dec 2023 03:18:36 UTC	Generated	PDF	⤓

显示 1 项 ‹ 1/1 ›

安全中心 – 预警



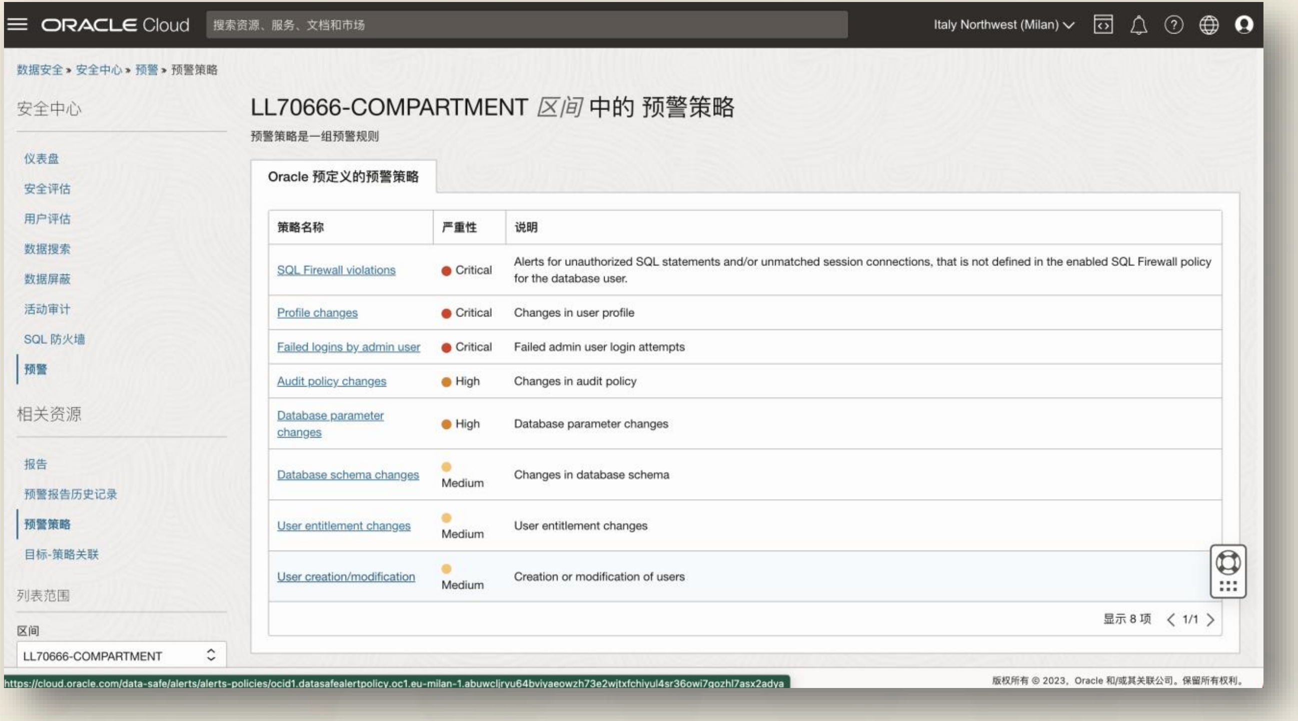
LL70666-COMPARTMENT *区间* 中的 预警

利用预警，您可以随时知悉发生的异常数据库行为。了解更多信息

显示 过去 1 周 的未解决预警

预警严重性	目标数据库	总计
严重	1	-
高	1	-
中	1	1
所有预警	1	1

安全中心 – 预警 – 预警策略



数据安全 » 安全中心 » 预警 » 预警策略

区间: LL70666-COMPARTMENT

LL70666-COMPARTMENT *区间* 中的 预警策略

预警策略是一组预警规则

Oracle 预定义的预警策略

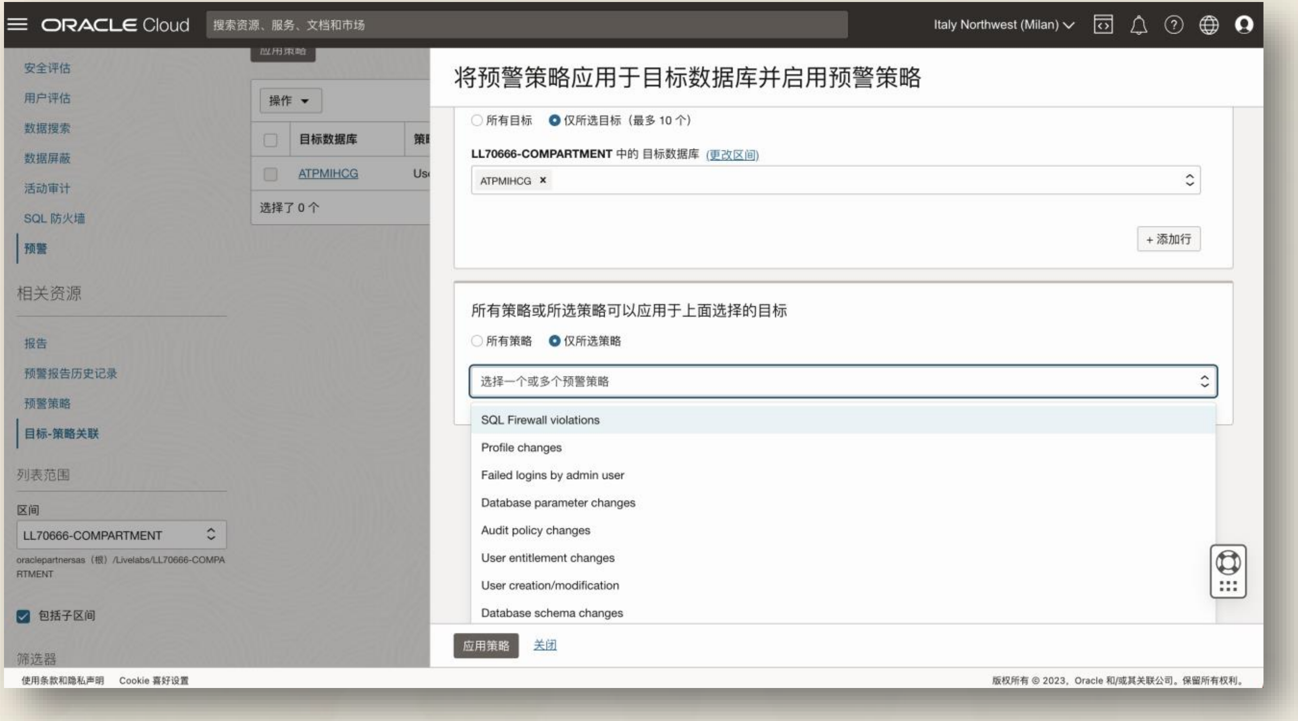
策略名称	严重性	说明
SQL Firewall violations	● Critical	Alerts for unauthorized SQL statements and/or unmatched session connections, that is not defined in the enabled SQL Firewall policy for the database user.
Profile changes	● Critical	Changes in user profile
Failed logins by admin user	● Critical	Failed admin user login attempts
Audit policy changes	● High	Changes in audit policy
Database parameter changes	● High	Database parameter changes
Database schema changes	● Medium	Changes in database schema
User entitlement changes	● Medium	User entitlement changes
User creation/modification	● Medium	Creation or modification of users

显示 8 项 < 1/1 >

https://cloud.oracle.com/data-safe/alerts/alerts-policies/ocid1.datasafealertpolicy.oc1.eu-milan-1.abuwcljryu64bviyaeowzh73e2wjtxfchiyul4sr36owi7gozhl7asx2adya

版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 预警 – 目标-策略关联



□	目标数据库	策
□	ATPMIHCG	Us

选择了 0 个

区间: LL70666-COMPARTMENT

oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

☑ 包括子区间

筛选器

将预警策略应用于目标数据库并启用预警策略

○ 所有目标 ● 仅所选目标（最多 10 个）

LL70666-COMPARTMENT 中的 目标数据库 (更改区间)

ATPMIHCG ×

+ 添加行

所有策略或所选策略可以应用于上面选择的目标

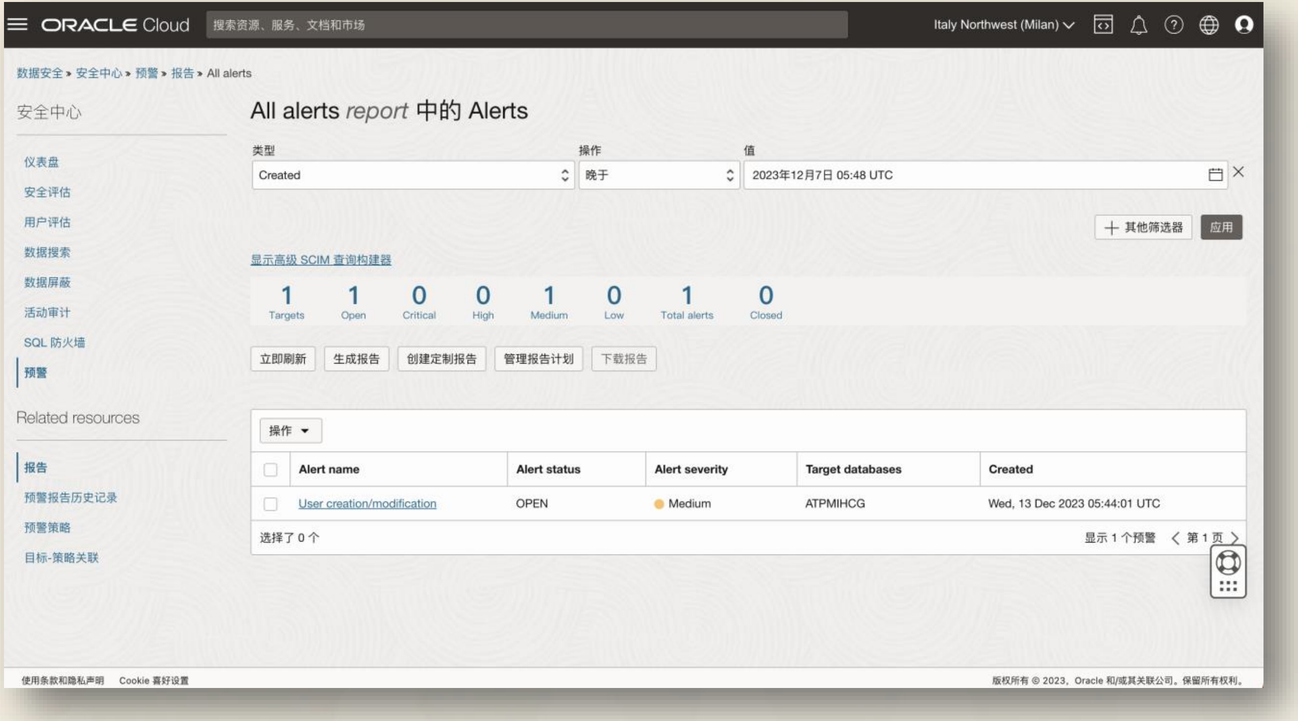
○ 所有策略 ● 仅所选策略

选择一个或多个预警策略

- SQL Firewall violations
- Profile changes
- Failed logins by admin user
- Database parameter changes
- Audit policy changes
- User entitlement changes
- User creation/modification
- Database schema changes

应用策略 关闭

安全中心 – 预警 – 报告



数据安全 » 安全中心 » 预警 » 报告 » All alerts

All alerts *report* 中的 Alerts

类型	操作	值
Created	晚于	2023年12月7日 05:48 UTC

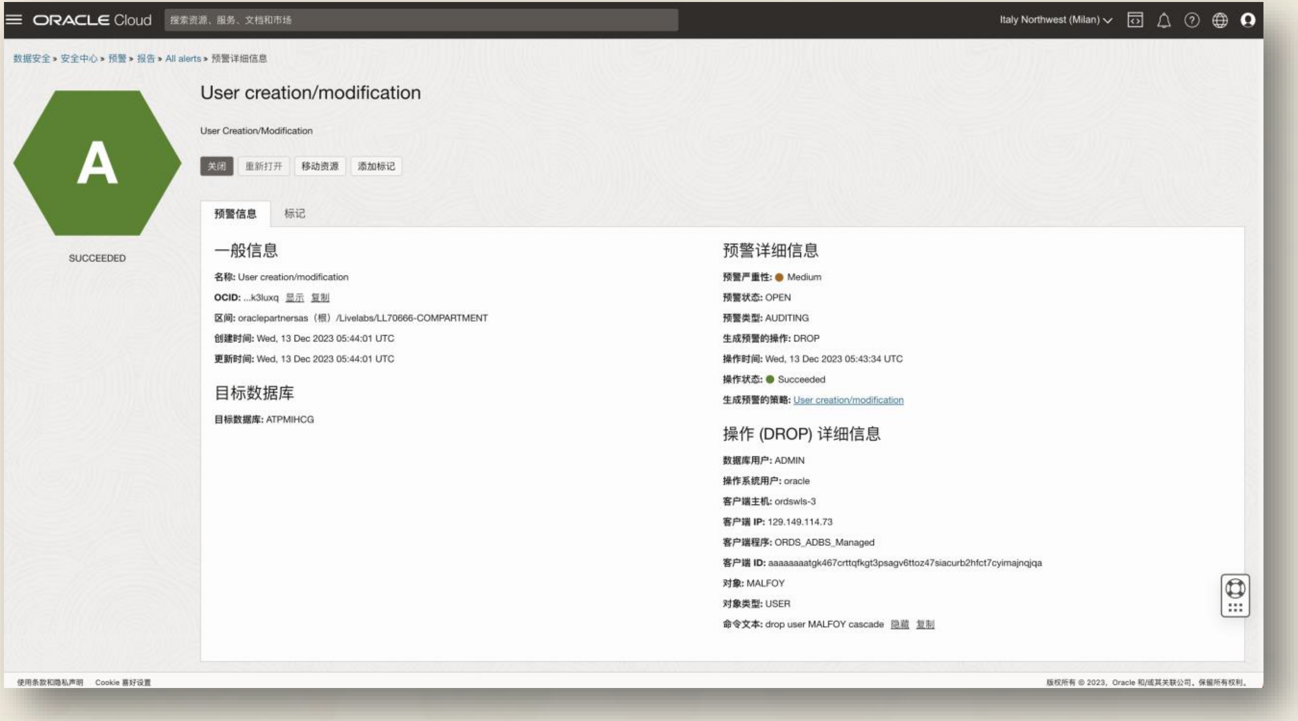
1	1	0	0	1	0	1	0
Targets	Open	Critical	High	Medium	Low	Total alerts	Closed

□	Alert name	Alert status	Alert severity	Target databases	Created
□	User creation/modification	OPEN	● Medium	ATPMIHCG	Wed, 13 Dec 2023 05:44:01 UTC

选择了 0 个　　显示 1 个预警　< 第 1 页 >

使用条款和隐私声明　Cookie 喜好设置　　版权所有 © 2023，Oracle 和/或其关联公司。保留所有权利。

安全中心 – 预警 – 报告 – 预警详细信息



User creation/modification

User Creation/Modification

一般信息

名称: User creation/modification

OCID: ...k3luxq 显示 复制

区间: oraclepartnersas（根）/Livelabs/LL70666-COMPARTMENT

创建时间: Wed, 13 Dec 2023 05:44:01 UTC

更新时间: Wed, 13 Dec 2023 05:44:01 UTC

目标数据库

目标数据库: ATPMIHCG

预警详细信息

预警严重性: ● Medium

预警状态: OPEN

预警类型: AUDITING

生成预警的操作: DROP

操作时间: Wed, 13 Dec 2023 05:43:34 UTC

操作状态: ● Succeeded

生成预警的策略: User creation/modification

操作 (DROP) 详细信息

数据库用户: ADMIN

操作系统用户: oracle

客户端主机: ordswls-3

客户端 IP: 129.149.114.73

客户端程序: ORDS_ADBS_Managed

客户端 ID: aaaaaaaatgk467crttqfkgt3psagv6ttoz47siacurb2hfct7cyimajnqjqa

对象: MALFOY

对象类型: USER

命令文本: drop user MALFOY cascade 隐藏 复制

为什么以及何时考虑Data Safe?Why and when to consider Data Safe?

- 不仅需评估，获得“快速上市”和功能即服务Go beyond assessment, get “quick time to market”, and functionality as-a-service
- 获取基线、漂移报告、APIs、事件和通知等Get baselining, drift reports, APIs, events and notifications and more
- 为所有Oracle数据库获得一个广泛的简化和集中的安全配置，加上用户评估、数据发现、数据屏蔽和活动审计Get a fleet-wide simplified and centralized security configuration for all Oracle Databases, plus User Assessment, Data Discovery, Data Masking and Activity Auditing
- 您的Oracle数据库运行在多云、混合部署模型或完全本地部署中Your Oracle databases run in a multi-cloud, hybrid deployment model, or fully on-premises

如果您希望大规模运行评估，并从作为云服务（主要是SaaS）提供的统一控制台中获益，而不需要安装或维护基础设施，那么Data Safe就是您的理想选择。 If you want to run assessments at scale and benefit from a unified console provided as a cloud service (mainly as a SaaS) where you do not need to install nor maintain infrastructure, Data Safe is the tool for you.

能力对比

能力	Data Safe	AVDF	DBSAT
整体安全配置状态	✓	✓	✓
配置漂移检测和报告	✓	✓	-
用户风险评估/用户权限报告	✓	✓ +	-
敏感数据发现	✓	✓ *	✓ *
多目标评估集中管理	✓	✓	-
历史报告和管理	✓	✓	-
支持云、本地和Cloud@Customer目标	✓	✓	✓
使用方式	OCI 云服务	OCI 市场映像或本地安装	命令行

+ 无风险评分；AVDF授权报告包括用户角色和权限授予、系统权限授予、对象权限授予——带有漂移。
** 只检查列名和注释，不检查数据*

更多信息……

数据库安全主页

https://www.oracle.com/cn/security/database-security/

DBSAT 下载

https://www.oracle.com/security/database-security/assessment-tool/

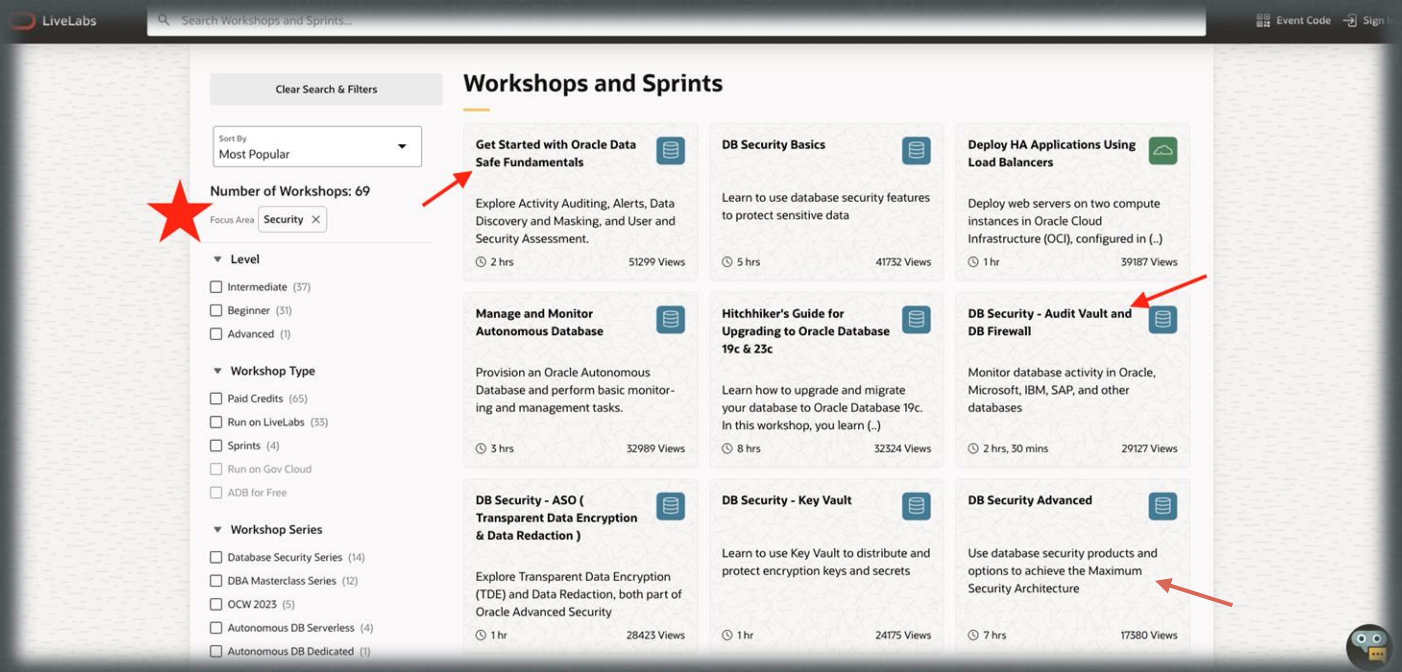
数据库安全Blog

https://blogs.oracle.com/cloudsecurity/category/ocs-database-security

电子书：Oracle Database 安全保护，第五版

https://download.oracle.com/database/oracle-database-security-primer.pdf

LiveLabs https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/home – 安全



LiveLabs
Search Workshops and Sprints...
Event Code
Sign In

Clear Search & Filters

Sort By
Most Popular

Number of Workshops: 69

Focus Area: Security ✕

Level

- ☐ Intermediate (37)
- ☐ Beginner (31)
- ☐ Advanced (1)

Workshop Type

- ☐ Paid Credits (65)
- ☐ Run on LiveLabs (33)
- ☐ Sprints (4)
- ☐ Run on Gov Cloud
- ☐ ADB for Free

Workshop Series

- ☐ Database Security Series (14)
- ☐ DBA Masterclass Series (12)
- ☐ OCW 2023 (5)
- ☐ Autonomous DB Serverless (4)
- ☐ Autonomous DB Dedicated (1)

Workshops and Sprints

Get Started with Oracle Data Safe Fundamentals
Explore Activity Auditing, Alerts, Data Discovery and Masking, and User and Security Assessment.
2 hrs 51299 Views

DB Security Basics
Learn to use database security features to protect sensitive data
5 hrs 41732 Views

Deploy HA Applications Using Load Balancers
Deploy web servers on two compute instances in Oracle Cloud Infrastructure (OCI), configured in (..)
1 hr 39187 Views

Manage and Monitor Autonomous Database
Provision an Oracle Autonomous Database and perform basic monitoring and management tasks.
3 hrs 32989 Views

Hitchhiker's Guide for Upgrading to Oracle Database 19c & 23c
Learn how to upgrade and migrate your database to Oracle Database 19c. In this workshop, you learn (..)
8 hrs 32324 Views

DB Security - Audit Vault and DB Firewall
Monitor database activity in Oracle, Microsoft, IBM, SAP, and other databases
2 hrs, 30 mins 29127 Views

DB Security - ASO (Transparent Data Encryption & Data Redaction)
Explore Transparent Data Encryption (TDE) and Data Redaction, both part of Oracle Advanced Security
1 hr 28423 Views

DB Security - Key Vault
Learn to use Key Vault to distribute and protect encryption keys and secrets
1 hr 24175 Views

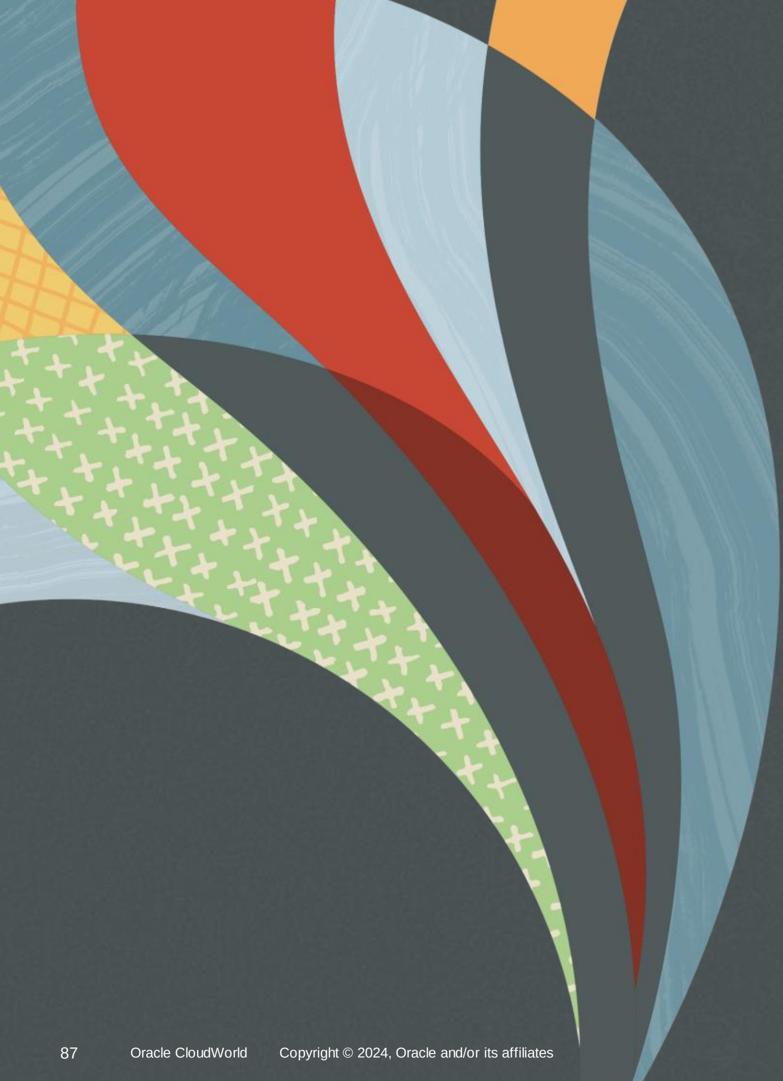
DB Security Advanced
Use database security products and options to achieve the Maximum Security Architecture
7 hrs 17380 Views

https://bit.ly/golivelabsdbsec

Oracle专家课程系列 – 数据安全实战演练系列

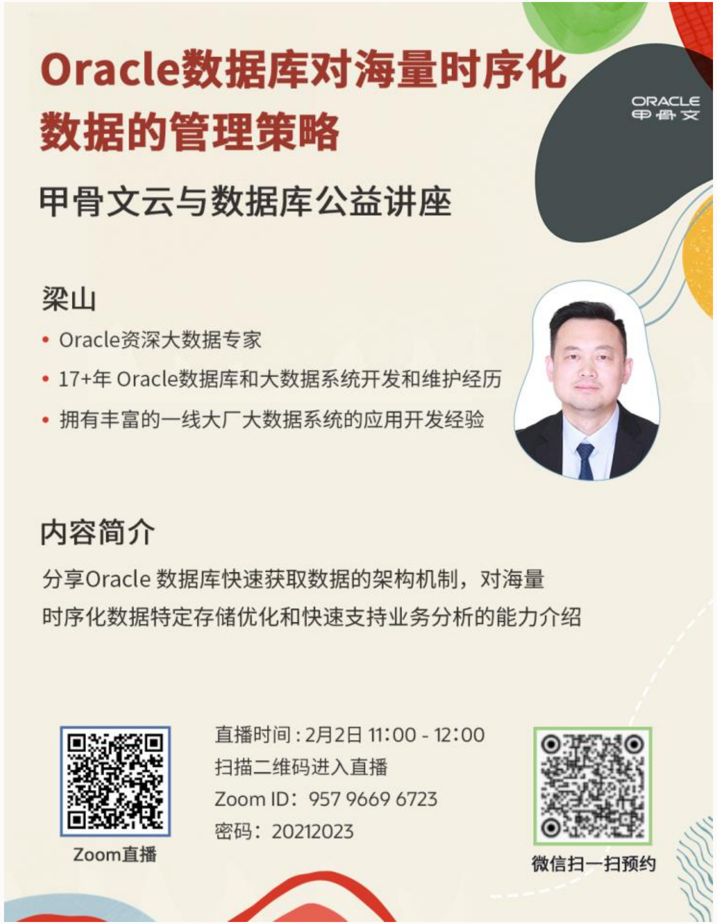
- Oracle透明数据加密（TDE）
- 深入了解Oracle审计仓库和数据库防火墙（AVDF）
- 深入了解Oracle动态数据脱敏
- 深入了解Oracle Key Vault (OKV)
- 深入了解Oracle Database Vault(DV)
- Oracle数据库高级安全特性，许您一个安全未来

B站专家系列课程



Q&A

谢谢聆听Thank you



Oracle数据库对海量时序化数据的管理策略

甲骨文云与数据库公益讲座

ORACLE 甲骨文

梁山

- Oracle资深大数据专家
- 17+年 Oracle数据库和大数据系统开发和维护经历
- 拥有丰富的一线大厂大数据系统的应用开发经验

内容简介

分享Oracle 数据库快速获取数据的架构机制，对海量时序化数据特定存储优化和快速支持业务分析的能力介绍

直播时间：2月2日 11:00 - 12:00
扫描二维码进入直播
Zoom ID：957 9669 6723
密码：20212023

Zoom直播

微信扫一扫预约

数据库和云讲座群

20-23

甲骨文云技术公众号

技术专家1V1深入交流