ORACLE

AUDIT VAULT
AND
DATABASE FIREWALL

Oracle Audit Vault and Database Firewall

Technical White Paper

ORACLE WHITE PAPER | MARCH 2018

Table of Contents

Introduction

Cyber threats, privacy laws and well-known regulations such as Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standard (PCI-DSS) have resulted in information protection becoming a top-level issue for the enterprise. As countries and industries are adopting new regulations, data protection has become a necessity. For example, the European Union's General Data Protection Regulation (GDPR), which was introduced to strengthen and unify data protection for all individuals within the EU, demands strict data protection compliance.

Various studies and surveys conducted by government and academic institutions conclude that a sizeable percentage of data breaches are perpetrated using SQL injection, stolen credentials or by insiders legitimately authorized access to the system and, by default, its data. Securing data on servers requires a defense-in-depth approach involving both technical and administrative functions that span preventive, detective, and administrative controls.

The principle of trust-but-verify not only applies to privileged users who have direct access to the host and database but also to applications accessing the database. Most applications today operate as highly trusted users, using a single privileged user account for communicating with the database, whether the database is Oracle or non-Oracle. This application architecture, combined with the increasing number of attacks on databases via SQL injection or privileged user accounts, makes deploying detective controls a crucial part of the overall defense-in-depth security strategy. New regulations such as GDPR make detective controls one of the key security requirements. GDPR not only mandates auditing of the activities on the personal data but also recommends secure and central management of these records. Auditing and monitoring are critical for detecting anomalies and also help in forensic analysis in case of a data breach.

When deploying a monitoring solution, it is important to note that the quality and accuracy of the information gathered will depend on the level of visibility the solution has into the activities of the target system. It is also important to understand the risk associated with individual systems so that you can determine the level of visibility required for activities on those systems. A good analogy to understand this concept is to consider the roles of cameras and guards at the front entrance to buildings. Both can see what is going into the building, only one can stop what goes into the building, but neither provides a complete view on what happens inside the building. If in our analogy the building were a database, the camera or guard could monitor SQL statements before they reach the database, but the challenge is in finding out what happens after the SQL executes inside the database. Recursive SQL spawned by stored procedures, dynamic SQL, privileged user operations, scheduled jobs, trigger executions, application user names, as well as "before" and "after" data values are all examples of information that is largely invisible from outside the database, but are visible to the auditing system inside the database. As a result, the value of monitoring is directly linked to the level and quality of information gathered as well as available reporting and alerting functionality.

Oracle Audit Vault and Database Firewall Overview

Oracle Audit Vault and Database Firewall provides a comprehensive and flexible solution for monitoring and protecting database systems. The Audit Vault Server component consolidates audit data from Oracle and non-Oracle databases, operating systems, directories, file systems, as well as application specific audit data. At the same time, Database Firewall acts as the database's first line of defense on the network, enforcing expected application behavior while helping prevent SQL injection, application bypass, and other malicious activities from reaching the database. Oracle Audit Vault and Database Firewall consolidates audit data from thousands of databases and monitors SQL traffic at the same time, looking for, alerting on, and preventing unauthorized or out-of-policy SQL statements. Out-of-the-box reports combined with a customizable reporting interface provide a comprehensive view of database activity across the enterprise, whether observed through the network or through the audit logs. Oracle Audit Vault and Database Firewall supports Oracle Databases, Microsoft SQL Server, IBM DB2 for Linux, Unix and Windows, SAP Sybase ASE and Oracle MySQL databases.

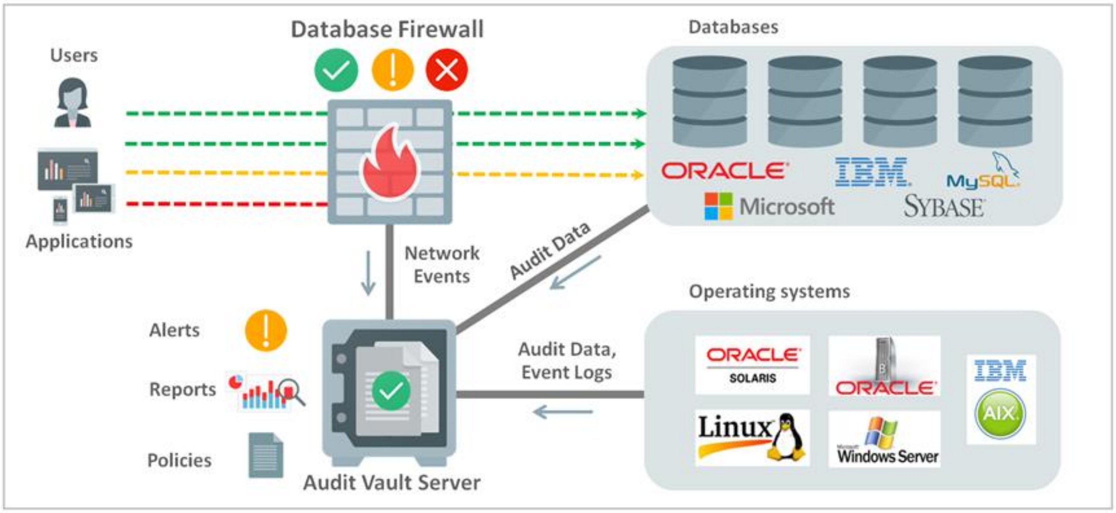
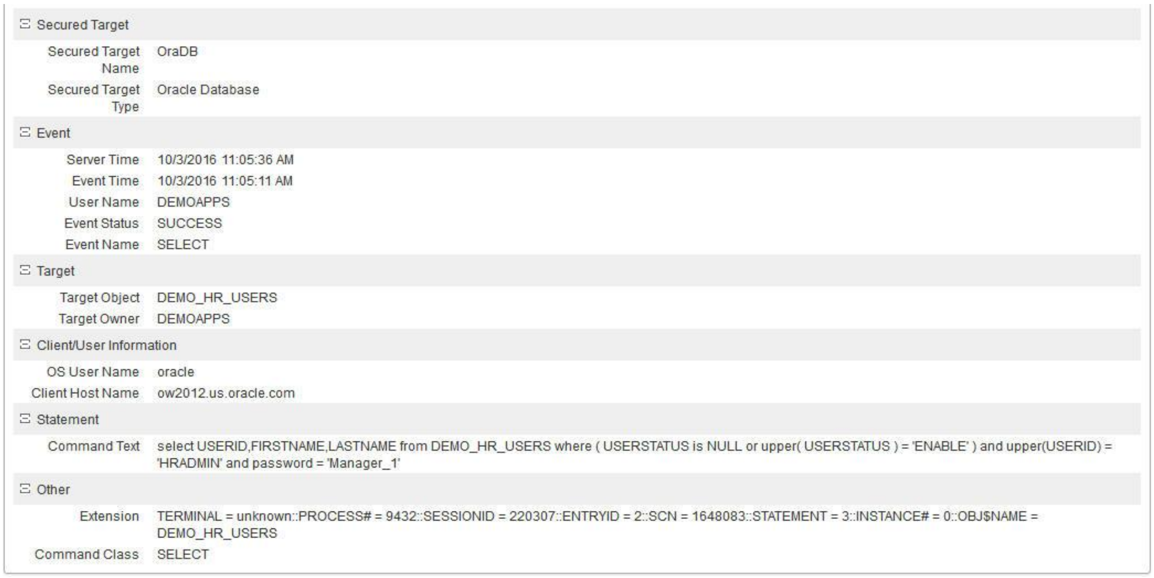


Figure 1. Oracle Audit Vault and Database Firewall

Auditing and Monitoring Overview

Auditing has become an important tool over the past 10 years for both compliance and forensic analysis of data breaches. Audit records provide an irrefutable record of actions taken whether they are generated by a database, directory, or operating system. Information such as the event type (create table, drop table, create procedure, truncate table, select, insert, update, delete) coupled with the context of the event such as the initiating IP address, event time, and actual SQL statement, are just a few examples of audit information that is commonly needed in compliance and forensic reports (see Figure 2). Oracle Audit Vault and Database Firewall can consolidate, report, and alert on audit information from databases, operating systems, file systems, and directories.



Secured Target

Secured Target Name	OraDB
Secured Target Type	Oracle Database

Event

Server Time	10/3/2016 11:05:36 AM
Event Time	10/3/2016 11:05:11 AM
User Name	DEMOAPPS
Event Status	SUCCESS
Event Name	SELECT

Target

Target Object	DEMO_HR_USERS
Target Owner	DEMOAPPS

Client/User Information

OS User Name	oracle
Client Host Name	ow2012.us.oracle.com

Statement

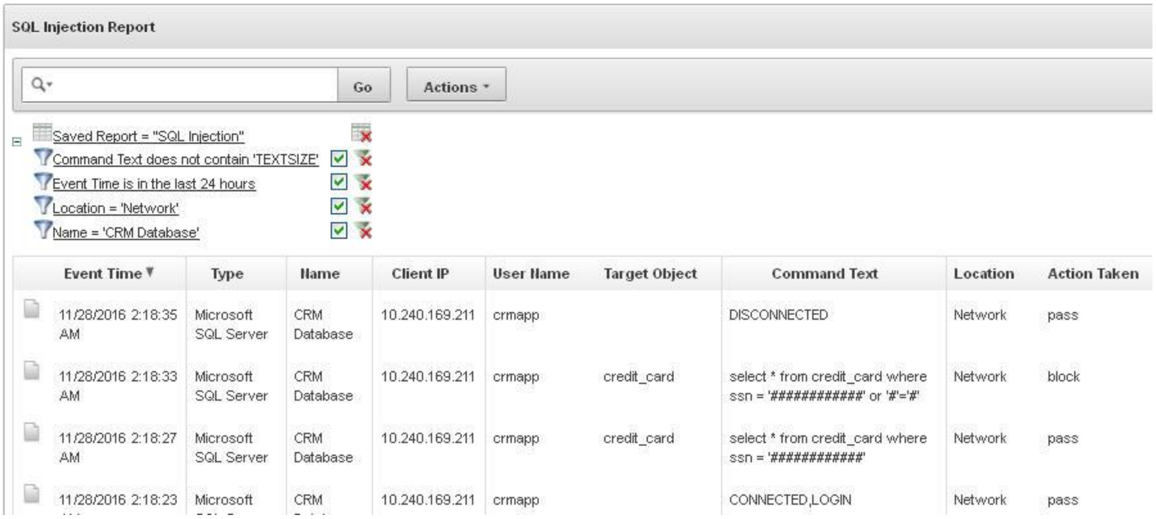
Command Text	select USERID,FIRSTNAME,LASTNAME from DEMO_HR_USERS where (USERSTATUS is NULL or upper(USERSTATUS) = 'ENABLE') and upper(USERID) = 'HRADMIN' and password = 'Manager_1'

Other

Extension	TERMINAL = unknown::PROCESS# = 9432::SESSIONID = 220307::ENTRYID = 2::SCN = 1648083::STATEMENT = 3::INSTANCE# = 0::OBJ$NAME = DEMO_HR_USERS
Command Class	SELECT

Figure 2. Sample Audit log entry managed in Oracle Audit Vault and Database Firewall

Monitoring includes the examination of the initiating events (SQL statements) that generate the audit data. Because monitoring of SQL traffic is done outside the database, Database Firewall can decide whether an event should be permitted, modified, blocked, or alerted on. Figure 3 shows an example of a report where a SQL injection attempt is blocked.



SQL Injection Report

Saved Report = "SQL Injection"

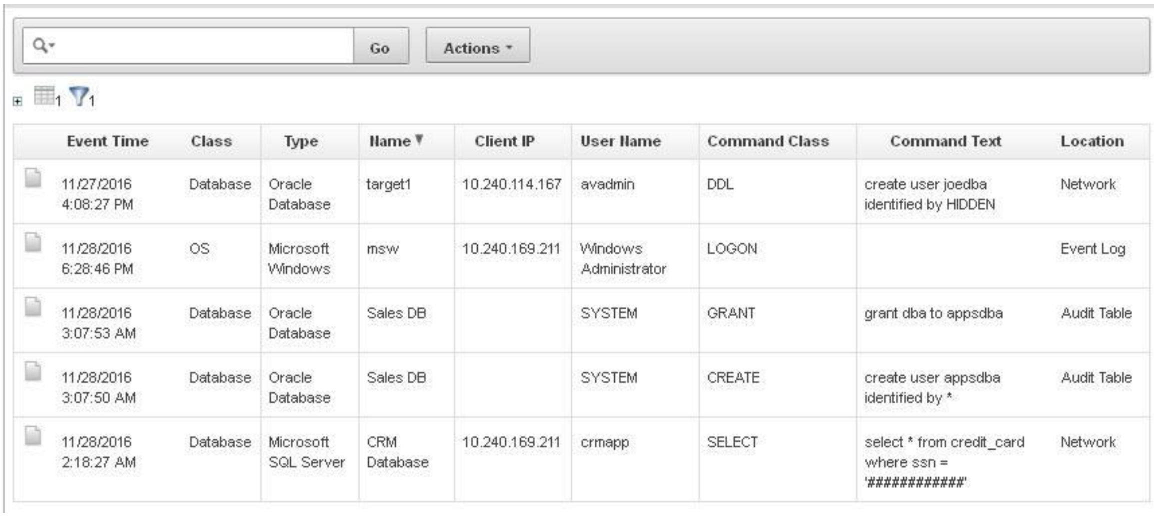
- Command Text does not contain 'TEXTSIZE' ☑
- Event Time is in the last 24 hours ☑
- Location = 'Network' ☑
- Name = 'CRM Database' ☑

Event Time	Type	Name	Client IP	User Name	Target Object	Command Text	Location	Action Taken
11/28/2016 2:18:35 AM	Microsoft SQL Server	CRM Database	10.240.169.211	crmapp		DISCONNECTED	Network	pass
11/28/2016 2:18:33 AM	Microsoft SQL Server	CRM Database	10.240.169.211	crmapp	credit_card	select * from credit_card where ssn = '############' or '#'='#'	Network	block
11/28/2016 2:18:27 AM	Microsoft SQL Server	CRM Database	10.240.169.211	crmapp	credit_card	select * from credit_card where ssn = '############'	Network	pass
11/28/2016 2:18:23	Microsoft	CRM	10.240.169.211	crmapp		CONNECTED,LOGIN	Network	pass

Figure 3. Database Firewall SQL Monitoring

Audit Vault Server

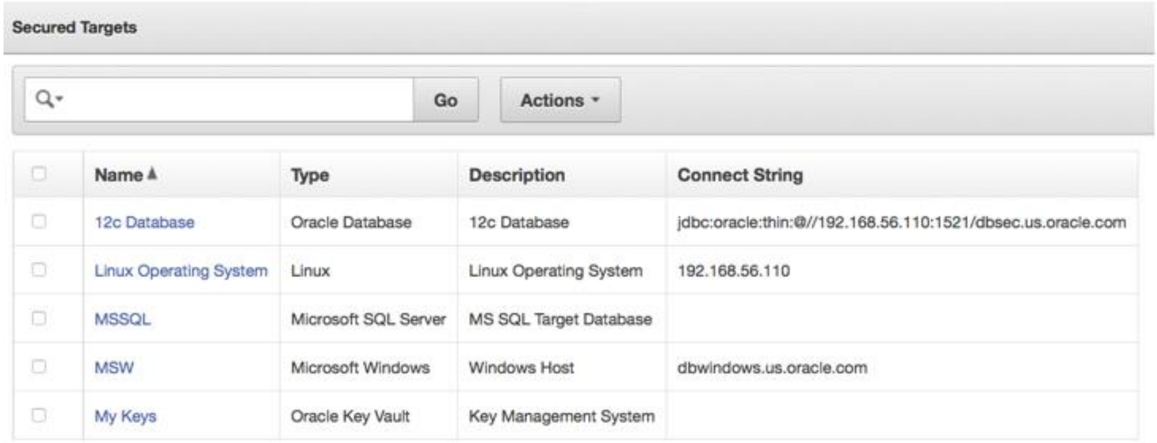
Audit Vault Server is the central, highly scalable and secure repository that stores the consolidated audit data as well as event logs generated by Database Firewall. Audit Vault Server is the central platform for data consolidation, reporting, alerting, and policy management. Using lightweight agents, the audit data is transferred from the target system, and then optionally removed from the target system. Audit Vault Server can consolidate audit information from all database sources and can be extended to custom sources, including application tables/files on Oracle and non-Oracle databases that log custom audit data. As shown in Figure 4, report data can span across multiple databases and include information from the target system and the network.



Event Time	Class	Type	Name	Client IP	User Name	Command Class	Command Text	Location
11/27/2016 4:08:27 PM	Database	Oracle Database	target1	10.240.114.167	avadmin	DDL	create user joedba identified by HIDDEN	Network
11/28/2016 6:28:46 PM	OS	Microsoft Windows	msw	10.240.169.211	Windows Administrator	LOGON		Event Log
11/28/2016 3:07:53 AM	Database	Oracle Database	Sales DB		SYSTEM	GRANT	grant dba to appsdba	Audit Table
11/28/2016 3:07:50 AM	Database	Oracle Database	Sales DB		SYSTEM	CREATE	create user appsdba identified by *	Audit Table
11/28/2016 2:18:27 AM	Database	Microsoft SQL Server	CRM Database	10.240.169.211	crmapp	SELECT	select * from credit_card where ssn = '############'	Network

Figure 4. Consolidated reporting from network, database audit and OS Event Logs

Secured targets from which audit data will be collected are configured using the Audit Vault Server console (Figure 5). The console is also used to manage the Database Firewall policies, customize audit policies, schedule and customize the reports, set up the report attestation, and configure the alerts.



Secured Targets

□	Name	Type	Description	Connect String
□	12c Database	Oracle Database	12c Database	jdbc:oracle:thin:@//192.168.56.110:1521/dbsec.us.oracle.com
□	Linux Operating System	Linux	Linux Operating System	192.168.56.110
□	MSSQL	Microsoft SQL Server	MS SQL Target Database	
□	MSW	Microsoft Windows	Windows Host	dbwindows.us.oracle.com
□	My Keys	Oracle Key Vault	Key Management System	

Figure 5. Audit Vault console showing secured targets

Database Firewall

Database Firewall is the network monitoring component outside the database that monitors the inbound SQL traffic and serves as the first line of defense against SQL injection threats and other unauthorized SQL statements. Database Firewall monitors data access, enforces access policies, highlights anomalies and helps protect against network-based attacks originating from outside or inside the organization. Unlike traditional SQL firewalls that rely on identifying out-of-policy SQL using regular expressions, Database Firewall enforces policies using a sophisticated grammar analysis engine that delivers the required scalability, accuracy, and management simplicity.

Organizations can choose to deploy Database Firewall in active monitoring mode to protect their database assets or in passive monitoring mode to alert security operations personnel of unexpected activity, and/or supplemental auditing to address compliance requirements. In passive monitoring mode, Database Firewall observes database traffic and analyzes SQL interactions. Information from Database Firewall is logged to Audit Vault Server, enabling reports to span information observed on the network alongside audit information from the database, operating systems, and directories.

In active monitoring mode, Database Firewall transparently intercepts SQL traffic coming from database clients acting as an application layer firewall, analyzes the security of the SQL payload in TCP packets before forwarding it on to the database. Attacks including SQL injection can be blocked by comparing incoming SQL against the approved white list of application SQL. Support for white list, black list, and exception list based policies, provides a high degree of deployment flexibility.

White List Policy Enforcement

The white list policy enforces security using a set of approved SQL statements along with the conditions under which they were executed including the username, IP address, time of day, and program name. Database Firewall compares SQL traffic with the approved white list and then based upon the policy, it chooses to alert, substitute, or block the SQL statement. The approved SQL or white list is learned over time by monitoring database traffic. The monitoring period needed to establish the white list varies depending on the application and business cycle.

Black List Policy Enforcement

In addition to the white list based positive security enforcement model, Database Firewall also supports a black list model that blocks specific SQL statements. As with white list policies, black list policies can evaluate various factors such as username, IP address, time of day and program, before making the decision.

Exception List Policy Enforcement

Exception list policies override white list and black list policies by allowing custom bypass policies to be created for specific activities. For example, exception list policies could be used to enable a specific remote administrator coming from a predetermined IP address to diagnose a particular application performance issue without being bound by the white list or the blacklist.

Handling Unauthorized SQL

Database Firewall monitors SQL traffic to database secured targets, creates traffic logs for analysis and reporting, and takes action according to the firewall policy. When Database Firewall finds an unauthorized SQL statement, it handles it in one (or a combination) of the following ways based on the policy:

- Alert on the out-of-policy SQL statement
- Block the SQL statement and take one of the following actions:

- Do nothing after blocking the statement. The actual end-user experience would depend upon how application handles this case where the server does not respond.
- Substitute the out-of-policy statement with a new harmless statement that does not return any data or returns an error (as shown in Table 1 below). This gives the best end user experience and ensures that applications can keep running.
- Drop the connection to the client. This blocks all traffic from that specific connection to the database. This is the most aggressive action, and if the application is using connection pooling, this will impact all the users using the pool.

ORIGINAL STATEMENT (FRAUDULENT)	SUBSTITUTED STATEMENT	DATABASE RESPONSE (RESULT)
SELECT * FROM tbl_users;	SELECT * FROM tbl_users WHERE 'a' = 'b';	No record found
DROP TABLE tbl_accounts;	SELECT * FROM aaabbbccc;	Error. Table not known
UPDATE tbl_accounts SET accounts = '123' WHERE user = 'Fred';	SELECT DUAL SET 'Fred';	Error. Incorrect Syntax.

Table 1. Oracle Audit Vault and Database Firewall SQL statement substitution examples

Reports

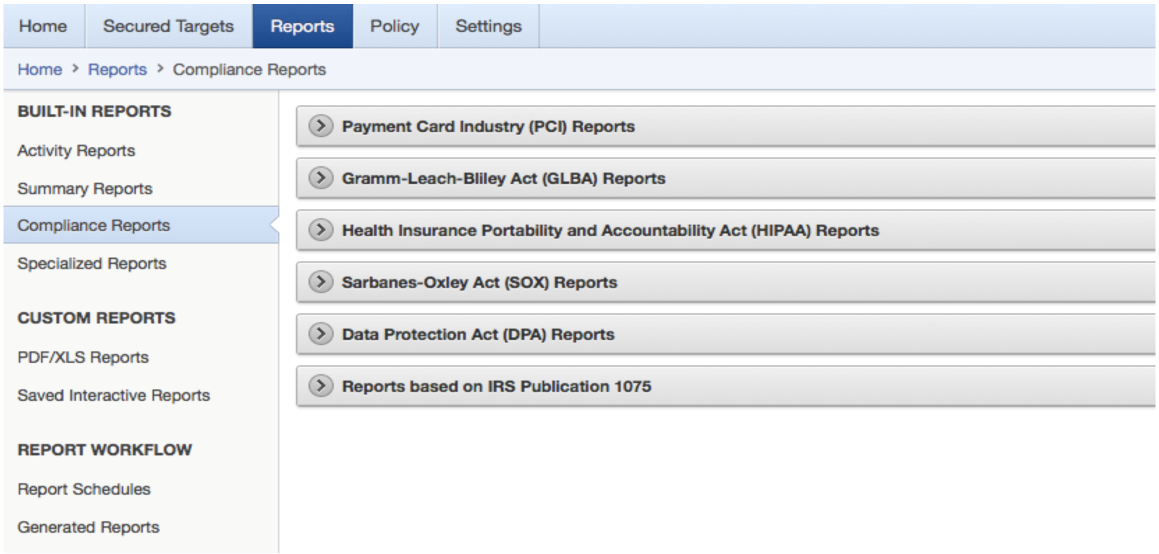
Oracle Audit Vault and Database Firewall reports can be used to monitor a wide range of activities including privileged user activity on the database server, changes to database structures, and inbound SQL statements on the network. Reports can be based on consolidated audit information from databases, operating systems, and directories, providing a holistic picture of activities across the enterprise. In addition, reports can include information on database account management, roles and privileges, object management, and stored procedure changes.

Auditors access reports interactively through a web interface, or through PDF or XLS report files. The console’s easy-to-use interactive browsing is built on Oracle Application Express technology and provides the ability to create color-coded charts and graphs. Report columns can be sorted, filtered, re-ordered, added, or removed. Rules can automatically highlight specific rows so that users can quickly spot suspicious or unauthorized activity. PDF and XLS report definitions can be used to schedule automatic generation of reports, which can be delivered via e-mail attachments or URLs. Reports can also be defined to require attestation by multiple auditors. Users can use Oracle BI Publisher to create new or customize PDF and XLS report templates to meet specific compliance and security requirements.

Audit Vault Server provides optimal performance by expediting report generation with the help of Oracle Database In-Memory feature. Audit Vault Server stores audit data in memory based on the selected date range, enabling reports to run faster. Furthermore, the Audit Vault Server repository schema is documented, enabling integration with third-party reporting solutions.

Compliance Reports

Standard out-of-the-box audit assessment reports are categorized to help meet standard regulations such as Payment Card Industry Data Security Standard (PCI-DSS), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and European Union Data Protection Act (DPA).

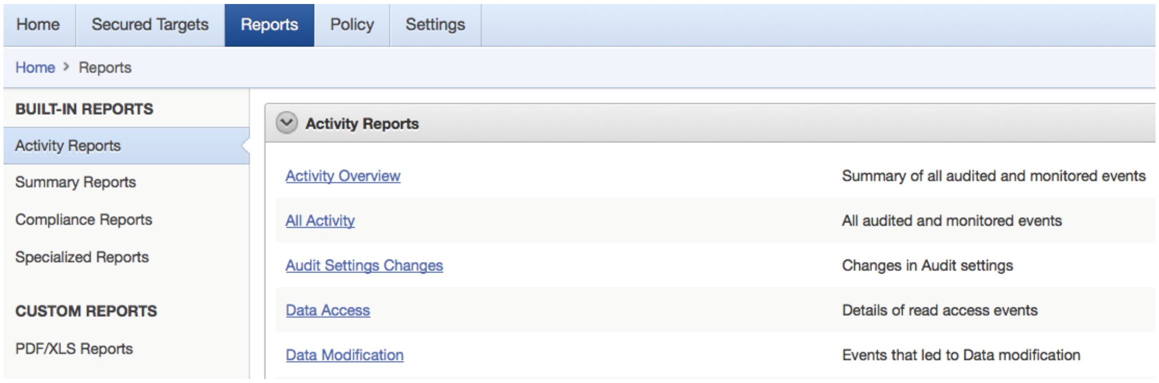


- Payment Card Industry (PCI) Reports
- Gramm-Leach-Bliley Act (GLBA) Reports
- Health Insurance Portability and Accountability Act (HIPAA) Reports
- Sarbanes-Oxley Act (SOX) Reports
- Data Protection Act (DPA) Reports
- Reports based on IRS Publication 1075

Figure 6. Oracle Audit Vault and Database Firewall Built-in Compliance Reports

Activity Reports

Activity Reports cover topics such as failed logins, changes to application tables, database schema changes, or user entitlements (see Figure 7). For example, if you want to audit each time a user performs data definition language (DDL) SQL statement such as DROP or ALTER, the pre-built “Database Schema Changes Report” highlights rows of that particular user and drills down to individual event details. You can also get an overview of all audit events which can be filtered by target system, user, operation, time, and so on.



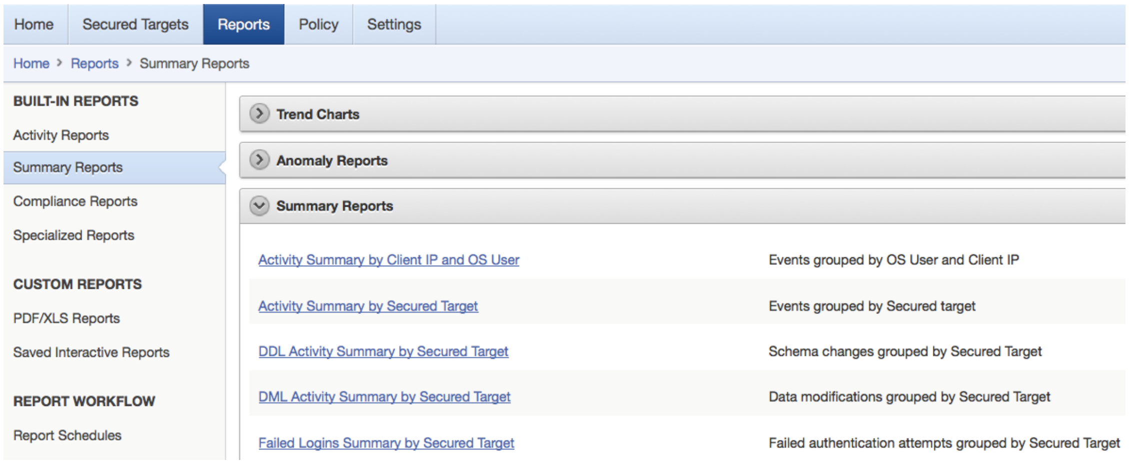
Activity Reports

Activity Overview	Summary of all audited and monitored events
All Activity	All audited and monitored events
Audit Settings Changes	Changes in Audit settings
Data Access	Details of read access events
Data Modification	Events that led to Data modification

Figure 7. Oracle Audit Vault and Database Firewall Built-in Activity Reports

Summary Reports

This report group contains summary reports, trend charts and anomaly reports (Figure 8). These reports can be used as an analytical tool to quickly review characteristics of user activity on specific secured targets or across the entire deployment environment. Summary reports focus on statistics of occurrence of various types of events, generated by individual users or initiated from specific client IP addresses. Trend charts graphically present general event trends and also trends based on specific user, client IP and secured target. Anomaly reports highlight new and dormant user and client IP anomalies.



Activity Summary by Client IP and OS User	Events grouped by OS User and Client IP
Activity Summary by Secured Target	Events grouped by Secured target
DDL Activity Summary by Secured Target	Schema changes grouped by Secured Target
DML Activity Summary by Secured Target	Data modifications grouped by Secured Target
Failed Logins Summary by Secured Target	Failed authentication attempts grouped by Secured Target

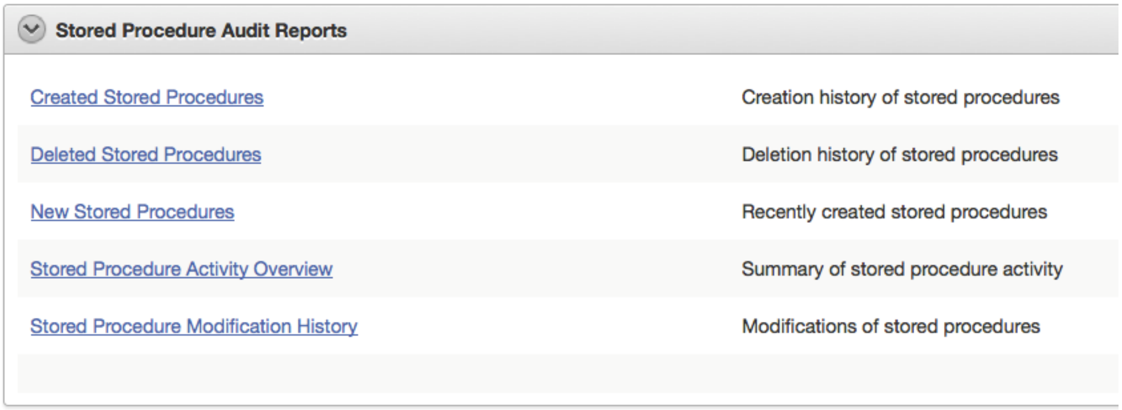
Figure 8. Oracle Audit Vault and Database Firewall Built-in Summary Reports

Entitlement Reports

Entitlement reports describe the types of access that users have to an Oracle database, providing information about the users, roles, profiles, and privileges used. These reports are useful for tracking unnecessary access to data, finding duplicate privileges, and simplifying privilege grants. After you generate an entitlement snapshot, you can compare different snapshots to find how the entitlement information has changed over time. This is particularly useful for identifying any drift from an approved database entitlement baseline.

Stored Procedure Audit Reports

For many organizations, stored procedures form the bulk of the application logic for many applications and may contain flaws that can be exploited for malicious attacks including SQL injection. DBAs often write stored procedures to automate the jobs or to improve security. It is important that these stored procedures once defined are not tampered with. Oracle Audit Vault and Database Firewall enables you to monitor any changes made to the stored procedures on secured target databases. It connects to the secured target databases at scheduled intervals and discovers any changes or additions that have been made to stored procedures. Stored Procedure Auditing report shows all stored procedure operations, deleted and created procedures, as well as modification history.

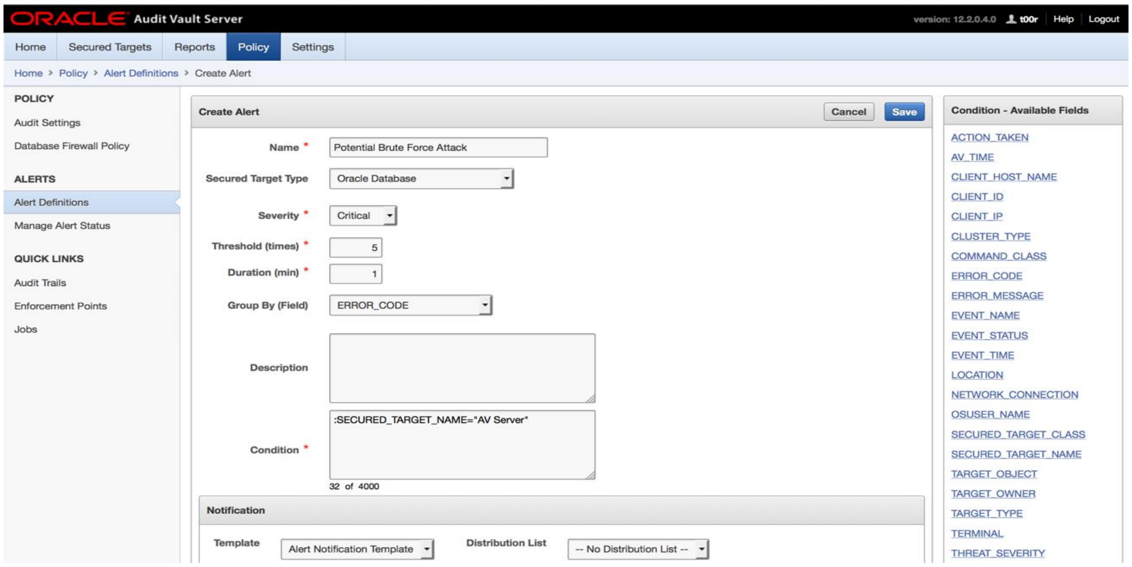


Created Stored Procedures	Creation history of stored procedures
Deleted Stored Procedures	Deletion history of stored procedures
New Stored Procedures	Recently created stored procedures
Stored Procedure Activity Overview	Summary of stored procedure activity
Stored Procedure Modification History	Modifications of stored procedures

Figure 9. Oracle Audit Vault and Database Firewall Stored Procedure Audit Reports

Alerts and Notifications

Oracle Audit Vault and Database Firewall provides the ability to detect and alert on activities that may indicate attempts to gain unauthorized access and/or abuse system privileges. It lets you define rule-based alerts on audit records, whether these records come from Audit Vault Agent or Database Firewall. Database Firewall policies can be configured to generate alerts on network activity, providing an early-warning detective control for potential malicious activity. Furthermore, Audit Vault continuously monitors the events collected, evaluating the activities against defined alert conditions. Alerts can be associated with any database event including system events such as changes to application tables, creating privileged users, or events when someone attempts to access sensitive business information and is blocked by an Oracle Database Vault policy. As shown in Figure 9, alerts can also be configured to be threshold and time based. For example, if 5 login failures occur within a 1-minute window, possibly indicating a brute force attack, then an alert is raised.



Name *	Potential Brute Force Attack
Secured Target Type	Oracle Database
Severity *	Critical
Threshold (times) *	5
Duration (min) *	1
Group By (Field)	ERROR_CODE
Description	
Condition *	:SECURED_TARGET_NAME="AV Server" 32 of 4000

Notification

Template	Alert Notification Template
Distribution List	-- No Distribution List --

Figure 10. Oracle Audit Vault and Database Firewall alert definition

The Audit Vault Server interface provides graphical summaries of alerts. These include a summary of alert activity and top sources by number of alerts. Users can click on the summary graphs and drill down to more detailed reports. For reporting, alerts can be grouped by source, event category, and severity (warning or critical). You can also specify notifications for the generated alerts. For example, you can set up an email to be automatically sent to a user, such as a security officer, or to a distribution list. Alerts can also be forwarded to syslog. This is useful if you want to integrate them with another system.

Scalability and Security

Audit data is an important record of business activity, and it must be protected against modification to ensure the integrity of reports and investigations. Oracle Audit Vault and Database Firewall stores audit data in a secure repository built using Oracle's industry leading database technology. To prevent unauthorized access or tampering, audit and event data is encrypted at every stage, in transition and at rest. Timely transfer of audit data from source systems to Audit Vault Server is critical to close the window on intruders who may attempt to modify audit data and cover their tracks. Oracle Audit Vault and Database Firewall can be configured to transfer audit data on a near real time basis.

The repository is built on an embedded Oracle Enterprise Edition database that includes numerous Oracle technologies, including compression, partitioning, encryption, and privileged user controls. The use of compression is particularly important for optimized storage of the consolidated data. The combination of these technologies and the Oracle Enterprise Edition 12c database results in a repository with massive scalability, high availability and security.

A single Oracle Audit Vault and Database Firewall can scale to support hundreds of Audit Vault Agents and Database Firewalls, each of which can in turn host multiple audit trails and hundreds of databases correspondingly. The integrated administrator console can configure the entire system, monitor the deployment, startup/shutdown Database Firewalls and Audit Vault Agents, configure Database Firewall High Availability operation, and manage the backup and restore operations.

The Audit Vault Server interface supports two broad categories of users: Auditors and Administrators. Auditors configure auditing and monitoring policies as well as define, generate, and access audit reports and alerts. Administrators configure basic network and host settings for the secured targets, start and stop Audit Vault Agents and Database Firewalls, and configure and monitor Audit Vault Server operation. Administrators do not have access to audit information. Within the two role categories, further separation of duties can be defined. A subset of protected assets can be assigned to individual auditors and administrators, ensuring that a single repository can be deployed to support an entire enterprise spanning multiple organizations, subsidiaries, or geographic regions. Fine-grained authorizations are particularly important when information may span multiple countries with different privacy regulations and safe harbor requirements.

Flexible Deployment Options

Database Firewall Network Deployment

Database Firewall can be deployed as a transparent network bridge, simply inserted into the network in a segment that lies between database clients/application servers and the databases being protected (Figure 11). This ‘in line’ bridge architecture requires no configuration changes to database clients, applications or the database itself, and provides the flexibility for both active and passive monitoring. Database Firewall can also be deployed on a network tap or span port to enable passive monitoring of database activity.

In scenarios where it is difficult to add a network bridge, or if the database servers are in some remote locations, Database Firewall can also be configured as a proxy such that all traffic to the database server is routed through it. In this deployment mode, the database server IP address/port on the database client or application is changed to the IP address/port for the Database Firewall proxy and the database listener is configured to reject direct connections. As another option, enterprise network switches and traditional firewalls can also be configured to redirect database traffic to a Database Firewall proxy port, allowing SQL traffic to be protected without any changes to database clients or applications. A given database firewall can operate as a transparent bridge for some databases and a proxy for others.

Database Firewall supports deployment of a local server-side, monitor-only agent to ensure flexibility in the choice of the network point at which the traffic is monitored. Host Monitor, part of Audit Vault Agent, captures SQL traffic reaching the database server and securely forwards it to Database Firewall. It can be used to remotely monitor database servers running on Linux, Oracle Solaris and Windows platforms.

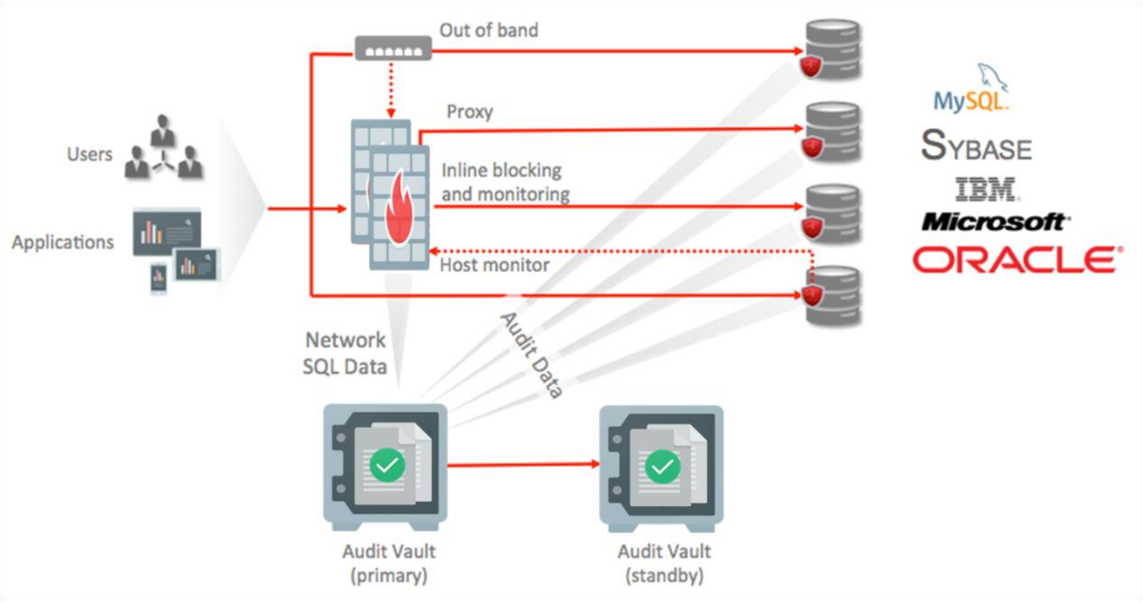


Figure 11. Oracle Audit Vault and Database Firewall deployment

Audit Agents Deployment

Audit Vault Agents collect the audit data from various sources including Oracle and non-Oracle databases, operating systems and directories. They contain collection plug-ins that collect audit data from specific secured targets. Audit Vault Agents are distributed as packaged files to the target systems and require no additional manual configuration or updates once they have been distributed. For Oracle databases SE or EE, the agents work independently of how the auditing is configured. For example, auditing can be configured to write audit data to the operating system or database. In addition, for Oracle databases, the agents can consolidate the “before” and “after” values for specific fields using the transaction or REDO logs and database entitlement information.

Policy Authoring and Management

Database Firewall policies are centrally managed from the system console. Users can define a white list, black list, or exception list of SQL statements for a given database. Database Firewall analyzes all captured SQL statements within a specified time period so that appropriate policies can be created. Firewall policies also allow factors such as user names, IP addresses, client programs, and time of day to be associated with policies for SQL statements.

Oracle Audit Vault and Database Firewall can centrally define and provision audit settings for Oracle databases. This provides both internal auditors and IT security a much easier way to manage audit settings across the enterprise and demonstrate compliance and repeatable controls to external auditors.

Oracle Audit Vault and Database Firewall Hybrid Cloud Deployment

With the rapid adoption of the cloud, companies often face the situation where some of their databases are on-premise and others are in the cloud. The risk profile for cloud databases is different from the on-premise databases as they are possibly managed by other administrators, or have different network protection mechanisms. Monitoring database activity is a key security control whether the database is on-premise or in the cloud.

Utilizing an on-premise security and audit infrastructure for both on-premise and cloud database targets has many advantages including consistent policies, unified reporting, and common alert management. In hybrid cloud deployments, the on-premise Audit Vault Server collects audit data from both on-premise databases and cloud database instances. Any cloud service with persistent network connection can use Oracle Audit Vault and Database Firewall. Figure 12 shows an example of hybrid cloud deployment to collect audit logs from Oracle Database Cloud Service (DBCS) instances. On-premise agents retrieve audit data from the DBCS instances over encrypted channels, and then transfer it to the on-premise Audit Vault Server. Appropriate ports on the DBCS instance needs to be open, but no other networking changes are needed on premise side.

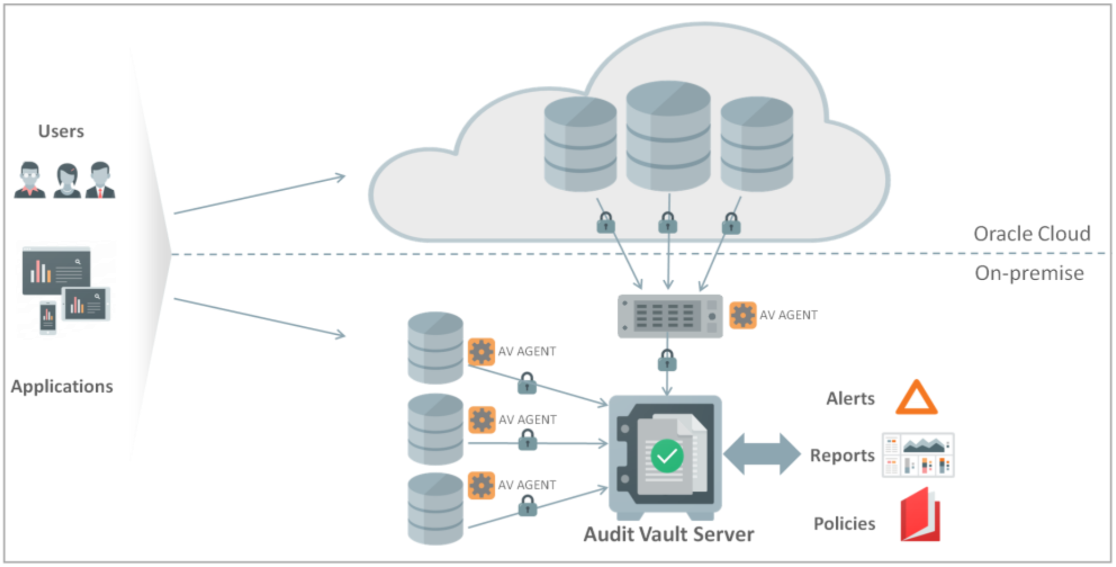


Figure 12. Oracle Audit Vault and Database Firewall hybrid cloud deployment

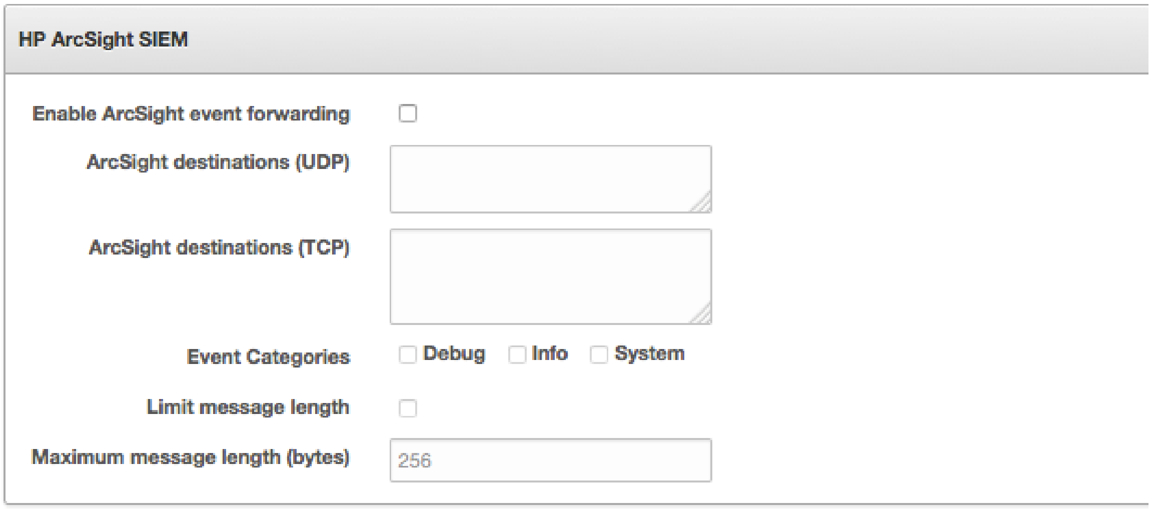
Custom Audit Collection Plug-ins

Developers and third-party vendors can build custom collection plug-ins to collect audit data from a new secured target type or a new audit trail where audit data is stored in database tables and XML files. Secured target type can be relational databases, operating systems, mid-tier systems, or enterprise applications. No coding is required as you can easily define a template-based XML mapper file to describe the audit data to be collected and whether to store the audit data either in database tables or XML files.

Integration with Third-Party Party Solutions

Oracle Audit Vault and Database Firewall can be configured to send alerts via e-mail or syslog. The content and the format of these alert messages is fully customizable. Auditors can define unlimited number of message templates and apply them to different alert definitions. This enables effortless integration with 3rd party enterprise monitoring and analytics solutions. An example of 3rd party solution is HP ArcSight Security Information Event Management (SIEM), which is a centralized system for logging, analyzing, and managing messages from different sources. Audit Vault Server forwards messages to the ArcSight SIEM system from both Audit Vault Server and Database Firewall components.

You do not need to install additional software if you want to integrate ArcSight SIEM with Oracle Audit Vault and Database Firewall. You configure the integration by using the Audit Vault Server console (Figure 13). When you enable the ArcSight SIEM integration, the settings take effect immediately. You do not need to restart the Audit Vault Server.



HP ArcSight SIEM

Enable ArcSight event forwarding	□
ArcSight destinations (UDP)	
ArcSight destinations (TCP)	
Event Categories	□ Debug □ Info □ System
Limit message length	□
Maximum message length (bytes)	256

Figure 13. Oracle Audit Vault and Database Firewall Integration with HP ArcSight SIEM

Conclusion

Oracle Audit Vault and Database Firewall helps organizations increase security by proactively monitoring database activity on the network and inside the database, protecting against SQL injection threats, consolidating audit data into a secure and scalable repository, and automating reporting to support audit and compliance activities. Extensive reporting and alerting capabilities provide auditors and security personnel with access to detailed information and early warning alerts on potential malicious activity. Sources beyond databases can be monitored, with out-of-the-box support for consolidation of audit data from various operating systems and directory services. An extensible plug-in architecture enables custom audit sources to be added to the collection framework, enabling application specific audit data to be aggregated and reported together with other event data in the repository. Audit Vault and Database Firewall delivers effective detective and preventive controls for Oracle and non-Oracle databases alike.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

ORACLE AUDIT VAULT AND DATABASE FIREWALL TECHNICAL WHITE PAPER
MARCH 2018

Oracle is committed to developing practices and products that help protect the environment