Frequently Asked Questions

AVDF Hybrid Cloud Deployment

Oracle Audit Vault and Database Firewall (AVDF) consolidates database activity monitoring events and audit data from databases, operating systems, and directories. AVDF now provides a solution for consolidating audit data for not only on-premise but also in Hybrid Cloud environments where some databases are on-premise while others are in the cloud. This document describes frequently asked questions about AVDF Hybrid Cloud deployments.

AVDF Hybrid Cloud Deployment model

Q: What is Hybrid Cloud Deployment for AVDF?

A: Audit Vault Server (AV Server) deployed on-premise can collect audit data from both Oracle Database Cloud Service (DBCS) and on-premise database instances. It utilizes on-premise Audit Vault (AV) agent(s) to collect audit data from database instances in DBCS. Currently, AV Server collects data for traditional audit, fine grained audit, Database Vault audit, and Unified Audit (12c only) only from table based audit trails on cloud databases.

Q: What exactly does the AV Agent do? How is it deployed?

A: On-premise AV Agents retrieve audit data from one or more DBCS instances over encrypted channels, and then transfer it to the on-premise AV Server. For platform support of the AV Agents, click on the following link.

Though a single AV Agent can collect audit data from both on-premise and cloud database targets, it is recommended to use dedicated AV Agent(s) for collecting audit data from DBCS instances. This is primarily for simplified management and maintenance.

Q: What are the networking requirements to connect an AV Agent to a cloud database? Do we need to open a port in the network firewall?

A: For TCP connections Port 1521, and for TCPS connections Port 1522 has to be open on the DBCS instances. There is no need to open ports on the on-premise network firewall.

Q: How is the traffic encrypted between the DBCS instance and the on-premise AV Agent?

A: Depending upon how the agents connect to the DBCS instance, the traffic is encrypted for SQL*Net over TCP using Oracle native encryption or TLS for TCPS connections.

Q: What configuration steps are needed on the DBCS instance?

A: If your databases already listening for SQLnet traffic, no further steps are needed. Otherwise the configuration steps are the following:

- For SQL*Net/TCP connection between AV Agent and the DBCS instance, open default listener port 1521 (or configured port number for the listener) on the DBCS instance so that AV Agent can read audit data. Only encrypted TCP connections are supported.
- For TCPS connection between AV Agent and DBCS instance, open port default listener 1522 (or configured port number for the listener) on the DBCS instance so that Audit Vault Agent can read audit data using TCPS (SQL*Net /TLS).

It is recommended to whitelist the IP address of the AV Agent on the DBCS listener as described on the following link.

Q: Can the AV Agents be installed in OPC?

A: Currently, AV Agents can be installed on-premise only. However we do plan to support AV Agent installations in DBCS.

Q: How many Cloud targets can be supported from one AV Agent?

A: Based upon the hardware configuration of the AV agent, one AV Agent can read up to 3000 audit records per second. If your audit data volume is higher, additional AV Agents have to be deployed on-premise. The recommended AV Agent configuration can be found here.

Q: Which Oracle Cloud Database Services are supported for audit data collection by AV Server?

A: Currently, audit data can be collected from DBCS and Exadata Cloud Service instances.

Q: Which version of AVDF supports Hybrid Cloud deployments?

A: Hybrid Cloud deployment is supported from AVDF 12.2.0.2.0 (12.2 BP2) onwards. Customers with prior releases need to upgrade to the latest AVDF release to get this functionality.

Q: Can the on-premise AV Server collect audit data from database instances in Amazon AWS or Microsoft Azure?

A: As long as the on-premise AV Agent can connect to the target database in the cloud, the audit data collection should work. If the AV Agent is installed on a database server in VPC or VPN, and it can connect to the on-premise AV Server, the audit data collection should work.

Audit Settings on Cloud Database Targets

Q: What audit policies should be there on the DBCS instances?

A: There are multiple options:

- For Oracle12c – if the Unified Audit Trail is enabled, there will be a set of pre-defined audit policies created, and some of them enabled. Users have to review this information directly on the DBCS instance. The list of pre-defined audit policies for the Unified Audit Trail can be found here.
- For Oracle 12c – if the Unified Audit Trail is not enabled, users can review the enabled audit policies on the AV server or directly on the DBSC instance.
- For Oracle 11gR2 - users can review the enabled audit policies on the AV server or directly on the DBCS instance.

Q: How does the audit data gets purged on Cloud targets after audit data is collected by AVDF?

A: Just like for on-premise databases, the AV Agent invokes the DBMS_AUDIT_MGMT package for Audit trail management on Cloud database targets. Customers are responsible for scheduling the actual audit data purges.

Feature Comparison with on-premise AVDF Deployments

Q: Is there any difference in functionality for reports, alerts, and data retention between Cloud targets and on-premise targets?

A: The features are identical.

Q: Are Operating Systems and Active Directory audit trail supported for audit data collection in Hybrid Cloud deployment scenarios?

A: Currently, only for on-premise targets.

Q: Are Database audit trails from Operating Systems or redo log supported for audit data collection in Hybrid Cloud deployment scenarios?

A: Currently, only for on-premise targets.

Q: Are the custom audit collectors supported in Hybrid deployment scenarios?

A: Currently, only for on-premise targets.

Q: What about support for Oracle Database Firewall?

A: Currently, only for on-premise targets.

Product Licensing and Support

Q: How do I license AVDF Cloud targets

A: One on-premise processor license can be deployed on 2 OCPUs.

Q: Who do I contact if I have issues with Hybrid Cloud deployment?

A: Please contact My Oracle Support at https://support.oracle.com

More Information?

Q: Where can users get more information about deploying AVDF in Hybrid Cloud environments?

A: More information can be found here.

Q: Is there a generic AVDF FAQ?

A: AVDF FAQ available from OTN.

ORACLE

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200