

AUDIT VAULT CLOUD TARGETS FOR HYBRID CLOUD DEPLOYMENTS

ORACLE®**AUDIT VAULT
AND
DATABASE FIREWALL**

KEY BUSINESS BENEFITS

- Centralized alerting and reporting for hybrid cloud environments
- Consistent security policies for both on-premise and cloud databases
- Lower TCO due to the utilization of the same infrastructure and operations for on-premise and cloud environments

With the rapid adoption of the cloud, companies increasingly face the situation where some of their databases are deployed on-premise while others are deployed in the cloud. The challenge is to secure them all, ideally with a unified security infrastructure. Oracle Audit Vault and Database Firewall continuously monitors on-premise database activity and consolidates monitoring events and audit data from databases, operating systems, and directories. Now it also monitors databases in the cloud, allowing sites to consolidate auditing across hybrid cloud environments where some databases are on-premise and others are in the cloud. Leveraging Oracle Audit Vault and Database Firewall for hybrid deployments make it possible to extend the same controls used for on-premise databases to cloud targets.

Monitoring Cloud Databases with an On-Premise Solution

The risk profile for cloud databases is different from on-premise databases. They could be managed by third-party administrators, have broader user populations, or different network protection mechanisms. Monitoring database activity is a key security control whether the database is deployed on-premise or in the cloud. Organizations want to monitor their cloud databases the same way they monitor their on-premise databases, but without the extra operations and infrastructure costs. In addition, they would like to transfer the audit data from the cloud to on-premise to minimize the potential for tampering and to have full control over the audit data for reporting and alerting. This helps enforce separation of duty and provide stronger security assurance.

Oracle Audit Vault for Hybrid Cloud Deployments

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 Oracle Audit Vault Server (AV Server) collects audit data from both on-premise and 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 AV Server. Outside of opening the appropriate ports on the

KEY FEATURES

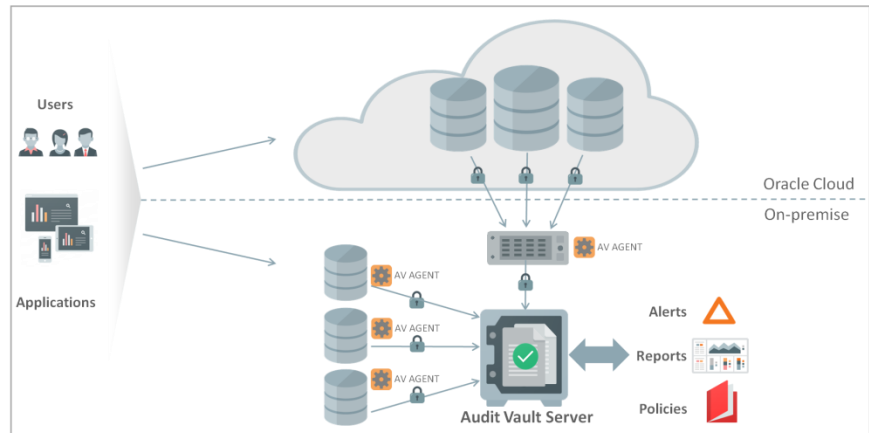
- Secure audit data collection from Oracle DBCS targets
- Consolidation of audit data for on-premise Oracle, MySQL, SQL Server, Sybase and IBM DB2 databases, along with various operating systems
- Interactive PDF and Excel reports incorporating both cloud and on-premise targets

RELATED PRODUCTS

Oracle Database 12c Defense-in-Depth Security Solutions:

- Oracle Advanced Security
- Oracle Data Masking and Subsetting
- Oracle Database Vault
- Oracle Key Vault
- Oracle Label Security

Cloud infrastructure, no other on-premise networking changes are necessary.



Audit Vault and Database Firewall Hybrid Cloud Deployment Architecture

Consistent Security Policies and Operations for Hybrid Cloud

Most companies already have existing security and audit policies in place for their on-premise database instances. Utilizing the same AV Server for both DBCS and on-premise database instances helps ensure that the same audit policies have been applied across all database instances. Similarly, existing alert configurations and data retention policies can be applied for cloud databases. Thus the same resources can be utilized for configuration and maintenance tasks across on-premise and cloud.

Enterprise Audit Data Consolidation in the Hybrid Cloud

Native audit data provides a complete view of database activity along with full execution context, regardless of whether the statement was executed directly, through dynamic SQL, or through stored procedures. The native audit is enabled by default in all DBCS instances, and is recommended for on-premise instances. The AV Server collects audit data from table, OS, and transaction logs for on-premise databases, and collects audit data from table-based audit trails for cloud databases.

Fine-grained, Customizable Reporting and Alerting





Dozens of out-of-the-box reports ensure conformance with SOX, PCI DSS, and HIPAA regulations. These reports aggregate audit data from monitored systems regardless of whether they are on-premise or in the cloud. Event data from cloud and on-premise targets can be combined, filtered and presented interactively or in PDF and Excel format reports to provide detailed trend analysis. Security managers can define threshold-based alerts on activities that may indicate attempts to gain unauthorized access and/or abuse of system privileges on any of their databases.



CONTACT US

For more information about Oracle Audit Vault and Database Firewall, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0318