Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Oracle Audit Vault

Release 12.1 (12.1.0.2.0)

E26595-02

September 2012

Oracle Audit Vault is used to transparently collect and consolidate audit data into a secure central repository. Audit Vault accomplishes this task by configuring policies, agents and collectors/trails to bring audit data from database sources such as Oracle database, Microsoft SQL Server, IBM DB2, and Sybase Adaptive Server Enterprise (ASE).

The Oracle Audit Vault plug-in provides support for monitoring Oracle Audit Vault Release 10.3.x Server and 10.2.3.2.x Agent components only. You can monitor these database source types in Enterprise Manager only if the source database is available and supported (for example, Database plug-in for IBM DB2, Sybase ASE plug-in, Microsoft SQL Server plug-in, etc.).

Audience

This document is intended for anyone who is responsible for administering an Oracle Audit Vault system and has purchased Oracle Enterprise Manager 12.1.

Related Documents

- *Oracle Audit Vault Administrator's Guide*
- *Oracle Audit Vault Auditor's Guide*
- *Oracle Enterprise Manager Cloud Control Administrator's Guide*

Versions Supported

This plug-in supports the following versions of products:

- Oracle Audit Vault product components:
  - Audit Vault Server 10.3.x or higher
  - Audit Vault Agent Version 10.2.3.2.x or higher
- Oracle Enterprise Manager Cloud Control 12*c* (Release 12.1.0.2)

Prerequisites

This section should contain any special instructions required that are specific to installing, configuring, or using the Audit Vault plug-in.

Note: The Oracle Database plug-in Release 12.1.0.2.0 or later should be deployed first. See Deploying the Oracle Database and Audit Vault Plug-ins.

The Oracle Audit Vault plug-in supports the following native Audit Vault manageable entities as a target or collection item types:

- **Audit Vault database** - the Audit Vault repository database already managed by the DB plug-in. The DB plug-in should already be installed and configured. The Audit Vault Database/repository must be added as an Enterprise Manager target explicitly.

  Note: The Audit Vault plug-in does not add the Database target. It only establishes association with the Audit Vault Repository Database target if it is added as an Enterprise Manager target.

- **Audit Vault agent** - Process that controls collector startup/shutdown. Depending on the Audit Vault release, this can be located under its own ORACLE_HOME directory.
- **Audit Vault collector** - Process to collect audit data from the source and send it to Audit Vault repository database.
- **Audit Vault source database** - The objects from which audit data is being collected by Audit Vault.

  If the source is an Oracle Database and added as an Enterprise Manager target, then the Audit Vault plug-in tries to create an association with managing Audit Vault Agent and source database target provided the collected properties do match for both targets like, global database name and host name.
- **OC4J target** - If your environment includes the Fusion Middleware Add-on and you have added OC4J (which manages the Audit Vault Console) as a target, then it can be managed out of the box.

  Note: The Audit Vault plug-in does not discover or create any special target for OC4J managing the Audit Vault Console. However, the Audit Vault plug-in reports the status of the Audit Vault Console application as part of Audit Vault targets.

SELECT_CATALOG_ROLE and AV_MONITOR User Role Requirements

To monitor Audit Vault through Enterprise Manager, a user with the AV_MONITOR and SELECT_CATALOG_ROLE roles should be used.

To create a new user with the required roles:

1. Connect to the Audit Vault repository with Oracle Database Vault Account Manager (user with DV_ ACCTMGR role) and create a new user:

   ```
   CREATE USER monitor_user
   IDENTIFIED BY password;
   ```

2. Connect to the Audit Vault repository with a user with SYSDBA privilege and grant SELECT_CATALOG_ROLE to the new user:

```
CONN sysdba_user
Enter password: password

GRANT SELECT_CATALOG_ROLE, CREATE SESSION TO monitor_user;
```

3. Connect to the Audit Vault repository with Audit Vault Administrator and grant `AV_MONITOR` role to the new user:

```
CONN avadmin_user
Enter password: password

GRANT AV_MONITOR to monitor_user;
```

Components Monitored

The Oracle Audit Vault plug-in provides monitoring support for the following Audit Vault components:

- Audit Vault Server
- Audit Vault Agent
- Audit Vault Collector

Deploying the Oracle Database and Audit Vault Plug-ins

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to deploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

Discovering Targets Automatically

After successfully deploying the plug-in, follow these steps to add the plug-in target to Enterprise Manager Cloud Control for central monitoring and management:

1. From the **Setup** menu, select **Add Target** and then **Configure Auto Discovery**.
2. Click on the Oracle Audit Vault module and then the Configure icon to display the **Configure Target Discovery for Target Types** screen.
3. Click **Add Host**. Make sure you have added all hosts that you want to manage.
4. In the Search and Select pop-up, select a host from the target list and click **Select**.
5. Click **OK**.

Manually Adding Targets

In addition to automatic discovery, Enterprise Manager Cloud Control allows you to manually add hosts as well as a wide variety of Oracle software and components as managed targets.

You must be able to specify the properties of a target to be managed and create an Enterprise Manager managed target.

Not all target types can be manually added. During registration with the discovery framework, the target type owner indicates whether a target type can be manually added or not.

To add targets manually to Enterprise Manager, follow these steps:

1. Log in into Enterprise Manager.
2. Click **Setup,** then click **Add Target** followed by **Add Targets Manually** from the drop-down menus. Enterprise Manager displays the Add Targets Manually page.
3. Under the Add Targets Manually page, go to the Add Targets Manually sub-section and choose an option:
   - Add Non-Host Targets Using Guided Process

     Choose one of the target types to add, such as **Oracle Cluster and High Availability Service**, **Oracle Database Machine**, or **WebLogic Domain Discovery**. This process will also add related targets.
   - Add Non-Host Targets by Specifying Target Monitoring Properties

     Choose one of the target types to add, such as **Fusion J2EE Application**, **Applications Utilities**, or **Supplier Portal**.
4. After you select the target type, you will follow a wizard specific to the target type to add the target.

   Upon confirmation, the target becomes a managed target in Enterprise Manager. Enterprise Manager simply accepts the information, performs validation of the supplied data where possible and starts monitoring the target.

Undeploying the Plug-in

To remove a plug-in from Oracle Management Service or a Management Agent:

1. From the Setup menu, select **Extensibility**, then **Plug-ins**.
2. Select the row for the plug-in you want to remove to in the table.
3. Click **Undeploy From**, then either **Management Servers** or **Management Agent**. You can then select the OMS or Management Agent you want to remove the plug-in from.
4. Confirm the plug-in removal. Enterprise Manager notifies the connected and relevant Enterprise Manager users and begins the de-configuration process.

Notes:

- Removing a plug-in also removes all of its metadata from the Management Repository.
- Default plug-ins provided by Oracle cannot be un-deployed.

Viewing Metrics

From the Oracle Audit Vault System drop-down menu, select **Monitoring**, then **All Metrics** for the All Metrics summary page. On this page, you can view metric summaries for all targets available through the Audit Vault plug-in. In the View section, the following metric options are available:

- **Auditor Activity Notifications**. This option shows the metric notifications that are Expired, Pending, and Ready to be Sent.

- **Collector Statistics**. This summary shows the collector statistics in terms of Throughput (bytes per second and records per second) and the Time Since Last Upload (in minutes).
- **Collector Status**. The Collector Status shows the status for each collector. Details include the collector source and agent, current severity, and the date an alert was triggered.
- **Collectors with no upload**. This option shows a summary of any collectors that have not provided any upload within a set time.
- **Response.** The Response option shows the collection schedule and thresholds for the following metrics:
  - Audit Vault Console Error
  - Audit Vault Console Status
  - Status
- **Other collected items**. This option shows the collection schedule of other metrics configured to be collected.

The All Metrics summary page includes any open metric events with a severity of Critical. Click the metric name link for details.

As a reference, the top five alerting metrics for the past seven days are also provided on the All Metrics summary page.

Metric and Collection Settings

From the Oracle Audit Vault System drop-down menu, select **Monitoring**, then **Metric and Collection Settings**. On this screen, you can set collection thresholds and schedules for each target.

Note: Empty thresholds will disable alerts for that metric.

Metric Collection Errors

From the Oracle Audit Vault System drop-down menu, select **Monitoring**, then **Metric Collection Errors**. This screen will show a list of errors if your managed target encounters any metric evaluation errors. These errors are usually a result of installation or configuration issues.

Metrics Collected Summary

The following Collection and Configuration metrics are available for the Oracle Audit Vault source database target type (`ORACLE_AV`):

Collection Metrics

- Collection name: Response
  - Metric Group: Response
  - Frequency: 5 minutes
  - Metric Name

        * Status: Collects the Audit Vault server Status (Threshold = Y)
        * Message: Error or informational message (Threshold = N)

- Collection name: AV_NOTIFICATIONS
    - Metric Group: AV_EMAIL_NOTIFICATIONS
    - Frequency: 15 minutes
    - Metric Name
        * Pending: Ready to be sent
        * Expired: Alert message expired
        * Queued: Alert e-mails that are still queued
- Collection name: AV_PROCESS_STATUS
    - Metric Group: AV_COLLECTOR_STATUS
    - Frequency:
    - Metric Name
        * Status: Collects Audit Vault agent status (Threshold = Y)
        * Message: Error or informational message (Threshold = N)
- Collection name: AV_PROCESS_STATS
    - Metric Group: AV_COLLECTOR_STAT
    - Frequency: 2 minutes
    - Metric Name
        * Collector with no upload: Collector name (Threshold = N)
        * Agent: Agent name (Threshold = N)
        * latency: *X* amount of data has not been sent to the Audit Vault Repository in *Y* time (Threshold = Y)
        * throughput: How much data has been sent to the Audit Vault Repository (Threshold = Y)
        * last_upload_time: Last time data was sent to the Audit Vault Repository (Threshold = N)

Configuration Metrics

- Collection name: AV_PROCESS_CONFIG
    - Metric Group: AV_AGENT_CONFIG
        * Frequency: 24 hours
        * Configuration Data: Name, host, installation location
        * Description: An association amongst agent, collector, and source needs to be established
    - Metric Group: AV_COLLECTOR_ATTRS
        * Frequency: 24 hours
        * Configuration Data: Collector attribute name, value, description

    - Description: Collects collector attribute details

- Metric Group: AV_COLLECTOR_CONFIG
    - Frequency: 24 hours
    - Configuration Data: Name, installation location, source being supported
    - Description: An association amongst agent, collector, and source needs to be established.

- Metric Group: AV_SOURCE_ATTRS
    - Frequency: 24 hours
    - Configuration Data: Source attribute name, value, description
    - Description: Collects source attribute details

- Metric Group: AV_SOURCE_CONFIG
    - Frequency: 24 hours
    - Configuration Data: Name, installation location, version
    - Description: An association amongst agent, collector, and source needs to be established.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Oracle Audit Vault, Release 12.1 (12.1.0.2.0)
E26595-02

Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.