ORACLE

Oracle审计仓库和数据库防火墙

Jim Kong
Database Security

议程

1 概览

2 AVDF20 功能简介

- 扩展的审计收集范围
- 简化的数据库防火墙
- 友好的用户界面
- 改进的企业级支持

3 总结

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

Oracle审计仓库和数据库防火墙

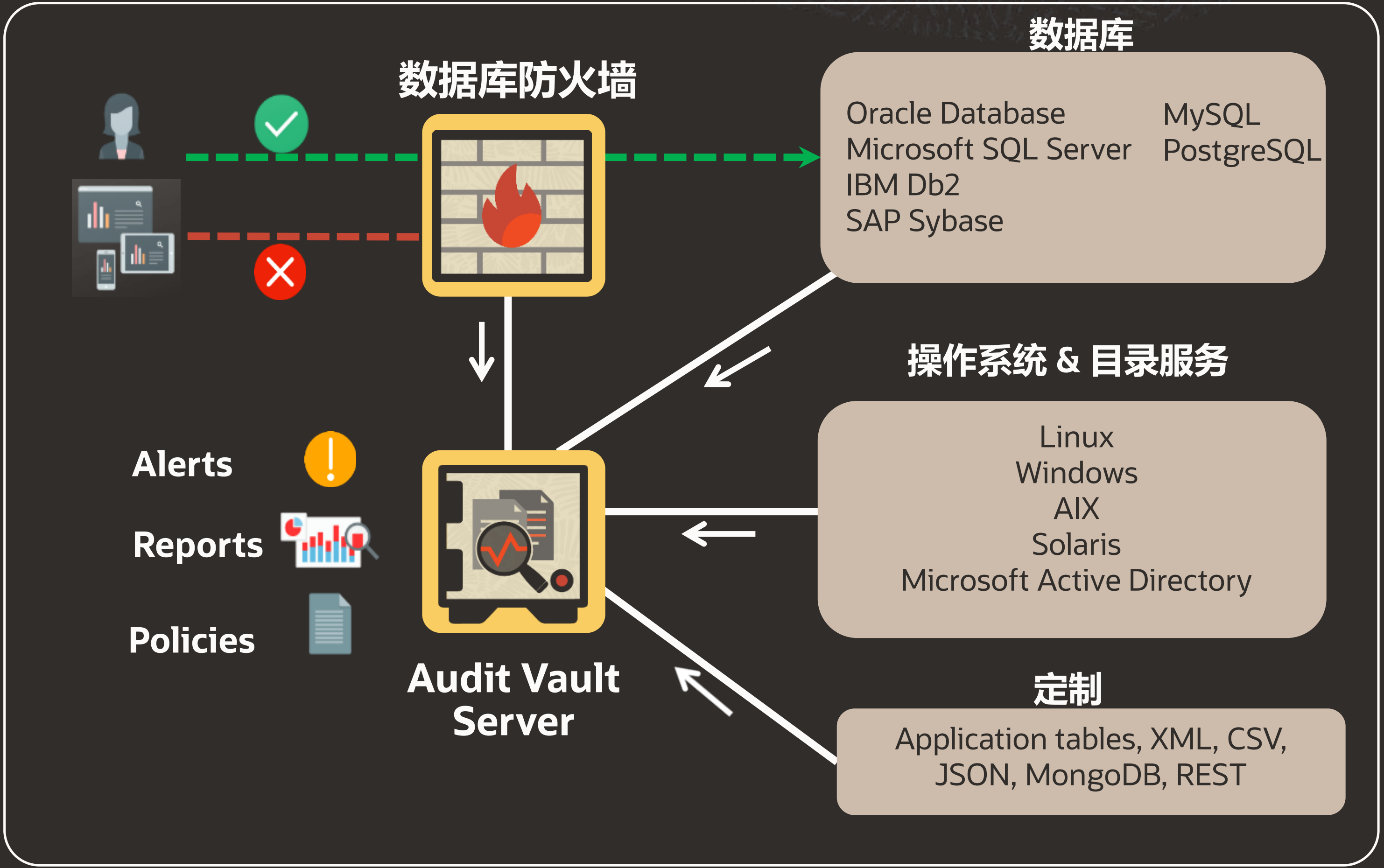
用例

保护你的数据和应用

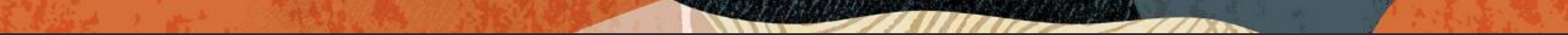
- 实施与活动监控和审计相关的公司安全政策
- 监控和审计特权用户对敏感数据的访问
- 访问企业应用程序的可信路径
- 拦截和监控SQL 语句

加速监管合规

- 满足合规性要求，例如：PCI、HIPAA、GDPR 等。
- 预定义合规报表
- 支持取证分析



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.



主要功能

数据库审计和审计收集

- 审计收集，包括数据访问和修改
- 数据变更之前/之后，权利更改，存储过程更改
- 自定义收集器收集应用审计
- 开箱即用的审计策略

使用数据库防火墙进行 SQL 流量监控

- 基于SQL语法分析的多级防火墙
- 基于会话参数、数据库对象，IP地址的策略
- SQL注入检测与预防
- 通过捕获 SELECT 查询返回的行数来监控和警报检测渗透尝试

报告和警告

- 支持定制的报告可用于取证分析
- 开箱即用的安全性和合规性报告
- 丰富的警报构建器来检测意外活动
- 支持与第三方工具集成

企业部署

- 自动更新代理，便于管理
- 自动归档审计数据以实现合规性
- LDAP/目录认证
- 用于管理审计和网络监控的统一控制台
- SIEM/系统日志集成
- 支持高可用
- 作为全栈软件设备交付

支持的监控目标类型和配置

- 异构目标类型 - Oracle 和非 Oracle 数据库、操作系统日志、目录服务、文件系统
- 可扩展自定义收集器框架（表、XML、CSV、JSON、REST）
- 混合云部署

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

AVDF 20: 新功能

扩大审计收集范围

- 对 PostgreSQL 的内置支持
- 扩展自定义收集器支持以包括 JSON、REST、MongoDB 和 CSV***
- Oracle 数据库数据变更的之前/之后值
- 支持对Oracle Cloud autonomous databases – Dedicated 的审计收集

简化的数据库防火墙

- 简化配置多级策略的防火墙
- 使用 SQL 集群创建更简单的策略
- 数据库对象规则中的会话配置文件过滤***
- 网络吞吐量的 NIC 绑定
- 检测 SELECT 语句的渗漏尝试**

友好的用户界面

- 常见工作流程的简化导航
- 面向审计员和管理员的丰富仪表板
- 审计和防火墙管理的统一控制台

改进的企业支持

- LDAP/目录认证
- 事件数据的自动归档
- FIPS 140-2 兼容性***
- 2X 审计收集率能力***
- 多路径光纤通道支持以实现高可用性
- 集群设置中代理的多个 IP 地址**

: RU3中新增　　*:RU4中 新增

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

扩展的审计收集范围

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

收集数据库审计信息

配置目标和轨迹

- 目标
- 安装代理
- 审计数据
- 数据保留策略

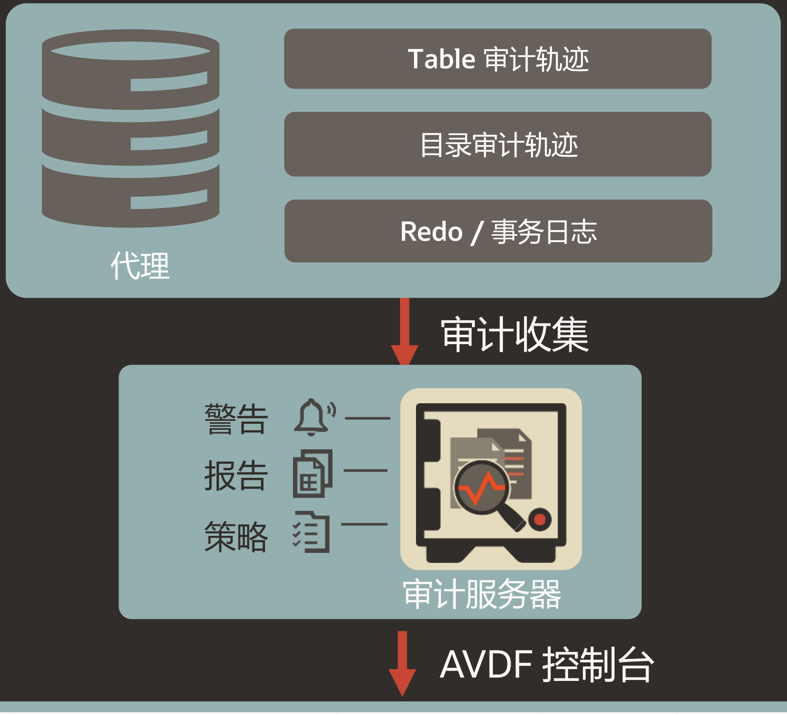
配置审计策略

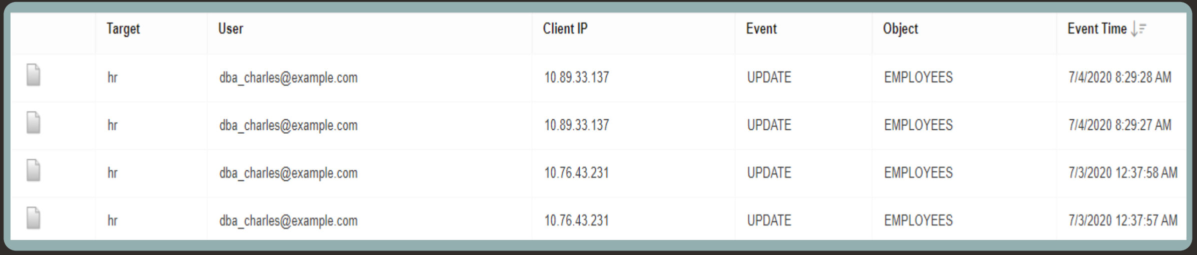
- 是谁
- 做了什么
- 何时
- 何地

创建报告和警告

- 定义警告规则
- 创建和规划报告

Oracle 数据库审计





	Target	User	Client IP	Event	Object	Event Time
	hr	dba_charles@example.com	10.89.33.137	UPDATE	EMPLOYEES	7/4/2020 8:29:28 AM
	hr	dba_charles@example.com	10.89.33.137	UPDATE	EMPLOYEES	7/4/2020 8:29:27 AM
	hr	dba_charles@example.com	10.76.43.231	UPDATE	EMPLOYEES	7/3/2020 12:37:58 AM
	hr	dba_charles@example.com	10.76.43.231	UPDATE	EMPLOYEES	7/3/2020 12:37:57 AM

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

其他支持的目标

AVDF 12.2可支持的目标

- 目标类型：数据库，操作系统日志，目录系统日志，文件系统日志

数据库
Oracle数据库：本地版，云（ATP,ADW）,Exadata, RAC
IBM Db2: LUW, AIX
Microsoft SQL Server
SAP Sybase ASE
MySQL
PostgreSQL

操作系统日志
Oracle Solaris
Oracle Linux
Red Hat Enterprise Linux
Microsoft Windows Server
IBM AIX Power Systems
SuSE Linux

目录服务
Microsoft Active Directory

文件系统
Oracle ACFS

AVDF 20可支持的目标

- 支持MongoDB
- 定制化收集器: REST, CSV, JSON, Quick JSON, MongoDB
- 使用GoldenGate捕获数据变更（Before/after data value)

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

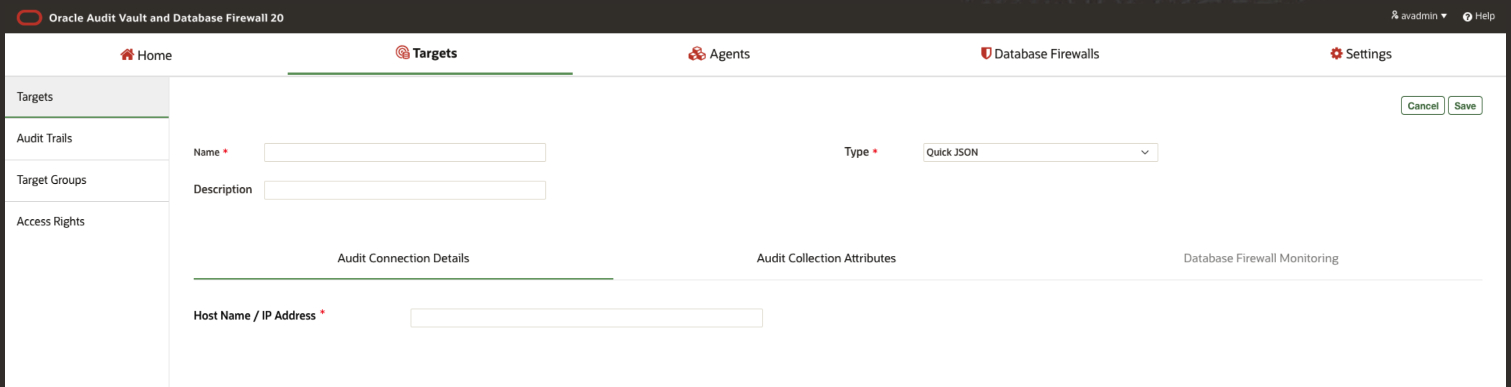
对MongoDB的支持

支持MongoDB

- 使用Quick JSON 作为目标类型
- 为MongoDB审计轨迹提供审计收集属性域

添加目录信息

- 目录信息
- 收集器使用映射从 MongoDB 审计轨迹中读取并映射到 Audit Vault Server 中的字段

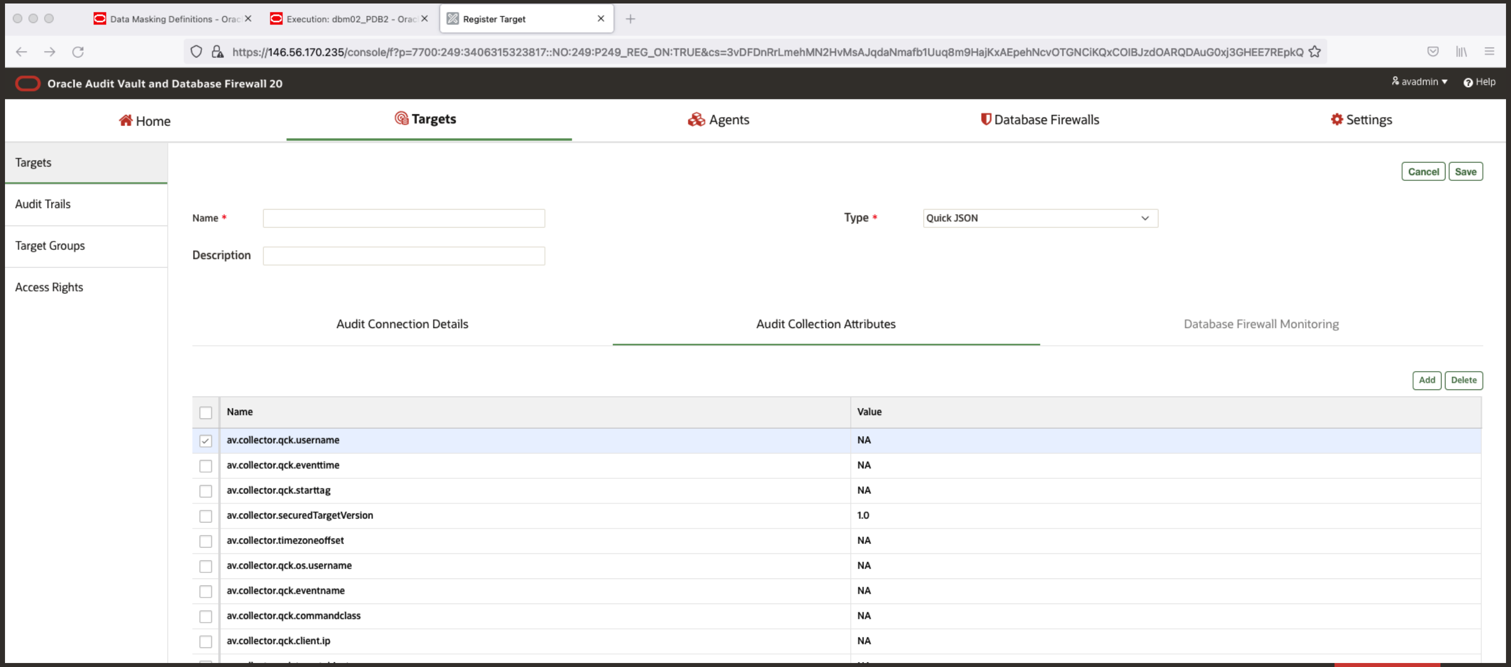

Oracle Audit Vault and Database Firewall 20

Name *

Description

Type * Quick JSON

Host Name / IP Address *



https://146.56.170.235/console/f?p=7700:249:3406315323817::NO:249:P249_REG_ON:TRUE&cs=3vDFDnRrLmehMN2HvMsAJqdaNmafb1Uuq8m9HajKxAEpehNcvOTGNCiKQxCOIBJzdOARQDAuG0xj3GHEE7REpkQ

Oracle Audit Vault and Database Firewall 20

Name *

Description

Type * Quick JSON

□	Name	Value
☑	av.collector.qck.username	NA
□	av.collector.qck.eventtime	NA
□	av.collector.qck.starttag	NA
□	av.collector.securedTargetVersion	1.0
□	av.collector.timezoneoffset	NA
□	av.collector.qck.os.username	NA
□	av.collector.qck.eventname	NA
□	av.collector.qck.commandclass	NA
□	av.collector.qck.client.ip	NA

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

Quick JSON 映射属性

映射

- 列出收集器属性与对应的JSON文件中值
- .收集器属性包括：事件时间，用户名，系统用户，对象，和行为等
- 文档中提供的映射

映射 (基于文档内容)

Audit Vault Collector Attribute	MongoDB JSON File Value
av.collector.qck.starttag	atype
av.collector.qck.eventtime	$.ts.$date
av.collector.qck.username	$.users[0].user
av.collector.qck.os.username	$.users[0].user
…	…

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

使用GoldenGate捕获数据变更（before/after value）

在 AVDF 12.2 中

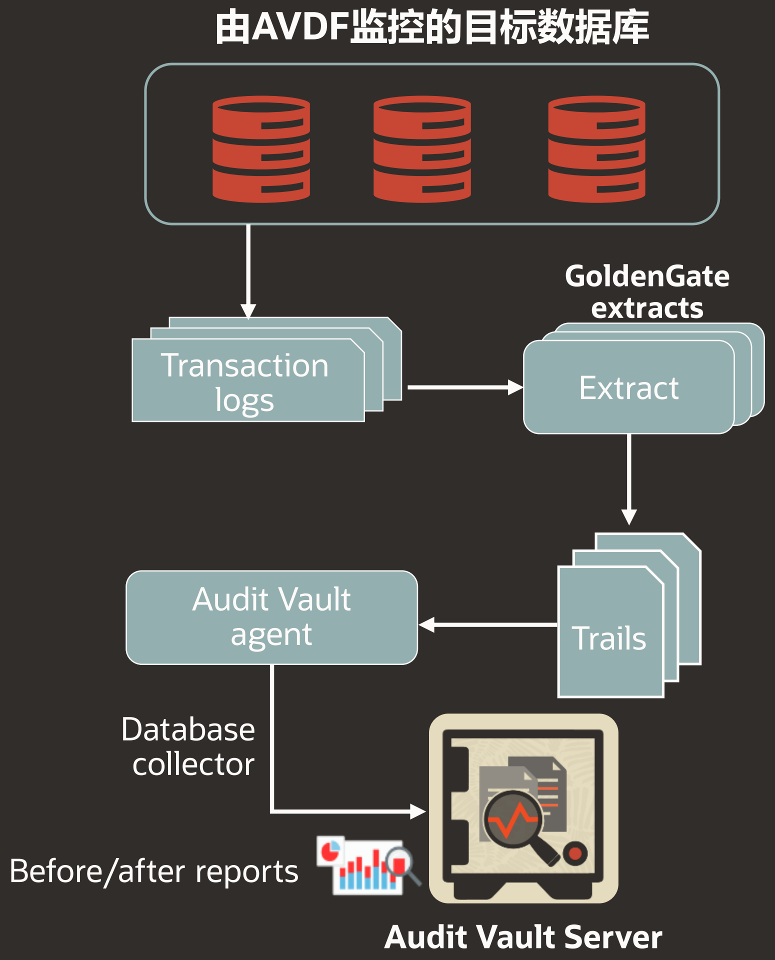
- 使用Oracle Streams 技术收集数据变更的事务日志
- 从Oracle DB19C 之后， Oracle Streams 技术不再支持
- Oracle GoldenGate 是 Oracle 数据库的复制解决方案

在AVDF 20中

- 使用 Oracle GoldenGate 19.1 集成提取流程捕获 Oracle 数据库数据的前后变更值
- 与流相比的附加功能：
  - 多租户的支持
  - 表对象的灵活选择
- Oracle GoldenGate 有限的使用许可
  - 对于 12.2 之前的 Oracle 数据库，需要配置下游挖掘- 需要 Oracle 企业版数据库，必须单独许可
  - 对于任何其他用途，客户需要获得适当的许可。

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

GoldenGate部署



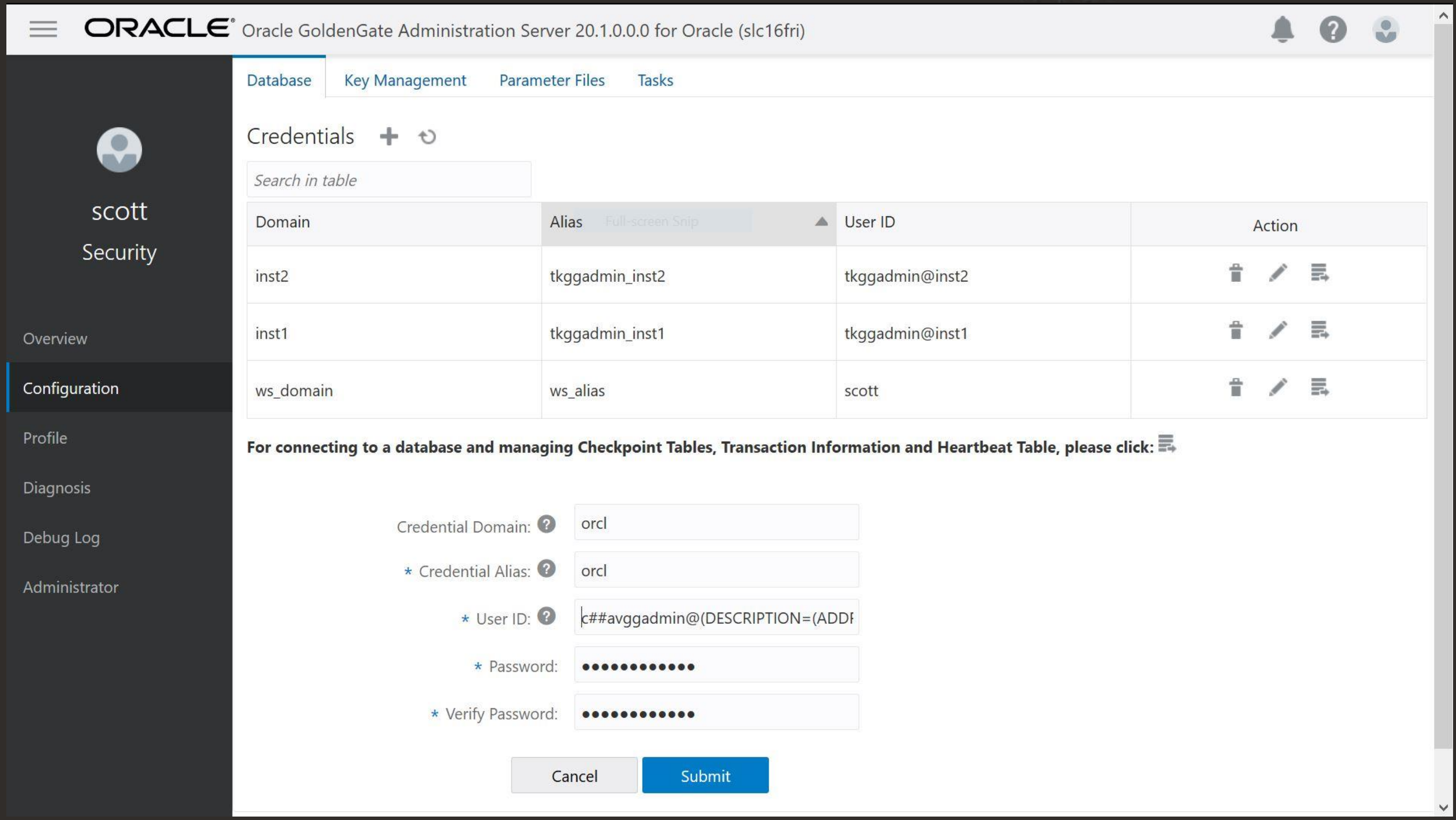
- 安装 Oracle GoldenGate 微服务架构（最低版本 19.1.0.0.4）
  - 可以在与源数据库相同的服务器上运行，也可以在独立服务器上运行
  - 无法在与 AVDF 相同的服务器上运行
- 在 GoldenGate 控制台中为每个源数据库配置集成提取过程
  - DDL和DML
  - 需要提取数据的表
- 在 AVDF 中配置事务日志审计跟踪
  - AVDF 代理应该能够访问trail文件

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

GoldenGate集成提取过程

1. 在 CDB 级别创建具有相关权限的新用户。 GoldenGate 用于获取事务日志
2. 在目标上启用 GoldenGate 复制
3. 在 GoldenGate 管理服务器中为目标创建新的凭证

步骤 3: 创建新的密码



Oracle GoldenGate Administration Server 20.1.0.0.0 for Oracle (slc16fri)

Credentials

Domain	Alias	User ID	Action
inst2	tkggadmin_inst2	tkggadmin@inst2	
inst1	tkggadmin_inst1	tkggadmin@inst1	
ws_domain	ws_alias	scott	

For connecting to a database and managing Checkpoint Tables, Transaction Information and Heartbeat Table, please click:

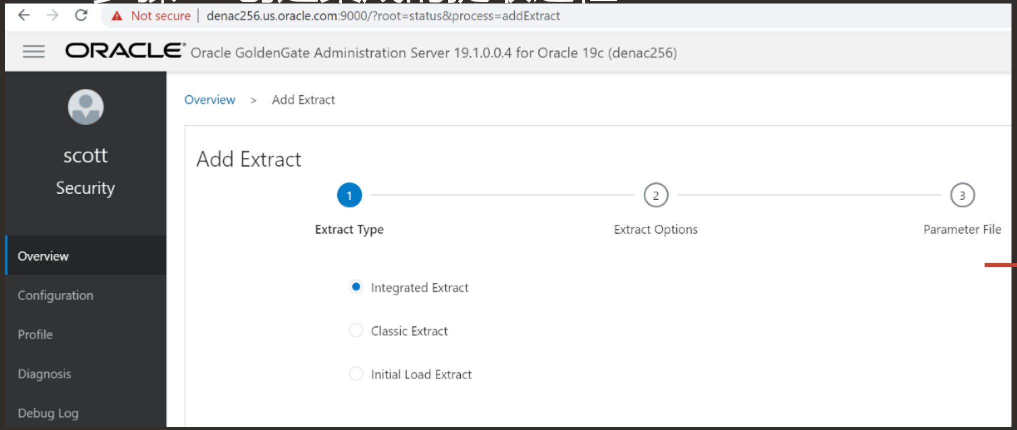
Credential Domain:	orcl
* Credential Alias:	orcl
* User ID:	c##avggadmin@(DESCRIPTION=(ADDI
* Password:	●●●●●●●●●●●●
* Verify Password:	●●●●●●●●●●●●

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

GoldenGate集成提取过程

4. 在 GoldenGate 管理服务器中创建新的集成提取流程
   - 指定单向、路径位置、PDB、参数文件等。

步骤 4: 创建集成的提取过程



← → C ▲ Not secure | denac256.us.oracle.com:9000/?root=status&process=addExtract

ORACLE Oracle GoldenGate Administration Server 19.1.0.0.4 for Oracle 19c (denac256)

scott
Security

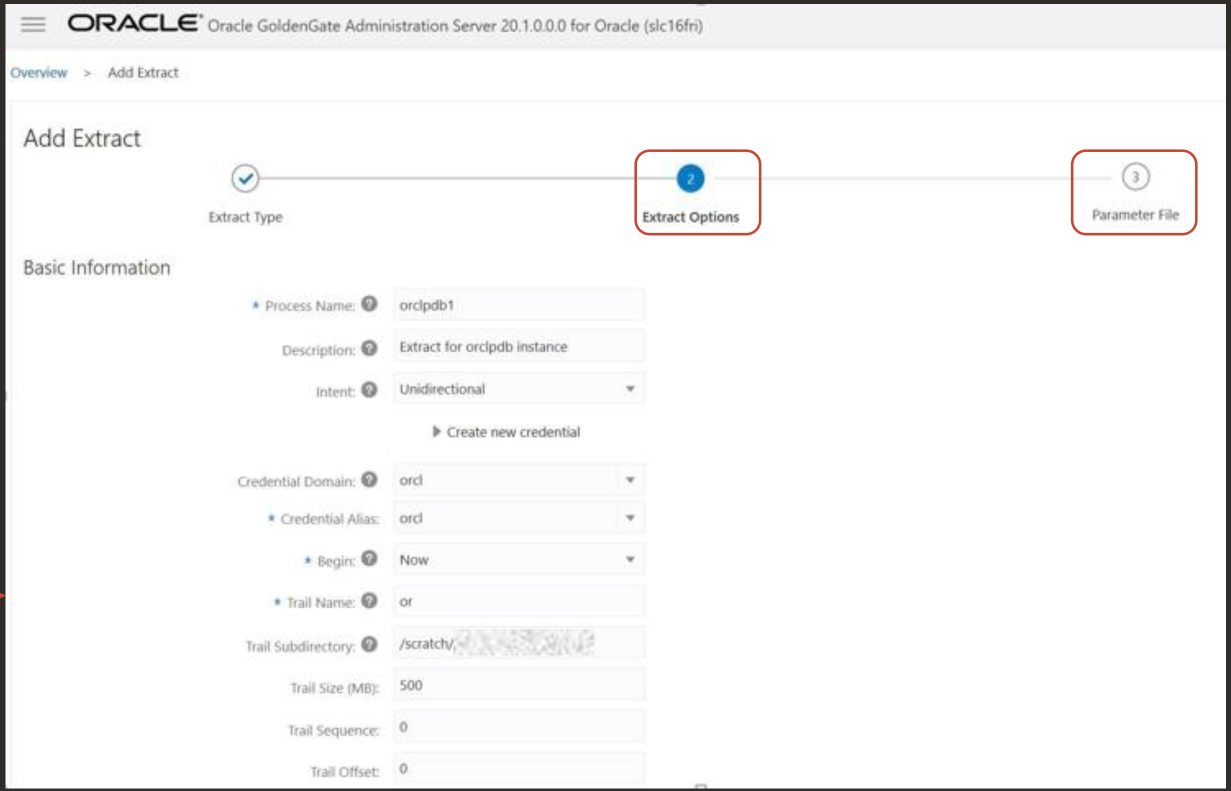
- Overview
- Configuration
- Profile
- Diagnosis
- Debug Log

Overview > Add Extract

Add Extract

1 Extract Type — 2 Extract Options — 3 Parameter File

● Integrated Extract
○ Classic Extract
○ Initial Load Extract



ORACLE Oracle GoldenGate Administration Server 20.1.0.0.0 for Oracle (slc16fri)

Overview > Add Extract

Add Extract

✓ Extract Type — 2 Extract Options — 3 Parameter File

Basic Information

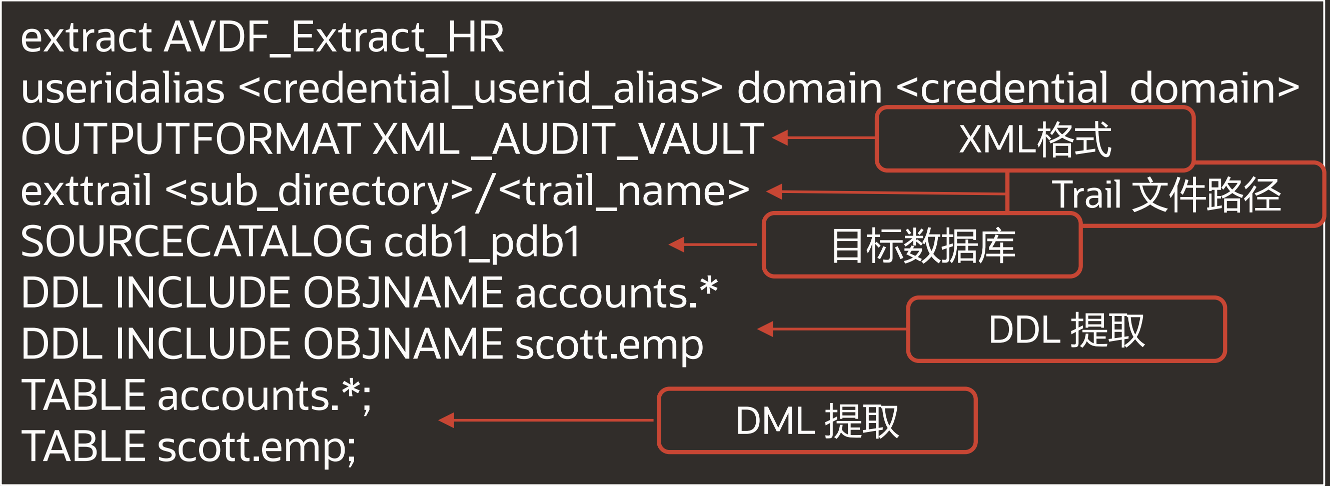
* Process Name:	orclpdb1
Description:	Extract for orclpdb instance
Intent:	Unidirectional
	▶ Create new credential
Credential Domain:	orcl
* Credential Alias:	orcl
* Begin:	Now
* Trail Name:	or
Trail Subdirectory:	/scratch/[redacted]
Trail Size (MB):	500
Trail Sequence:	0
Trail Offset:	0

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

GoldenGate 集成提取过程

4
在参数文件窗口中，输入参数以指示需要提取哪些表 DDL/DML

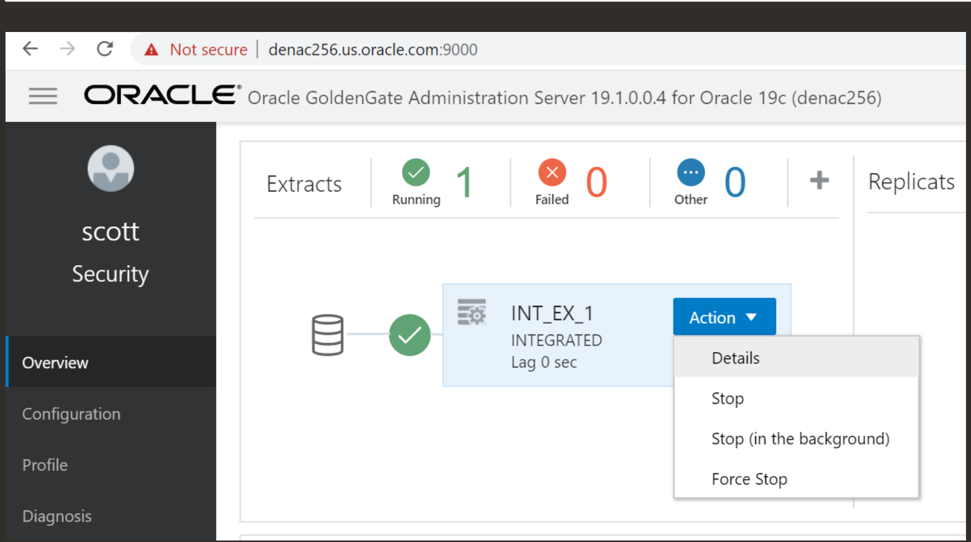
Step 4: 参数文件



```
extract AVDF_Extract_HR
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
DDL INCLUDE OBJNAME accounts.*
DDL INCLUDE OBJNAME scott.emp
TABLE accounts.*;
TABLE scott.emp;
```

5. 点击创建并运行以启动集成提取过程

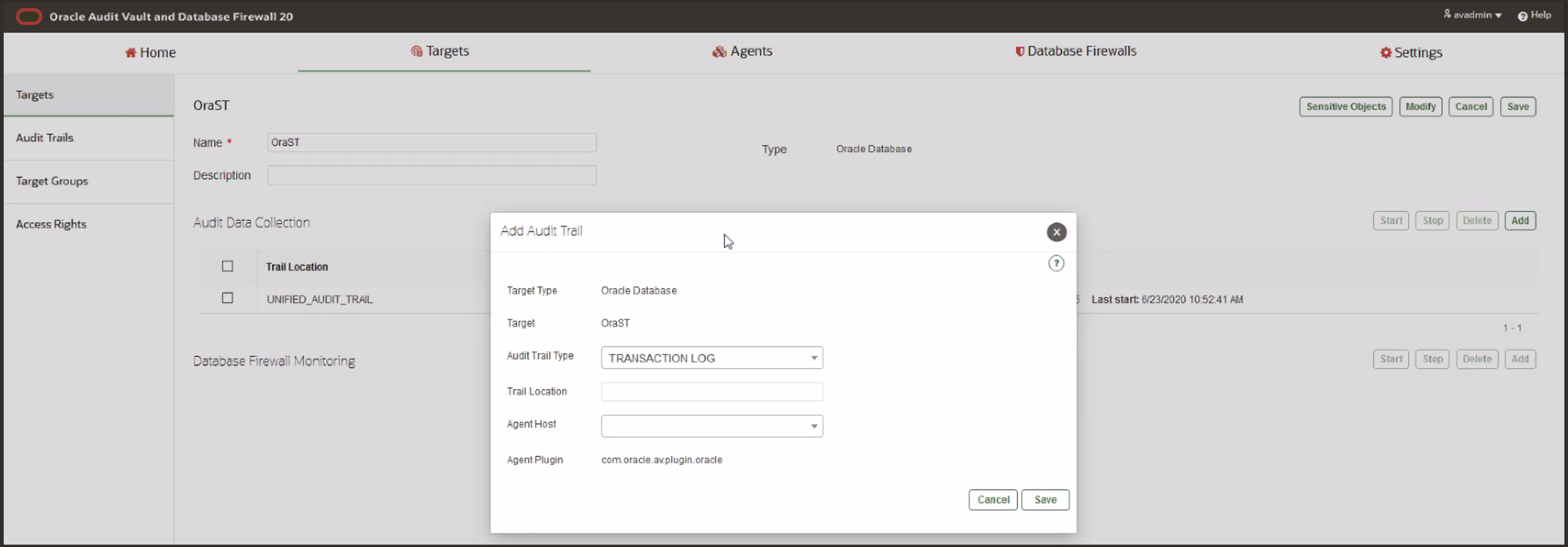
Step 5



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

在AVDF中添加事务日志轨迹

步骤6：添加事务轨迹



OraST

Name * OraST

Description

Type Oracle Database

□	Trail Location
□	UNIFIED_AUDIT_TRAIL

Last start: 6/23/2020 10:52:41 AM

Add Audit Trail

Target Type	Oracle Database
Target	OraST
Audit Trail Type	TRANSACTION LOG
Trail Location	
Agent Host	
Agent Plugin	com.oracle.av.plugin.oracle

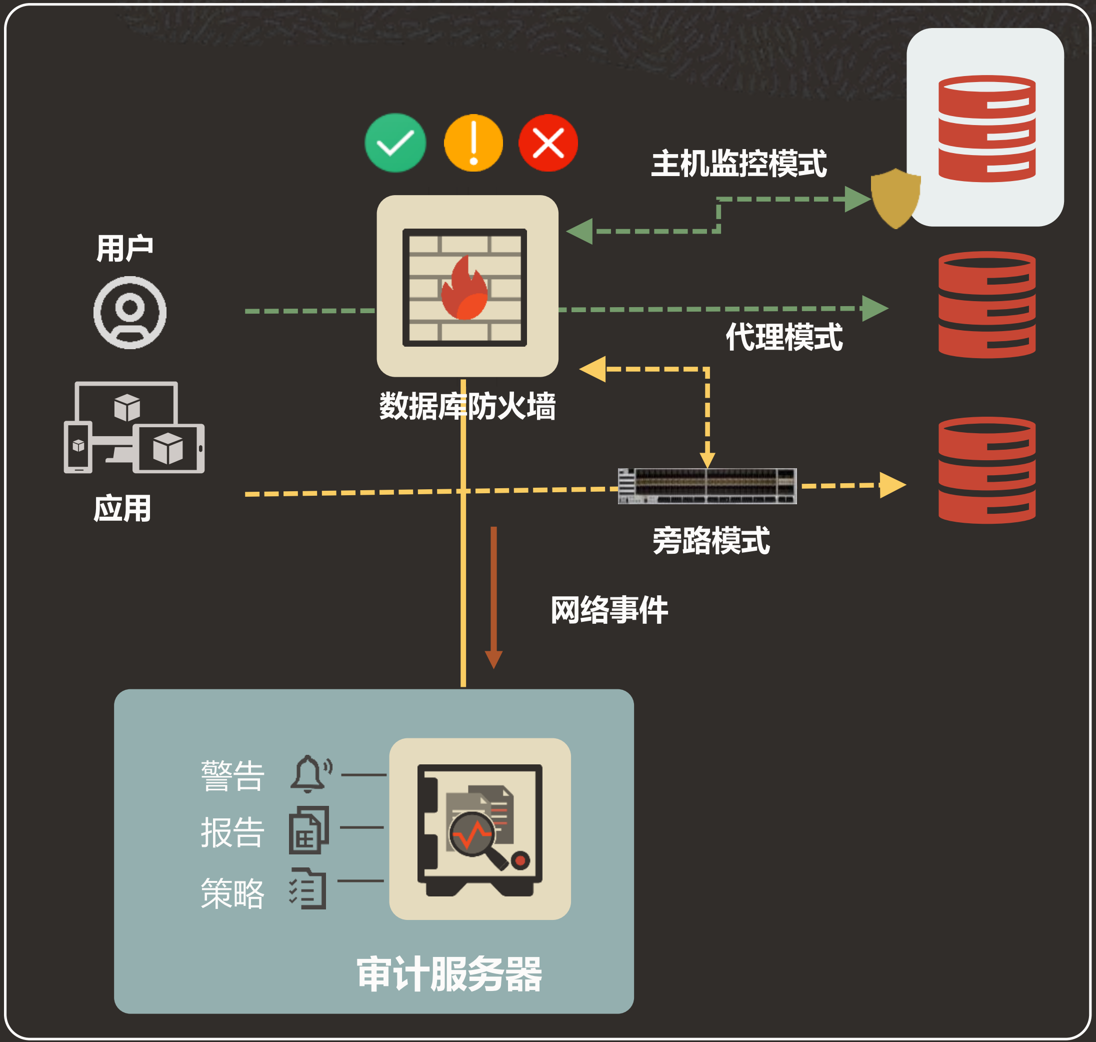
Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

简化的数据库防火墙

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

防火墙部署模式

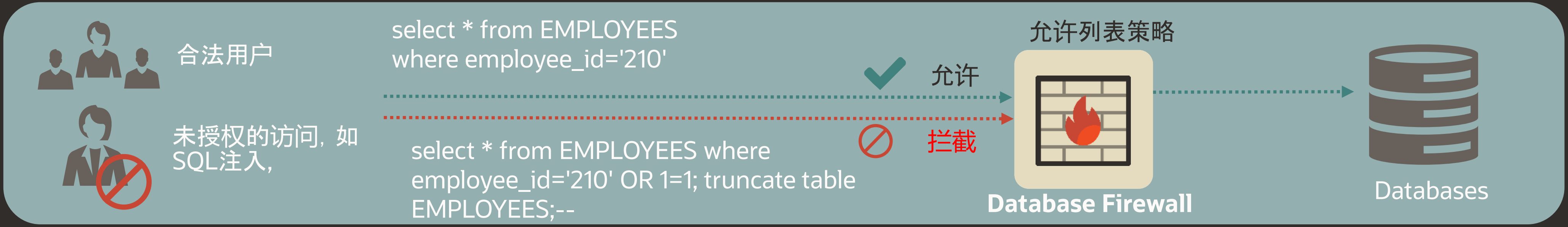
模式	内容	支持的功能	
		监控	拦截
代理模式	所有客户端连接都通过防火墙，包括返回流量	✓	✓
主机监控模式	在数据库主机上运行的代理侦听传入流量	✓	
旁路模式	通过路由器或交换机转发数据库端的流量	✓	



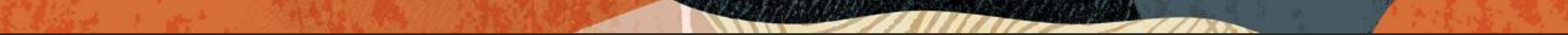
Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

使用数据库防火墙进行网络监控

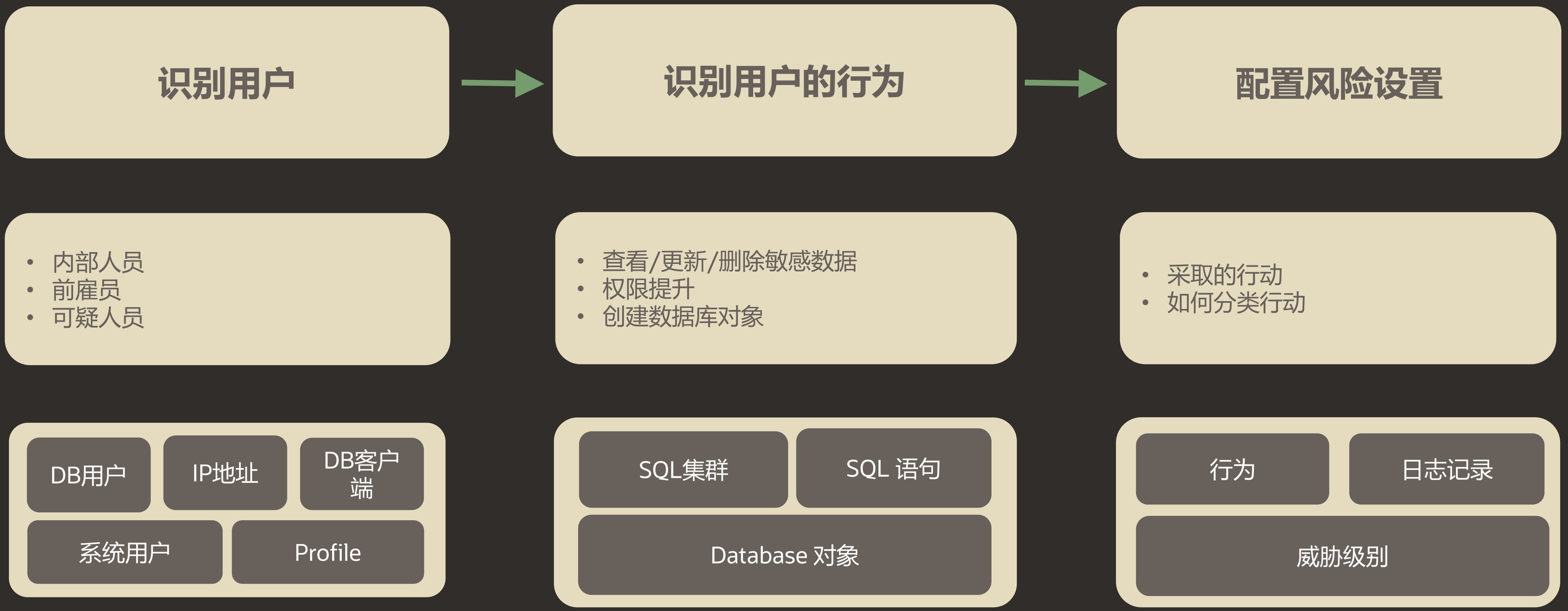
- 收集常规的应用查询模式
- 监控或拦截未见过的查询到达数据库
- 使用基于允许列表或拒绝列表的策略进行异常监控和威胁拦截
- 并不是使用正则表达式识别查询语句



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.



在数据库防火墙中构建策略



识别用户 → 识别用户的行为 → 配置风险设置

- 内部人员
- 前雇员
- 可疑人员

DB用户 IP地址 DB客户端

系统用户 Profile

- 查看/更新/删除敏感数据
- 权限提升
- 创建数据库对象

SQL集群 SQL 语句

Database 对象

- 采取的行动
- 如何分类行动

行为 日志记录

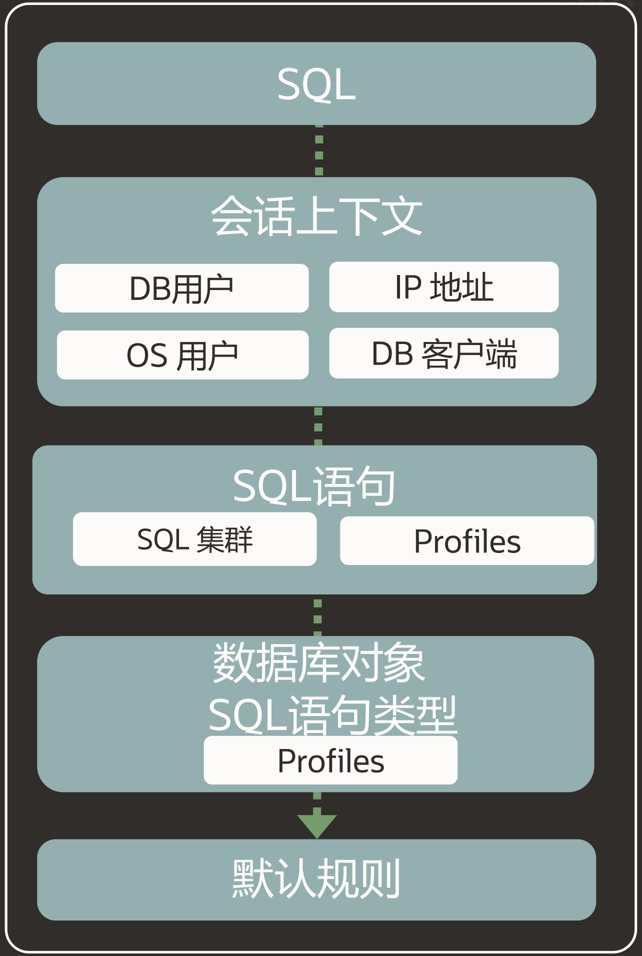
威胁级别

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

多级防火墙策略

- 防火墙策略可以基于会话上下文、查询语句、数据库对象或它们的组合
- 策略按顺序执行
- 可以开发满足各种用例的从简单到复杂的防火墙策略

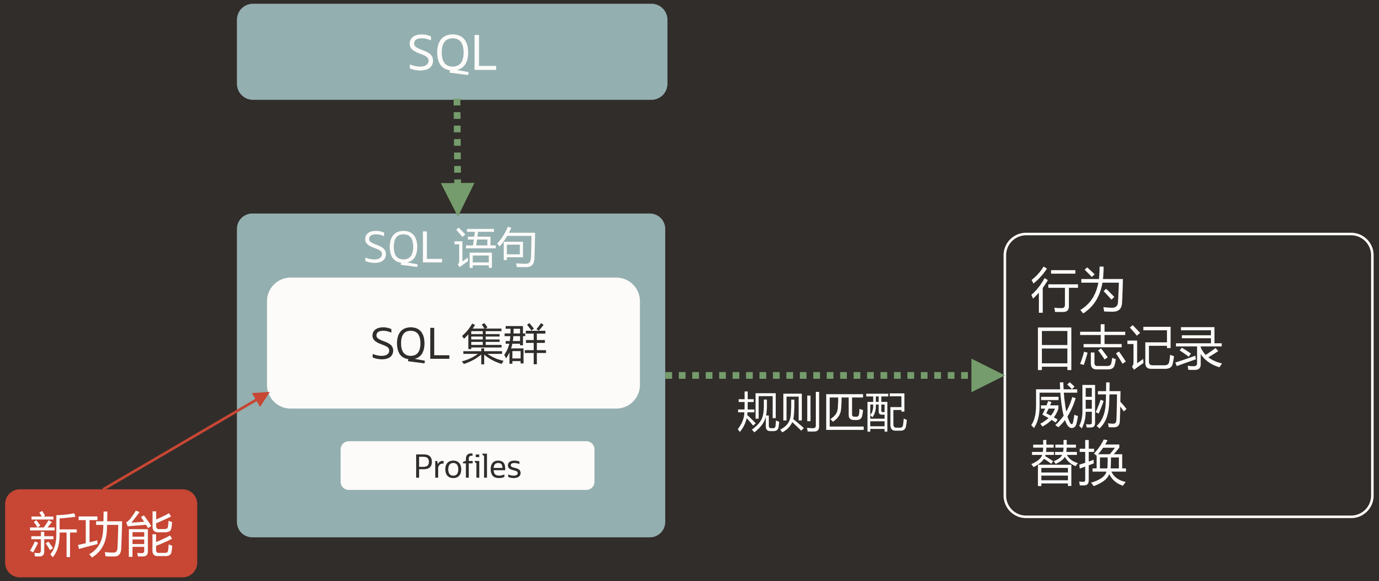
执行顺序



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

在 SQL 集群上创建策略

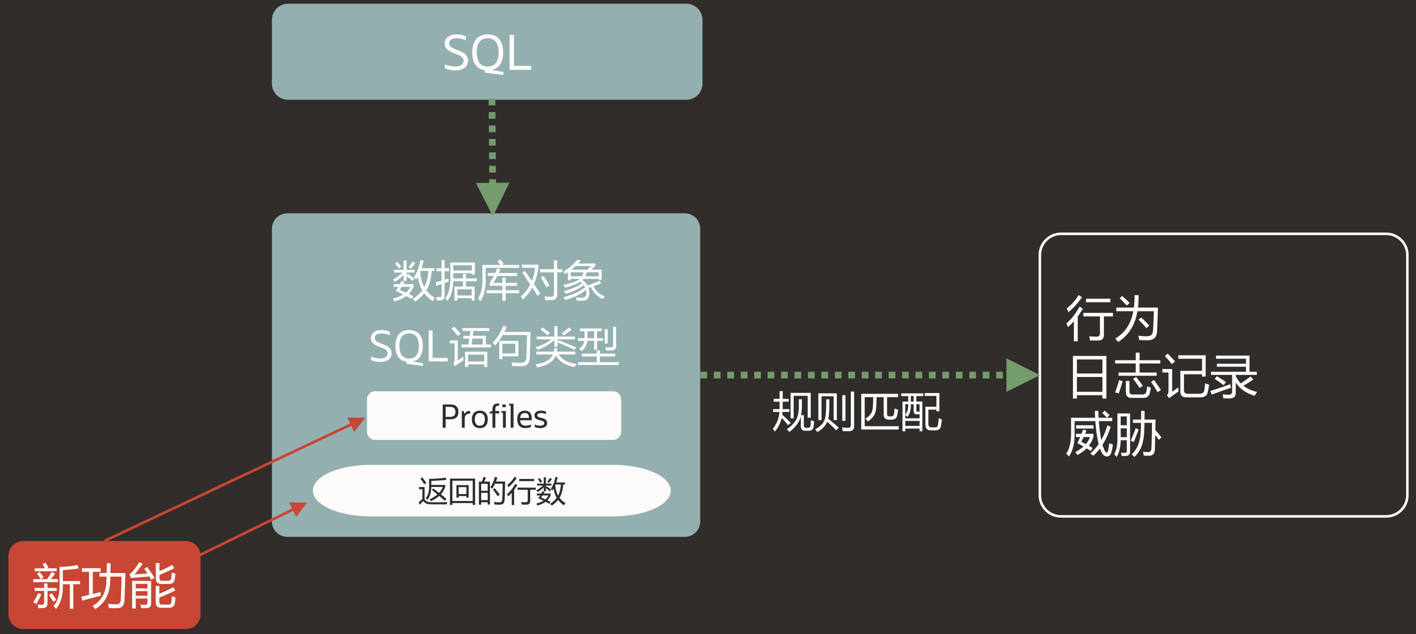
- 基于已知 SQL 训练防火墙以创建允许列表或拒绝列表
- 实施基于特定 SQL 集群的策略——例如 特权用户访问



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

检测数据库对象上的 SQL 访问/响应模式

- 可基于DDL/DML创建防火墙策略，同时也可基于会话生成更细粒度的控制
  - 例如 监控特权用户对敏感表的修改尝试并发出警报
- 能够通过捕获 SQL SELECT 查询返回的行数来监控和警报检测到渗透尝试



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

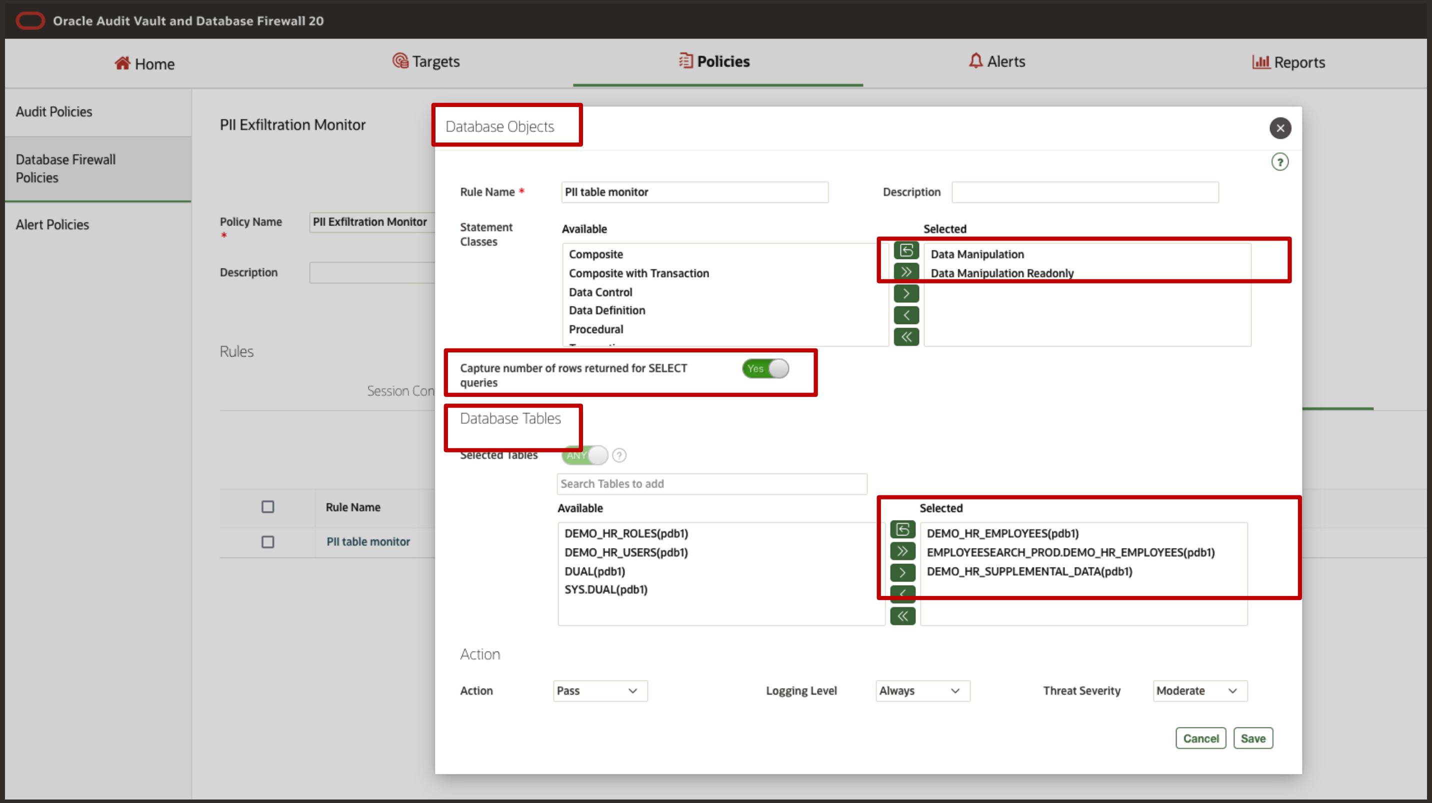
数据泄露监控和警报

监视和警告从 Oracle 数据库的敏感表中进行的数据提取

- 捕获并报告返回的行数
- 仅在 Select 语句的数据库对象规则中受支持
- 返回的行数超过阈值时发出警报

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

示例：监控员工数据信息泄露的尝试



Policy Name * PII Exfiltration Monitor

Description

Database Objects

Rule Name * PII table monitor

Description

Statement Classes

Available: Composite, Composite with Transaction, Data Control, Data Definition, Procedural

Selected: Data Manipulation, Data Manipulation Readonly

Capture number of rows returned for SELECT queries: Yes

Database Tables

Selected Tables: ANY

Search Tables to add

Available: DEMO_HR_ROLES(pdb1), DEMO_HR_USERS(pdb1), DUAL(pdb1), SYS.DUAL(pdb1)

Selected: DEMO_HR_EMPLOYEES(pdb1), EMPLOYEESEARCH_PROD.DEMO_HR_EMPLOYEES(pdb1), DEMO_HR_SUPPLEMENTAL_DATA(pdb1)

Action

Action: Pass

Logging Level: Always

Threat Severity: Moderate

Cancel Save

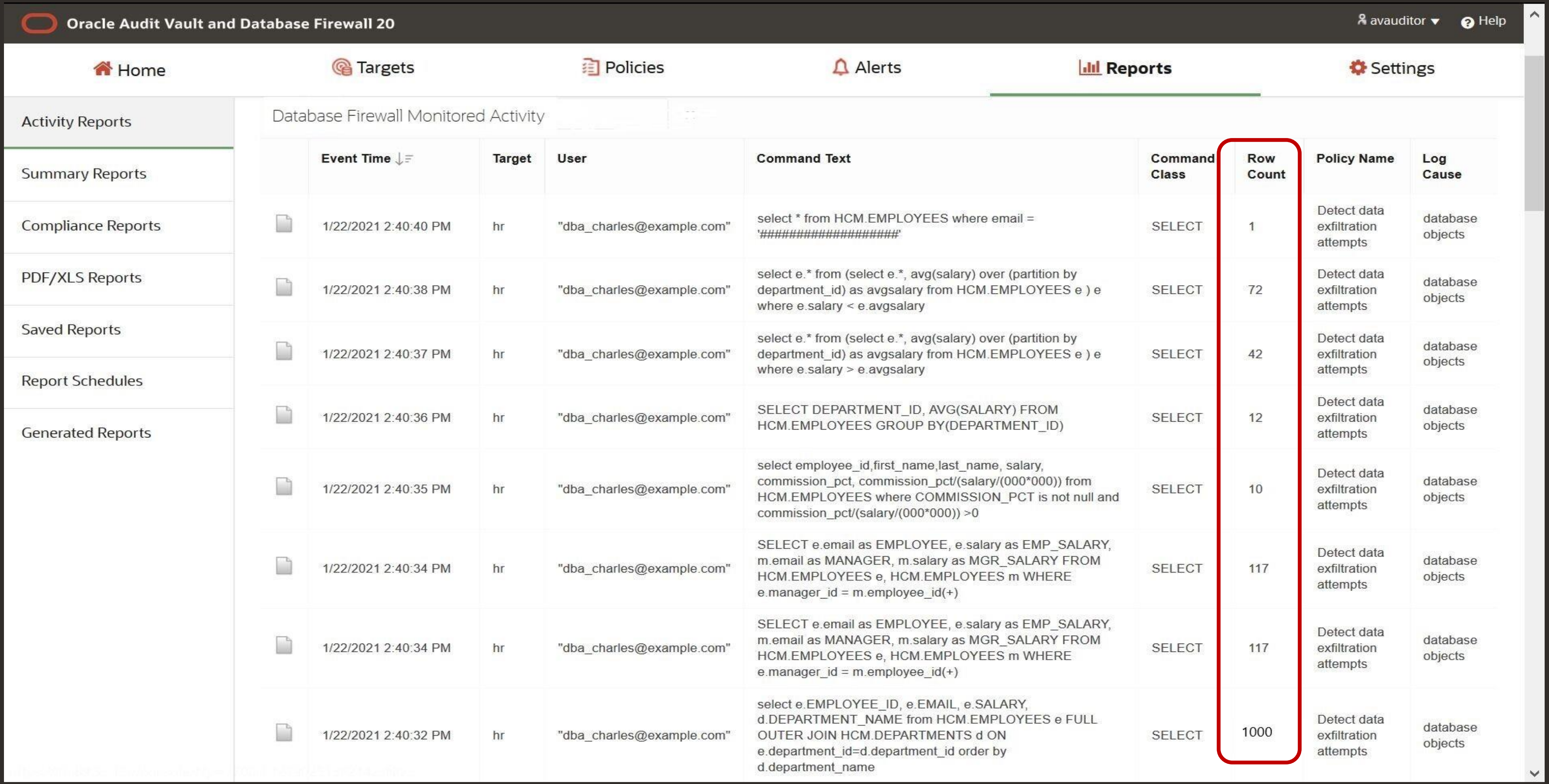
- 使用数据库对象规则
- 语句类型： SELECT
- 监控员工表

注:

- 应用于SELECT语句的规则

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

示例：监控员工数据信息泄露的尝试—审计报告



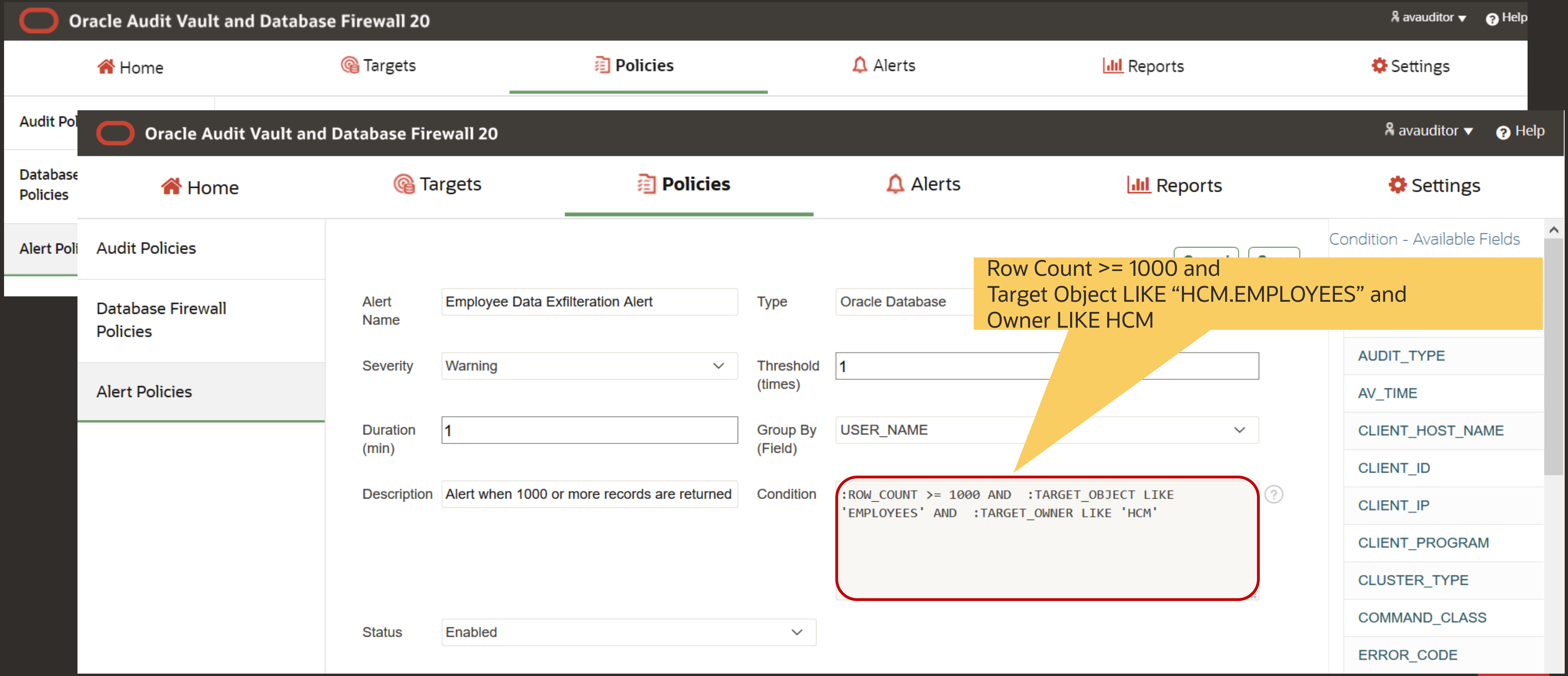
Oracle Audit Vault and Database Firewall 20

Database Firewall Monitored Activity

	Event Time	Target	User	Command Text	Command Class	Row Count	Policy Name	Log Cause
	1/22/2021 2:40:40 PM	hr	"dba_charles@example.com"	select * from HCM.EMPLOYEES where email = '#######################'	SELECT	1	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:38 PM	hr	"dba_charles@example.com"	select e.* from (select e.*, avg(salary) over (partition by department_id) as avgsalary from HCM.EMPLOYEES e) e where e.salary < e.avgsalary	SELECT	72	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:37 PM	hr	"dba_charles@example.com"	select e.* from (select e.*, avg(salary) over (partition by department_id) as avgsalary from HCM.EMPLOYEES e) e where e.salary > e.avgsalary	SELECT	42	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:36 PM	hr	"dba_charles@example.com"	SELECT DEPARTMENT_ID, AVG(SALARY) FROM HCM.EMPLOYEES GROUP BY(DEPARTMENT_ID)	SELECT	12	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:35 PM	hr	"dba_charles@example.com"	select employee_id,first_name,last_name, salary, commission_pct, commission_pct/(salary/(000*000)) from HCM.EMPLOYEES where COMMISSION_PCT is not null and commission_pct/(salary/(000*000)) >0	SELECT	10	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:34 PM	hr	"dba_charles@example.com"	SELECT e.email as EMPLOYEE, e.salary as EMP_SALARY, m.email as MANAGER, m.salary as MGR_SALARY FROM HCM.EMPLOYEES e, HCM.EMPLOYEES m WHERE e.manager_id = m.employee_id(+)	SELECT	117	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:34 PM	hr	"dba_charles@example.com"	SELECT e.email as EMPLOYEE, e.salary as EMP_SALARY, m.email as MANAGER, m.salary as MGR_SALARY FROM HCM.EMPLOYEES e, HCM.EMPLOYEES m WHERE e.manager_id = m.employee_id(+)	SELECT	117	Detect data exfiltration attempts	database objects
	1/22/2021 2:40:32 PM	hr	"dba_charles@example.com"	select e.EMPLOYEE_ID, e.EMAIL, e.SALARY, d.DEPARTMENT_NAME from HCM.EMPLOYEES e FULL OUTER JOIN HCM.DEPARTMENTS d ON e.department_id=d.department_id order by d.department_name	SELECT	1000	Detect data exfiltration attempts	database objects

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

示例：监控员工数据信息泄露的尝试—警告设置



Alert Name	Employee Data Exfilteration Alert	Type	Oracle Database
Severity	Warning	Threshold (times)	1
Duration (min)	1	Group By (Field)	USER_NAME
Description	Alert when 1000 or more records are returned	Condition	:ROW_COUNT >= 1000 AND :TARGET_OBJECT LIKE 'EMPLOYEES' AND :TARGET_OWNER LIKE 'HCM'
Status	Enabled		

```
:ROW_COUNT >= 1000 AND  :TARGET_OBJECT LIKE
'EMPLOYEES' AND  :TARGET_OWNER LIKE 'HCM'
```

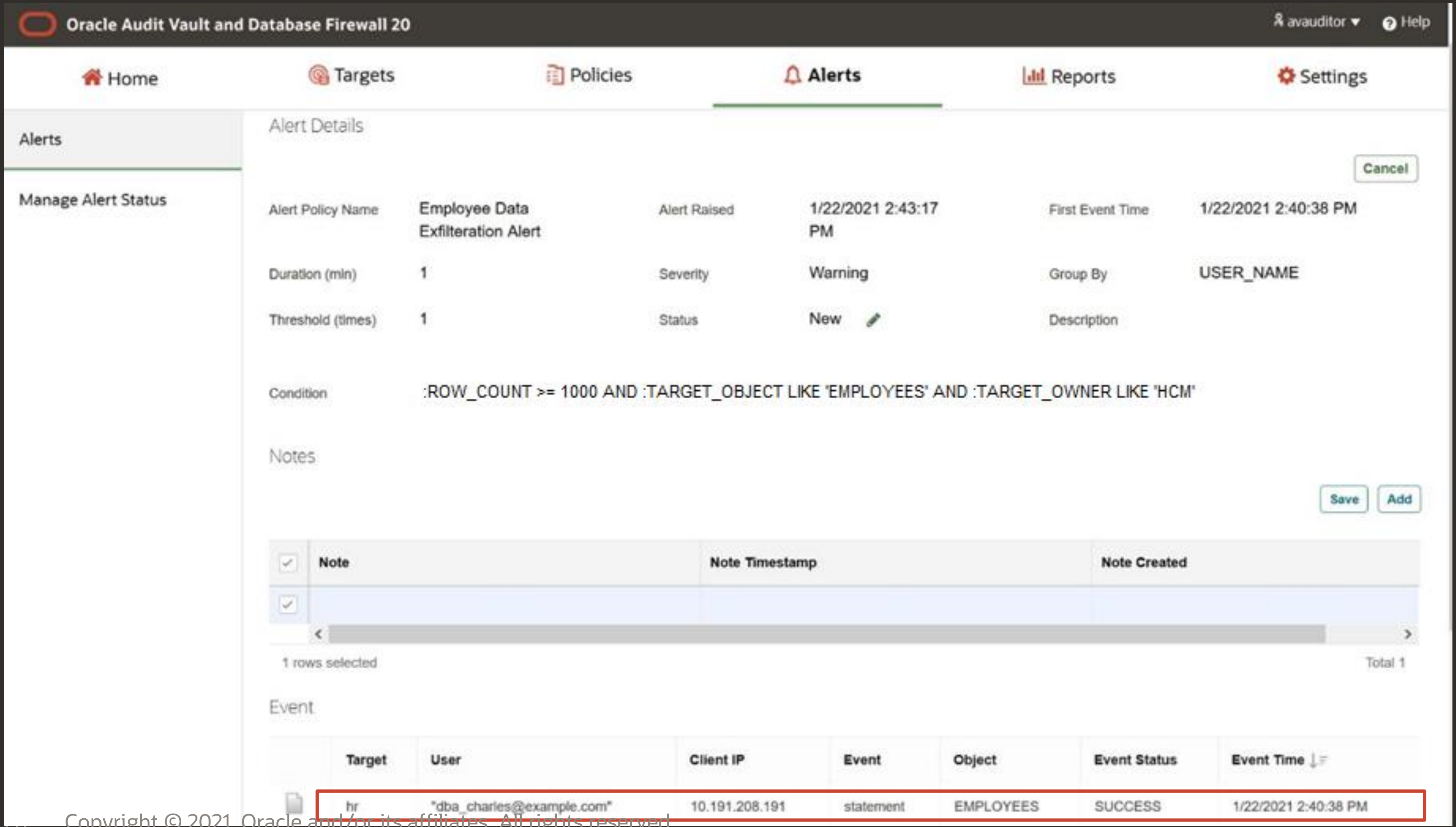
Condition - Available Fields:

- AUDIT_TYPE
- AV_TIME
- CLIENT_HOST_NAME
- CLIENT_ID
- CLIENT_IP
- CLIENT_PROGRAM
- CLUSTER_TYPE
- COMMAND_CLASS
- ERROR_CODE

Row Count >= 1000 and
Target Object LIKE “HCM.EMPLOYEES” and
Owner LIKE HCM

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

示例：监控员工数据信息泄露的尝试—警告内容



Alert Details

Alert Policy Name	Employee Data Exfiltration Alert	Alert Raised	1/22/2021 2:43:17 PM	First Event Time	1/22/2021 2:40:38 PM
Duration (min)	1	Severity	Warning	Group By	USER_NAME
Threshold (times)	1	Status	New	Description	

Condition :ROW_COUNT >= 1000 AND :TARGET_OBJECT LIKE 'EMPLOYEES' AND :TARGET_OWNER LIKE 'HCM'

Notes

✓	Note	Note Timestamp	Note Created
✓			

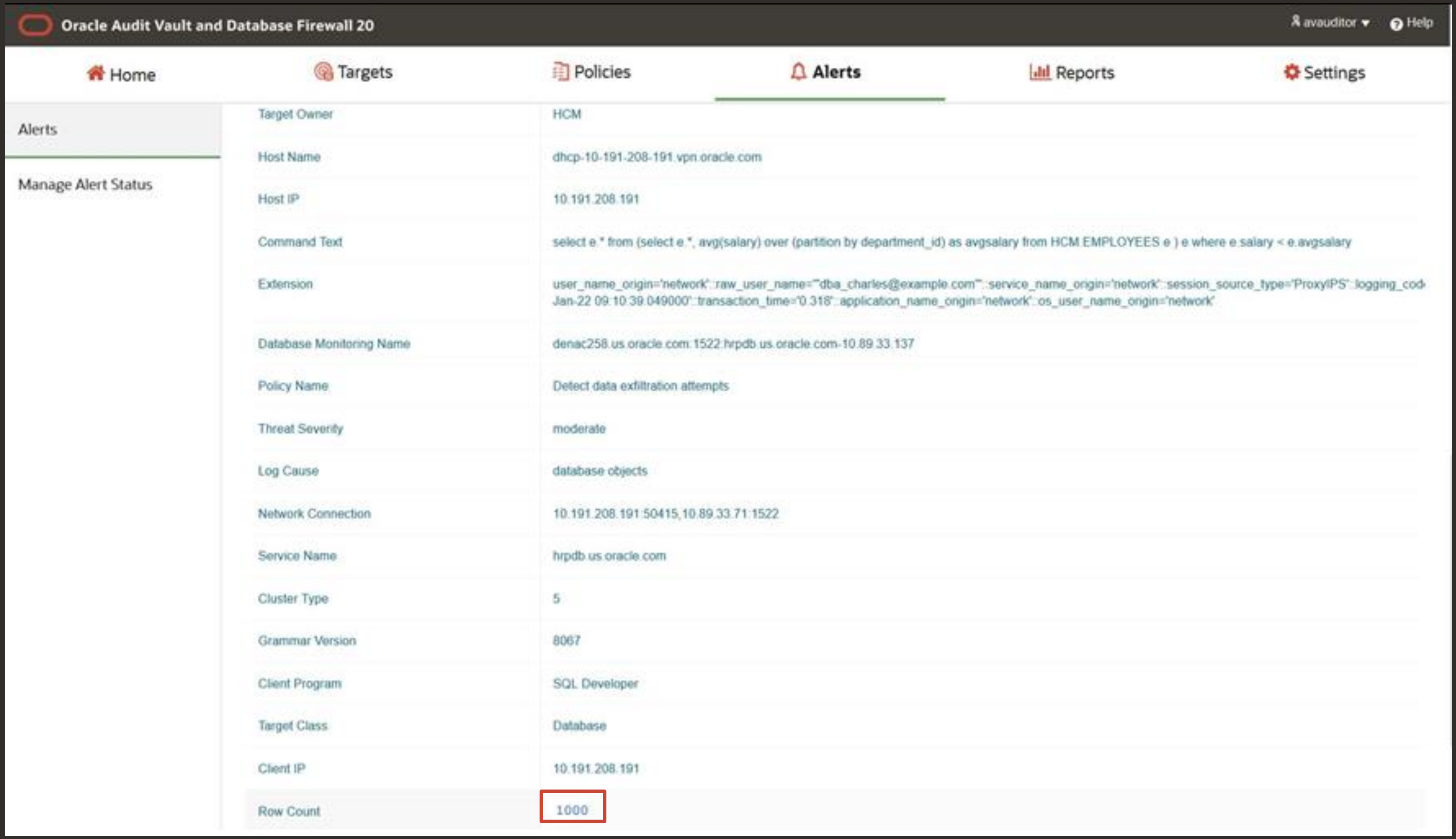
1 rows selected Total 1

Event

	Target	User	Client IP	Event	Object	Event Status	Event Time
	hr	"dba_charles@example.com"	10.191.208.191	statement	EMPLOYEES	SUCCESS	1/22/2021 2:40:38 PM

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

示例：监控员工数据信息泄露的尝试—查看具体信息



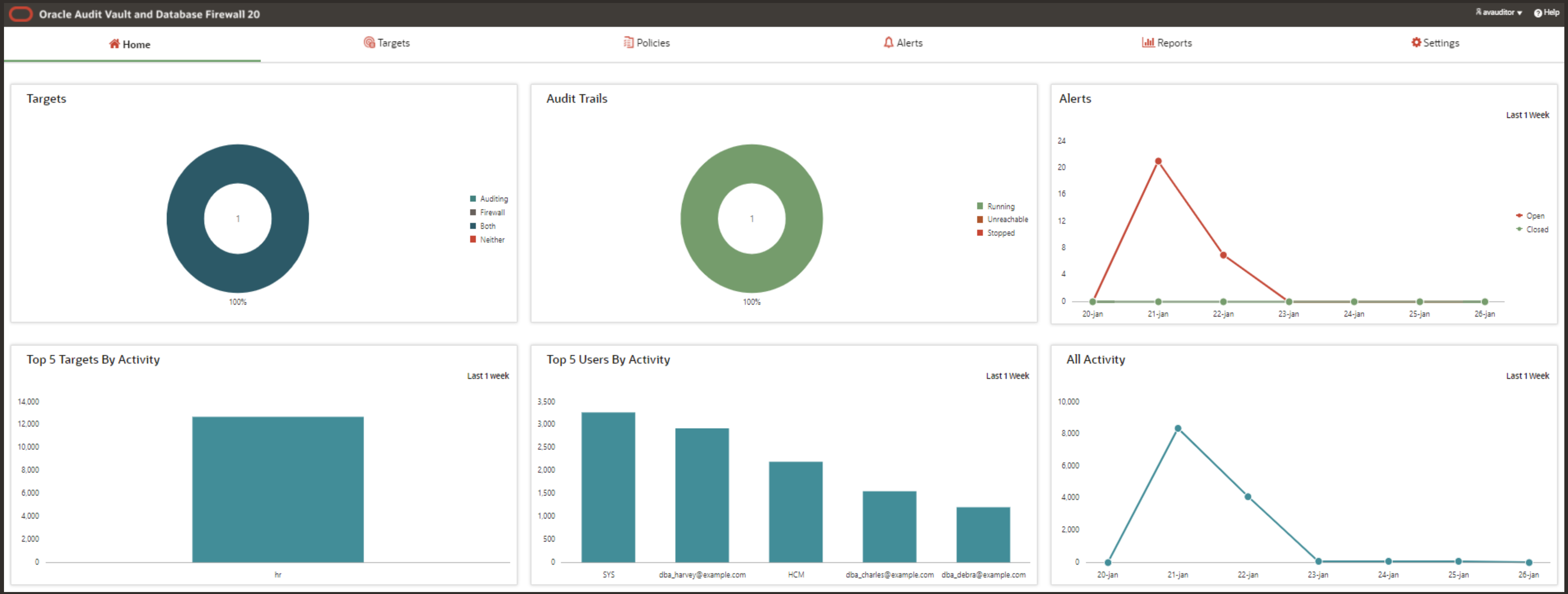
Target Owner	HCM
Host Name	dhcp-10-191-208-191.vpn.oracle.com
Host IP	10.191.208.191
Command Text	select e.* from (select e.*, avg(salary) over (partition by department_id) as avgsalary from HCM.EMPLOYEES e) e where e.salary < e.avgsalary
Extension	user_name_origin='network'::raw_user_name='"dba_charles@example.com"'::service_name_origin='network'::session_source_type='ProxyIPS'::logging_cod Jan-22 09:10:39.049000'::transaction_time='0.318'::application_name_origin='network'::os_user_name_origin='network'
Database Monitoring Name	denac258.us.oracle.com:1522:hrpdb.us.oracle.com-10.89.33.137
Policy Name	Detect data exfiltration attempts
Threat Severity	moderate
Log Cause	database objects
Network Connection	10.191.208.191:50415,10.89.33.71:1522
Service Name	hrpdb.us.oracle.com
Cluster Type	5
Grammar Version	8067
Client Program	SQL Developer
Target Class	Database
Client IP	10.191.208.191
Row Count	1000

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

友好的用户界面

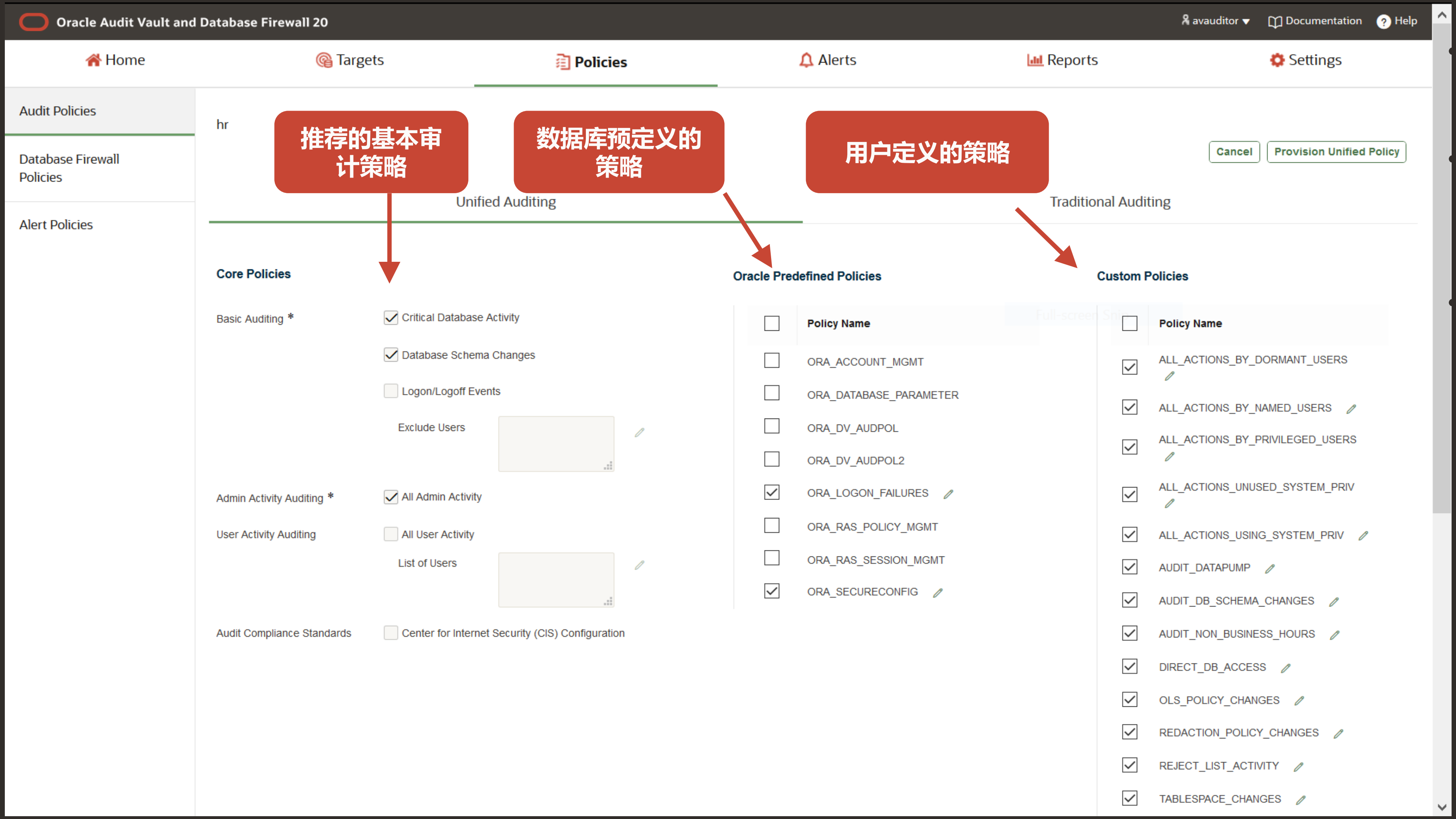
Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

审计活动仪表盘



Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

提供默认的Oracle审计策略



推荐的基本审计策略

数据库预定义的策略

用户定义的策略

hr

Unified Auditing | Traditional Auditing

Core Policies

Basic Auditing *
☑ Critical Database Activity
☑ Database Schema Changes
□ Logon/Logoff Events
Exclude Users

Admin Activity Auditing *
☑ All Admin Activity

User Activity Auditing
□ All User Activity
List of Users

Audit Compliance Standards
□ Center for Internet Security (CIS) Configuration

Oracle Predefined Policies

□	Policy Name
□	ORA_ACCOUNT_MGMT
□	ORA_DATABASE_PARAMETER
□	ORA_DV_AUDPOL
□	ORA_DV_AUDPOL2
☑	ORA_LOGON_FAILURES
□	ORA_RAS_POLICY_MGMT
□	ORA_RAS_SESSION_MGMT
☑	ORA_SECURECONFIG

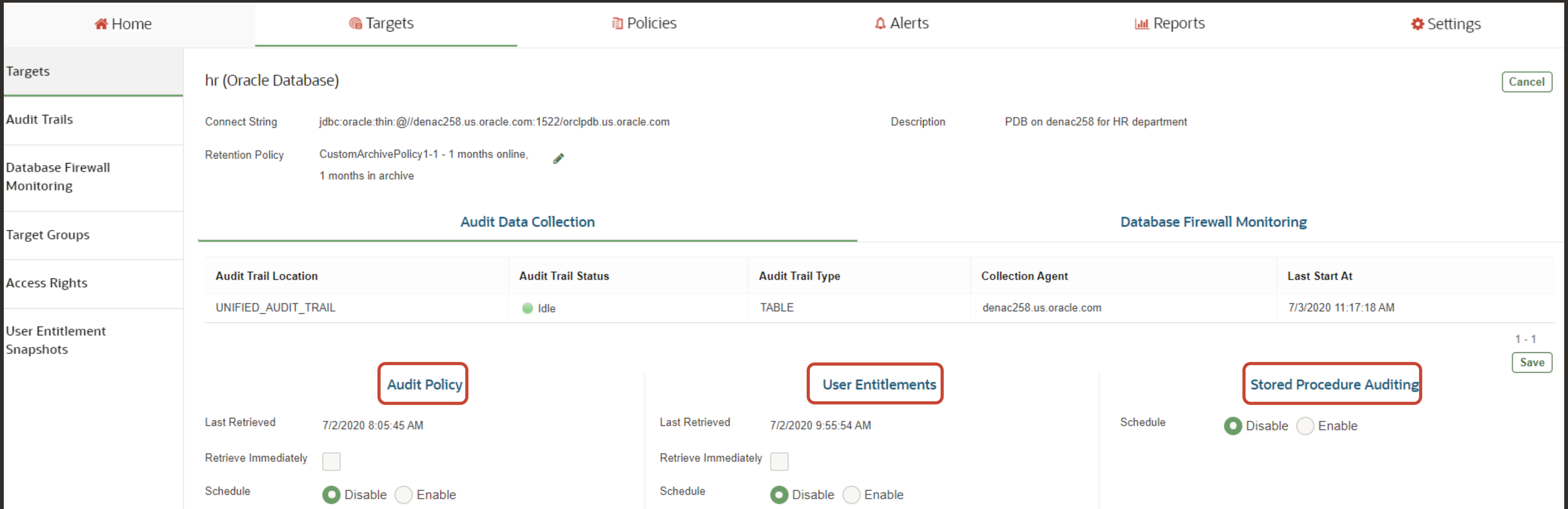
Custom Policies

□	Policy Name
☑	ALL_ACTIONS_BY_DORMANT_USERS
☑	ALL_ACTIONS_BY_NAMED_USERS
☑	ALL_ACTIONS_BY_PRIVILEGED_USERS
☑	ALL_ACTIONS_UNUSED_SYSTEM_PRIV
☑	ALL_ACTIONS_USING_SYSTEM_PRIV
☑	AUDIT_DATAPUMP
☑	AUDIT_DB_SCHEMA_CHANGES
☑	AUDIT_NON_BUSINESS_HOURS
☑	DIRECT_DB_ACCESS
☑	OLS_POLICY_CHANGES
☑	REDACTION_POLICY_CHANGES
☑	REJECT_LIST_ACTIVITY
☑	TABLESPACE_CHANGES

- 预先创建的推荐策略
- 显示和启用用户创建的统一审计策略
- 轻松一键启用
- 基于数据库用户或角色策略的细粒度支持

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

审计和权限数据收集



hr (Oracle Database)

Connect String: jdbc:oracle:thin:@//denac258.us.oracle.com:1522/orclpdb.us.oracle.com

Description: PDB on denac258 for HR department

Retention Policy: CustomArchivePolicy1-1 - 1 months online, 1 months in archive

Audit Data Collection | Database Firewall Monitoring

Audit Trail Location	Audit Trail Status	Audit Trail Type	Collection Agent	Last Start At
UNIFIED_AUDIT_TRAIL	● Idle	TABLE	denac258.us.oracle.com	7/3/2020 11:17:18 AM

1 - 1

Audit Policy

Last Retrieved: 7/2/2020 8:05:45 AM

Retrieve Immediately □

Schedule ● Disable ○ Enable

User Entitlements

Last Retrieved: 7/2/2020 9:55:54 AM

Retrieve Immediately □

Schedule ● Disable ○ Enable

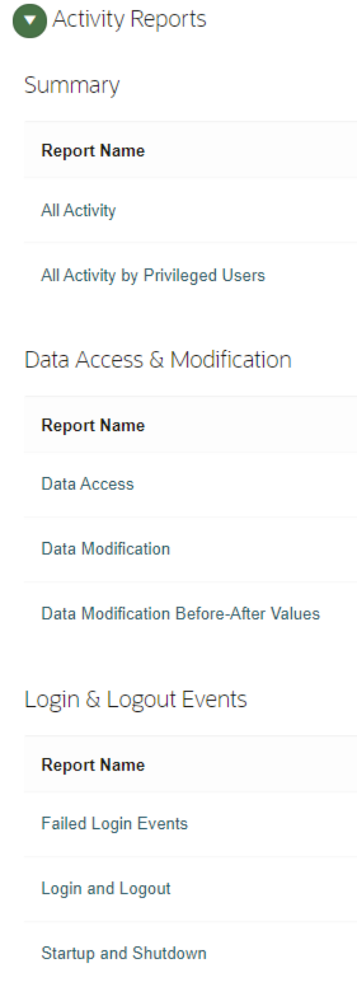
Stored Procedure Auditing

Schedule ● Disable ○ Enable

- 审计策略
- 用户权限
- 存储过程的变更

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

丰富的开箱即用的分析报告



Activity Reports

Summary

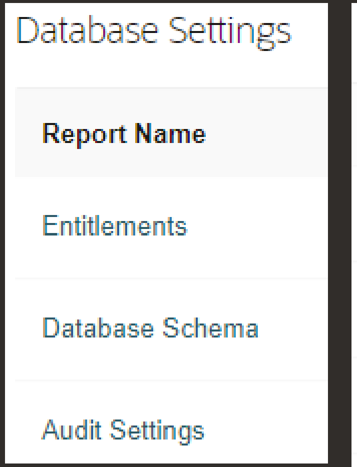
Report Name
All Activity
All Activity by Privileged Users

Data Access & Modification

Report Name
Data Access
Data Modification
Data Modification Before-After Values

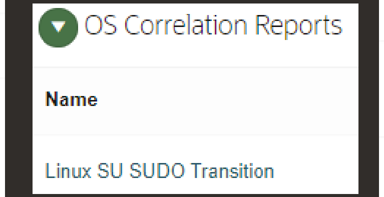
Login & Logout Events

Report Name
Failed Login Events
Login and Logout
Startup and Shutdown



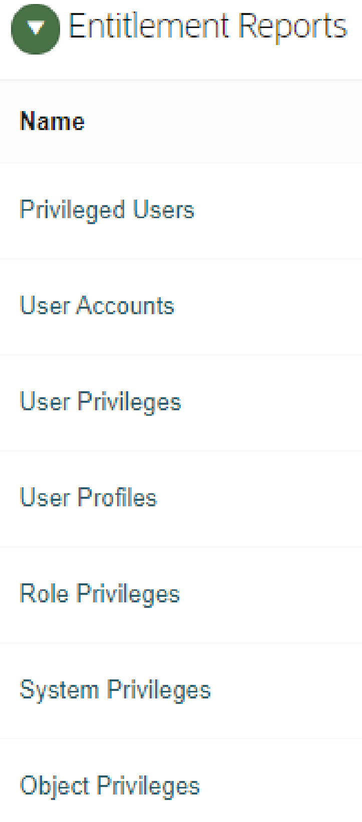
Database Settings

Report Name
Entitlements
Database Schema
Audit Settings



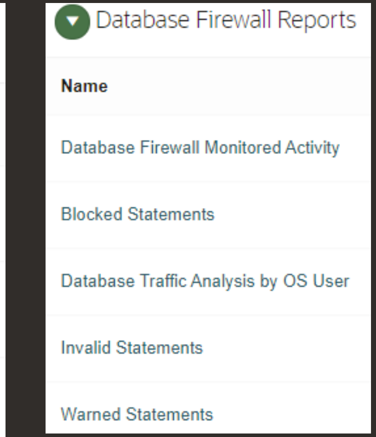
OS Correlation Reports

Name
Linux SU SUDO Transition



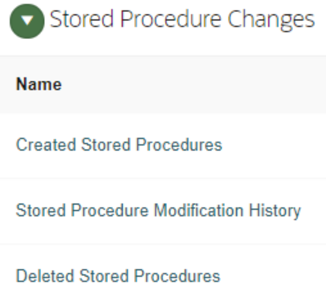
Entitlement Reports

Name
Privileged Users
User Accounts
User Privileges
User Profiles
Role Privileges
System Privileges
Object Privileges



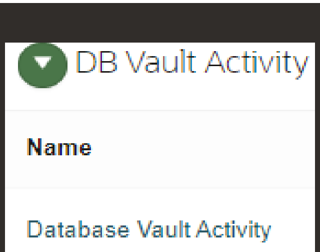
Database Firewall Reports

Name
Database Firewall Monitored Activity
Blocked Statements
Database Traffic Analysis by OS User
Invalid Statements
Warned Statements



Stored Procedure Changes

Name
Created Stored Procedures
Stored Procedure Modification History
Deleted Stored Procedures



DB Vault Activity

Name
Database Vault Activity

在AVDF 12.2中

- 来自审计跟踪和防火墙的合并数据
- 可定制
- 可以安排和通过电子邮件发送
- 开放模式允许使用第三方工具进行分析

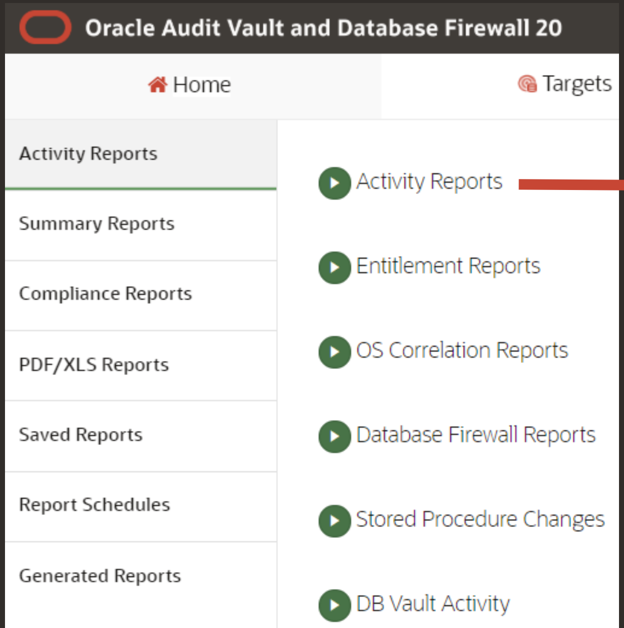
在AVDF 20中

- 报告分类

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

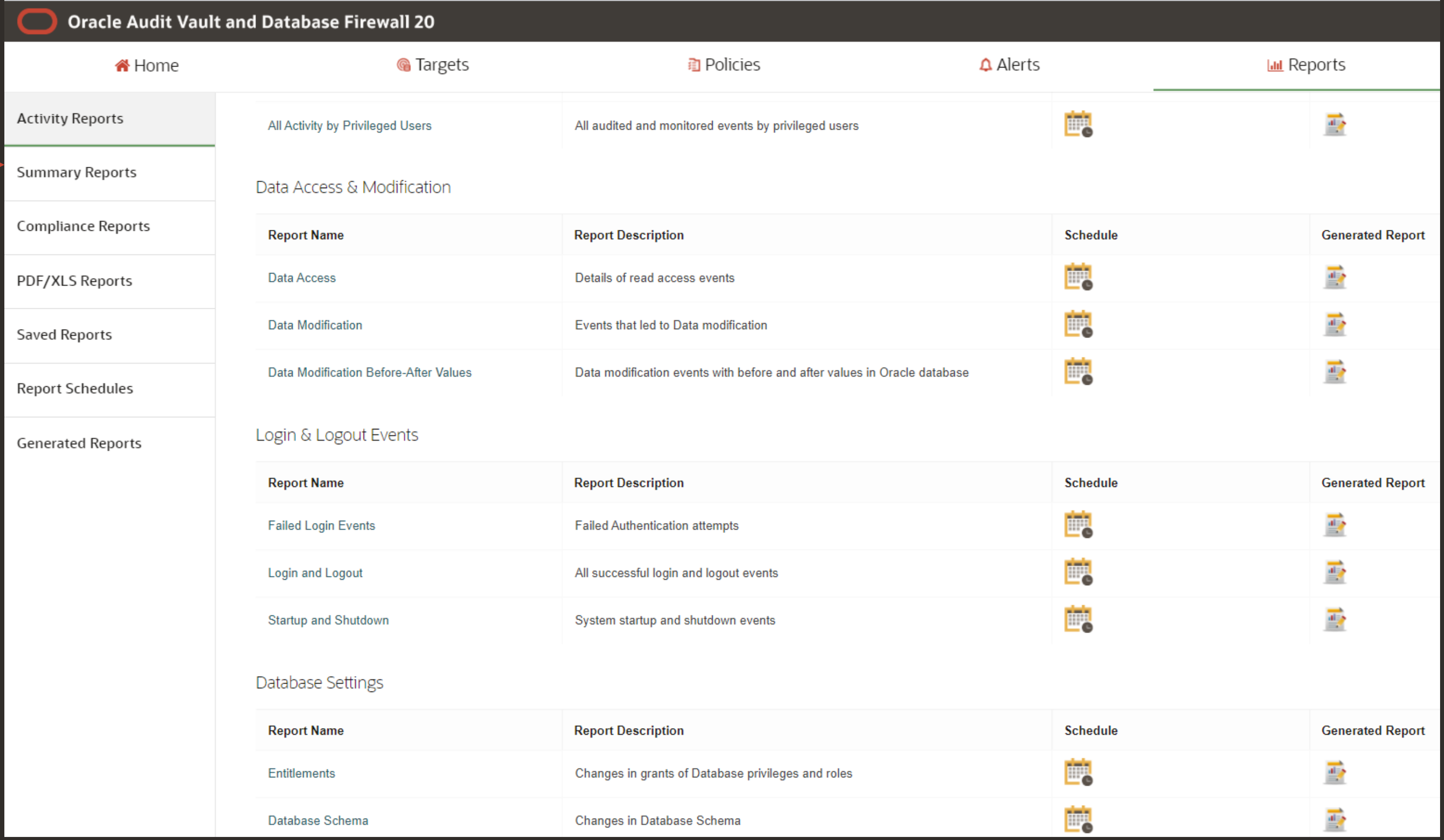
行为活动报告

活动报告显示所有相关的数据库和防火墙活动的审计



- Activity Reports
- Summary Reports
- Compliance Reports
- PDF/XLS Reports
- Saved Reports
- Report Schedules
- Generated Reports

- Activity Reports
- Entitlement Reports
- OS Correlation Reports
- Database Firewall Reports
- Stored Procedure Changes
- DB Vault Activity



- Activity Reports
- Summary Reports
- Compliance Reports
- PDF/XLS Reports
- Saved Reports
- Report Schedules
- Generated Reports

All Activity by Privileged Users	All audited and monitored events by privileged users	📅	📊

Data Access & Modification

Report Name	Report Description	Schedule	Generated Report
Data Access	Details of read access events	📅	📊
Data Modification	Events that led to Data modification	📅	📊
Data Modification Before-After Values	Data modification events with before and after values in Oracle database	📅	📊

Login & Logout Events

Report Name	Report Description	Schedule	Generated Report
Failed Login Events	Failed Authentication attempts	📅	📊
Login and Logout	All successful login and logout events	📅	📊
Startup and Shutdown	System startup and shutdown events	📅	📊

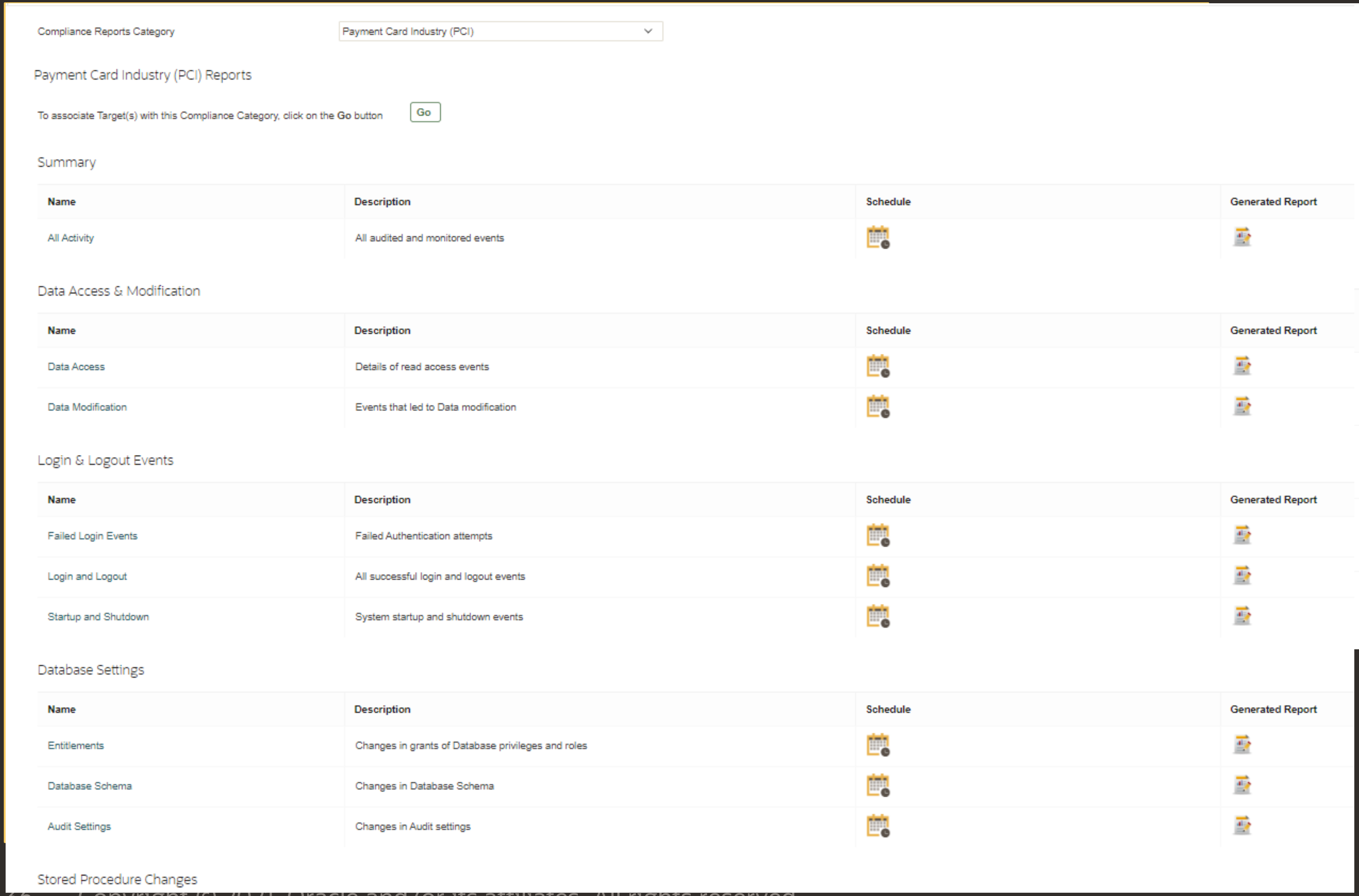
Database Settings

Report Name	Report Description	Schedule	Generated Report
Entitlements	Changes in grants of Database privileges and roles	📅	📊
Database Schema	Changes in Database Schema	📅	📊

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

简化的合规报告

合规报告: GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, UK DPA



Compliance Reports Category: Payment Card Industry (PCI)

Payment Card Industry (PCI) Reports

To associate Target(s) with this Compliance Category, click on the **Go** button [Go]

Summary

Name	Description	Schedule	Generated Report
All Activity	All audited and monitored events	📅	📝

Data Access & Modification

Name	Description	Schedule	Generated Report
Data Access	Details of read access events	📅	📝
Data Modification	Events that led to Data modification	📅	📝

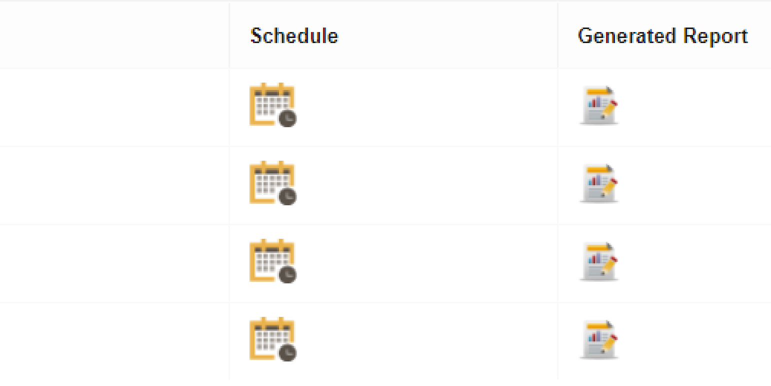
Login & Logout Events

Name	Description	Schedule	Generated Report
Failed Login Events	Failed Authentication attempts	📅	📝
Login and Logout	All successful login and logout events	📅	📝
Startup and Shutdown	System startup and shutdown events	📅	📝

Database Settings

Name	Description	Schedule	Generated Report
Entitlements	Changes in grants of Database privileges and roles	📅	📝
Database Schema	Changes in Database Schema	📅	📝
Audit Settings	Changes in Audit settings	📅	📝

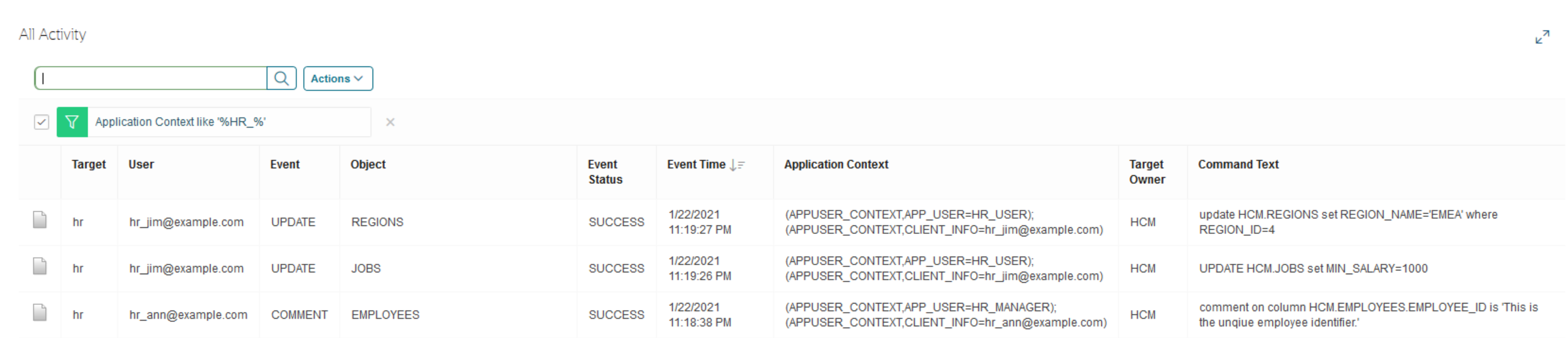
Stored Procedure Changes



Schedule	Generated Report
📅	📝
📅	📝
📅	📝
📅	📝

报告中的其他字段

- 添加应用程序属性和数据库组件作为附加字段
- 用于警报、报告和过滤
- 数据库组件 (AUDIT_TYPE) 字段可用于过滤审计数据
  - 标准, 细粒度审计, Database Vault, Label Security, Datapump, DirectPath API 等
- 应用程序内容包含应用上下文属性
  - 格式: APPLICATION_CONTEXT,CONTEXT_ATTRIBUTE=<value>
  - 逗号分隔的列表可以作为文本字段进行搜索
- 字段相关文档



	Target	User	Event	Object	Event Status	Event Time	Application Context	Target Owner	Command Text
	hr	hr_jim@example.com	UPDATE	REGIONS	SUCCESS	1/22/2021 11:19:27 PM	(APPUSER_CONTEXT,APP_USER=HR_USER); (APPUSER_CONTEXT,CLIENT_INFO=hr_jim@example.com)	HCM	update HCM.REGIONS set REGION_NAME='EMEA' where REGION_ID=4
	hr	hr_jim@example.com	UPDATE	JOBS	SUCCESS	1/22/2021 11:19:26 PM	(APPUSER_CONTEXT,APP_USER=HR_USER); (APPUSER_CONTEXT,CLIENT_INFO=hr_jim@example.com)	HCM	UPDATE HCM.JOBS set MIN_SALARY=1000
	hr	hr_ann@example.com	COMMENT	EMPLOYEES	SUCCESS	1/22/2021 11:18:38 PM	(APPUSER_CONTEXT,APP_USER=HR_MANAGER); (APPUSER_CONTEXT,CLIENT_INFO=hr_ann@example.com)	HCM	comment on column HCM.EMPLOYEES.EMPLOYEE_ID is 'This is the unqiue employee identifier.'

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

改进的企业级支持

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

改进的企业级支持

在AVDF 12.2中

- 审计数据归档、与SIEM/Syslog 集成
- 支持高可用
- 统一的策略配置 - 防火墙和数据库
- 自动更新代理，更易于管理和升级

在AVDF 20中

- LDAP/目录认证
- 自动数据归档
- FIPS 140-2 兼容性
- 2 倍审计收集率
- 集群设置中代理的多个 IP 地址配置

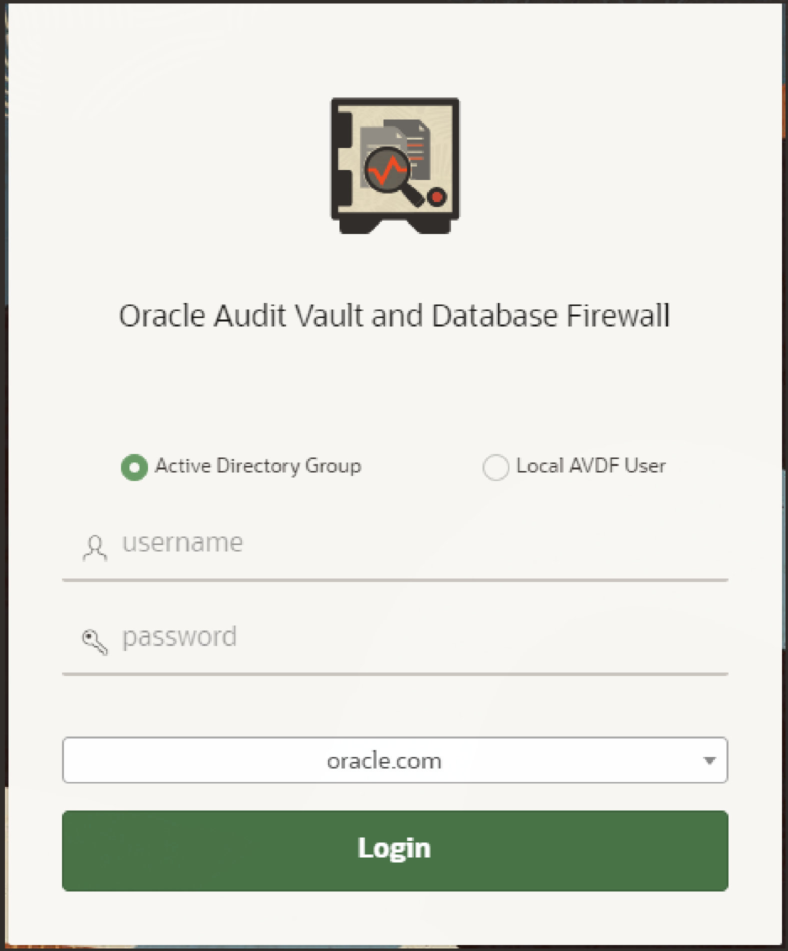
Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

Microsoft active directory / OpenLDAP 集成

支持用户认证和创建新用户

登录AVDF控制台

- 用户（管理员或审计员）可以通过选择要使用的身份验证机制来登录 AVDF
- 选项 1: 以AVDF用户进行登录
- 选项 2: 以 Active Directory 或 OpenLDAP 用户身份登录
  - 用户名, 密码
  - 提供他们所属的组（管理或审计）



Oracle Audit Vault and Database Firewall

● Active Directory Group ○ Local AVDF User

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

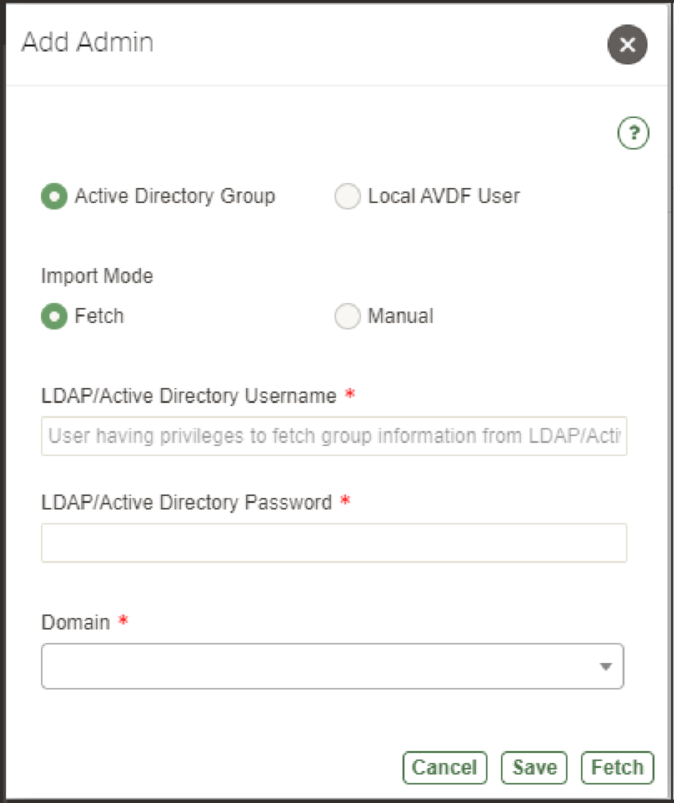
Microsoft active directory / OpenLDAP 集成

支持用户认证和创建新用户

创建新用户

- 基于现存的Active Directory/OpenLDAP 用户，创建新的AVDF用户（管理或审计）

- 选项 1: AVDF 用户:
  - 用户，密码，admin类型
- 选项 2: 现存的 AD/OpenLDAP 用户:
  - 添加AVDF用户前该用户必须存在
  - 从下拉列表中选取用户并指定用户类型 (admin, auditor etc.)



Add Admin

● Active Directory Group ○ Local AVDF User

Import Mode

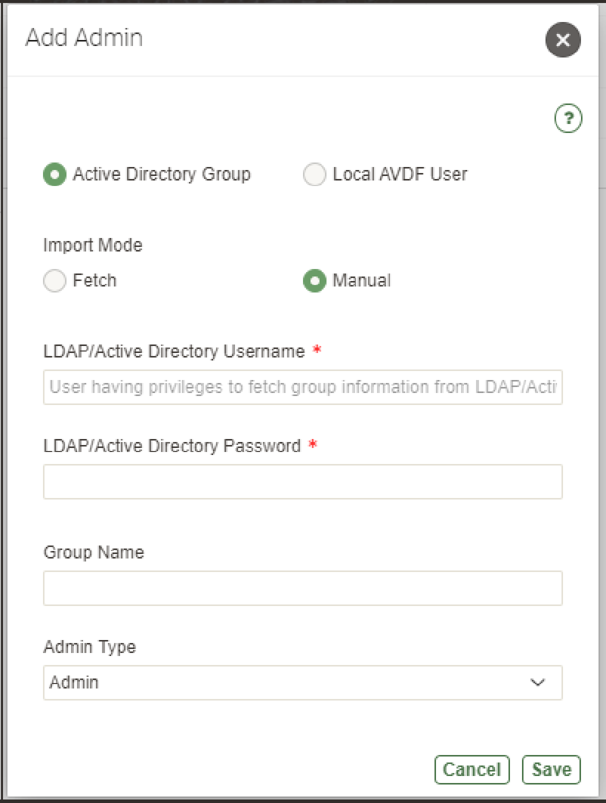
● Fetch ○ Manual

LDAP/Active Directory Username *

User having privileges to fetch group information from LDAP/Acti

LDAP/Active Directory Password *

Domain *



Add Admin

● Active Directory Group ○ Local AVDF User

Import Mode

○ Fetch ● Manual

LDAP/Active Directory Username *

User having privileges to fetch group information from LDAP/Acti

LDAP/Active Directory Password *

Group Name

Admin Type

Admin

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

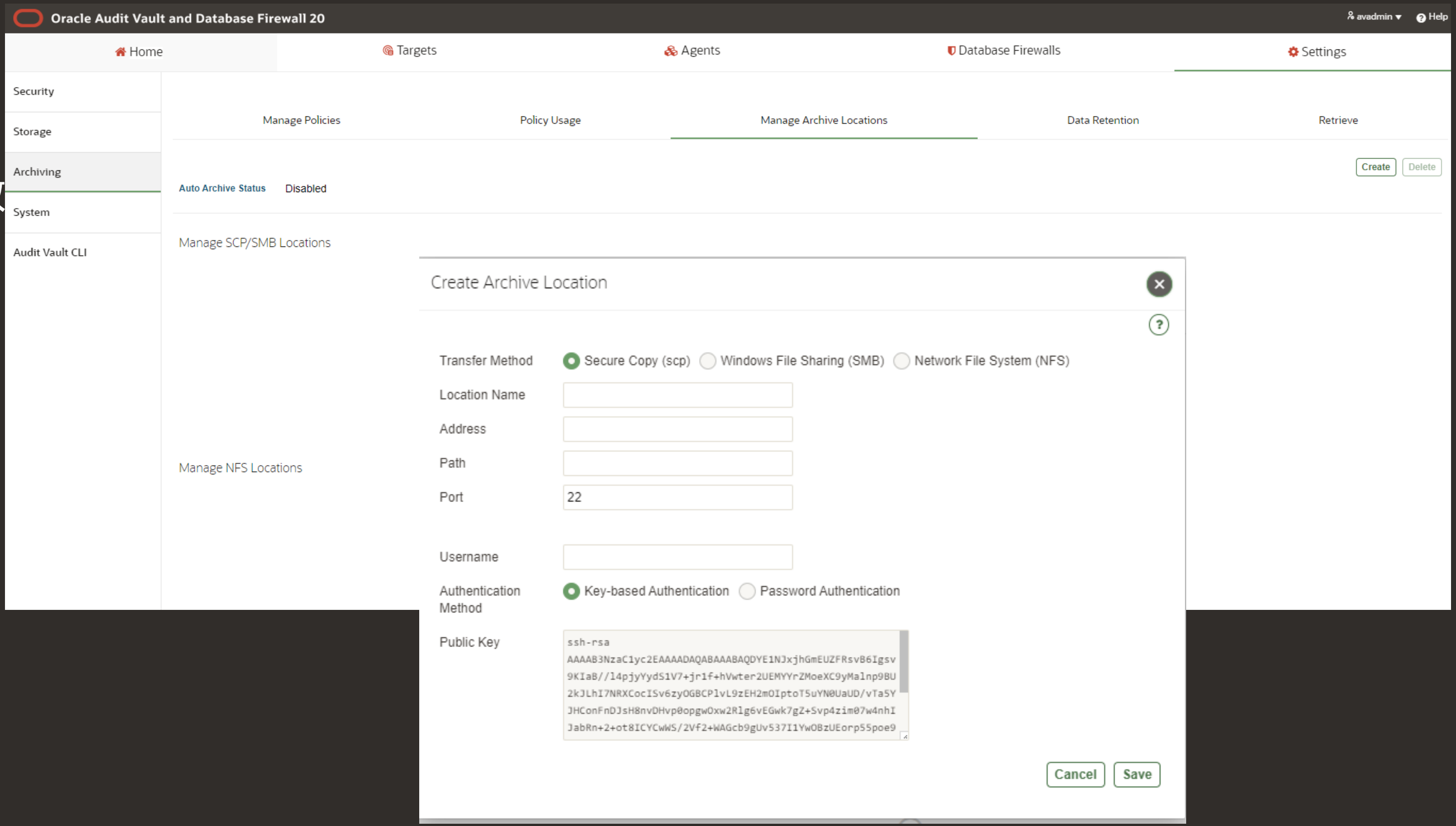
审计数据生命周期管理

在AVDF 12.2中

- 可以创建每个数据库的归档策略
  - 指定在线时间（月），存档
- 可以通过指定起始日期来恢复存档数
- 支持安全复制、windows文件共享、络文件系统
  - 手动归档

在AVDF 20中: 自动归档

- 夜间作业任务将数据移至存档



Auto Archive Status Disabled

Create Archive Location

Transfer Method ● Secure Copy (scp) ○ Windows File Sharing (SMB) ○ Network File System (NFS)

Location Name

Address

Path

Port 22

Username

Authentication Method ● Key-based Authentication ○ Password Authentication

Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDYE1NJxjhGmEUZFRsvB6Igsv
9KIaB//l4pjyYydS1V7+jr1f+hVwter2UEMYYrZMoeXC9yMalnp9BU
2kJLhI7NRXCocISv6zyOGBCPlvL9zEH2mOIptoT5uYN0UaUD/vTa5Y
JHConFnDJsH8nvDHvp0opgwOxw2Rlg6vEGwk7gZ+Svp4zim07w4nhI
JabRn+2+ot8ICYCwWS/2Vf2+WAGcb9gUv537I1YwOBzUEorp55poe9
```

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

高可用

审计服务器和数据库防火墙都支持高可用

- 审计和配置数据可以复制到备用审计服务器
- 发生故障时，可以主备切换

数据库防火墙高可用

- 在旁路和主机监控模式下，主和备防火墙都可以接收到相同的数据流量
  - 审计服务器会将相同的配置同步到两个数据库防火墙
- 在代理模式下，只有一个数据库防火墙处于激活状态

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

总结

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

总结

在AVDF 12.2中

- 数据库审计收集和SQL流量监控
  - 使用可扩展的收集器框架收集异构数据库和操作系统的审计信息
  - 数据库防火墙可监控和阻止可疑 SQL 并防止 SQL 注入
- 可过滤报告和警告以支持举证分析
- 企业级部署，例如 HA、ILM、SIEM/Syslog 集成和 LDAP 身份验证
- 支持的异构目标类型 - Oracle 和非 Oracle 数据库、操作系统日志、目录服务、文件系统

AVDF 20新特点

- 扩展审计收集范围
  - PostgreSQL、REST、JSON、CSV、Quick JSON、MongoDB（通过配置 Quick JSON）、数据变更前后值（before/after value）
- 简化的数据库防火墙
  - 简化的配置、SQL集群、RAC 支持、NIC 绑定、使用 SQL SELECT 操作对敏感表进行渗漏尝试的监视和警报
- 友好的用户界面
  - 简化的导航、预设定的审计策略
- 改进的企业级支持
  - LDAP/active directory、自动归档、FIPS 140-2

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

其他资源

- AVDF 20 Blog
- Auditing Best Practices
- Upgrade Steps
- Software Download: Oracle Software Delivery Cloud
- AVDF 20 Documentation
- Cookbook to try AVDF 20 features
- Oracle Technical Resource Site

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

谢谢

Copyright © 2021, Oracle and/or its affiliates