ORACLE

Oracle Audit Vault and Database Firewall 20

Upgrade Tips

Nov 2020

Topics

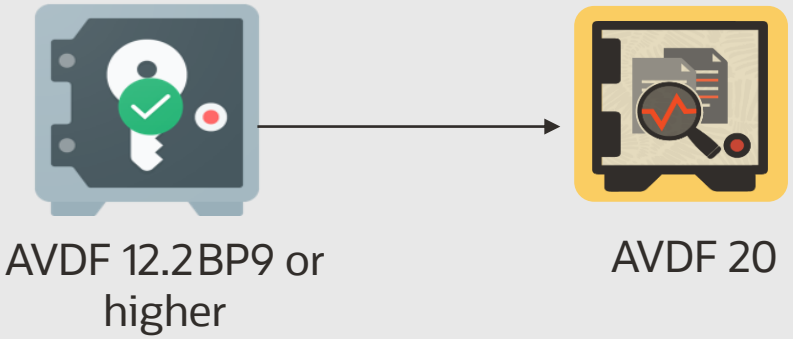
1. Upgrade Paths to AVDF20
2. Pre-Upgrade Checklist
3. Upgrade Checklist
4. Post-Upgrade Checklist

Upgrade Paths to AVDF20

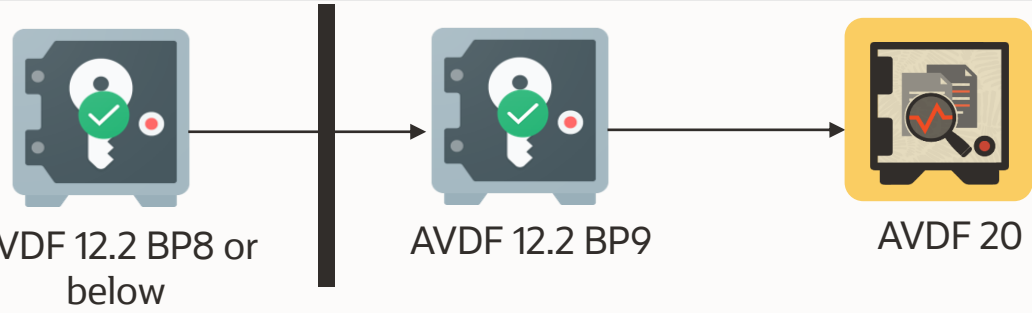
Upgrading from AVDF 12.2 to AVDF 20 (Latest RU)

AVDF 12.2 to AVDF 20 < latest RU>

Must start from *at least* AVDF 12.2 bundle patch 9



If your current version < 12.2 BP9, then you must first update to either BP9 or above prior to the upgrade



Mandatory AVDF BP9 Pre-upgrade Patch
(Doc ID 2457374.1)

Pre-Upgrade Checklist

#1 Using Host Monitor on Windows Platform ?

You most probably are at AVDF 12.2 BP10 or below, or at AVDF 12.2 BP13

While AVDF12.2 is still configured:

- Stop the audit trails and the Audit Vault Agent on Windows host machine
- Configure host monitor on Windows host following instructions in Section 8.2.1 Host Monitor Requirements
- Start the Audit Vault Agent and audit trails on the Windows host machine
  - The Host Monitor is now powered by Npcap during runtime
- Log Service Request if network trail collection is not up

#2 Using Transaction Log Collection ?

While AVDF12.2 is still configured:

- Install and deploy Oracle GoldenGate following instructions in section D.7 Migrating Transaction Log Audit Trail from Oracle AVDF 12.2 to 20
  - Log Service Request if Integrated Extract XML files are not receiving the redo log data
  - Ignore the duplicate records observed for a brief duration as indicated in the section

Note:

Post the AVDF upgrade, you will delete and recreate the transaction log audit trails pointing to the Integrated Extract XML file location. Since the XML files will already be receiving redo log data, redo data will not be lost.

#3 What is your Firmware Boot Option – Legacy BIOS / UEFI ?

- While AVDF12.2 is still configured, check the boot disk size
- If boot disk > 2 TB and firmware boot option is in Legacy BIOS mode, there are two options:
  - Option#1 : Reconfigure the boot disk to be less than 2TB, with no changes to boot mode
    - Take full backup of AVDF appliance
    - Shutdown the appliance
    - Choose a server that has at least one hard disk which is less than 2 TB
    - System is still configured to boot in legacy BIOS mode
    - Install the same bundle patch version of Audit Vault Server in 12.2 release
    - Restore from the backup
- Option#2: Change the firmware boot option to UEFI
    - Take full backup of AVDF appliance
    - Shutdown the appliance
    - Configure the system to boot in UEFI mode, while still keeping the boot disk >2TB
    - Install the same bundle patch version of Audit Vault Server in 12.2 release
    - Restore from the backup
- Refer to section 5.2.6 Pre-upgrade RPM Boot Device Greater than 2 TB

UEFI boot option is the preferred choice

#4 Is there enough space in Boot Partition ?

- While AVDF12.2 is still configured, check the boot partition space
- Boot partition should have at least 500 MB before the upgrade process can begin
- If partition space < 500MB
    - Take L0 Full backup of AVDF appliance
    - Shutdown the appliance
    - Install the same bundle patch version of Audit Vault Server in 12.2 release
    - Restore from the backup

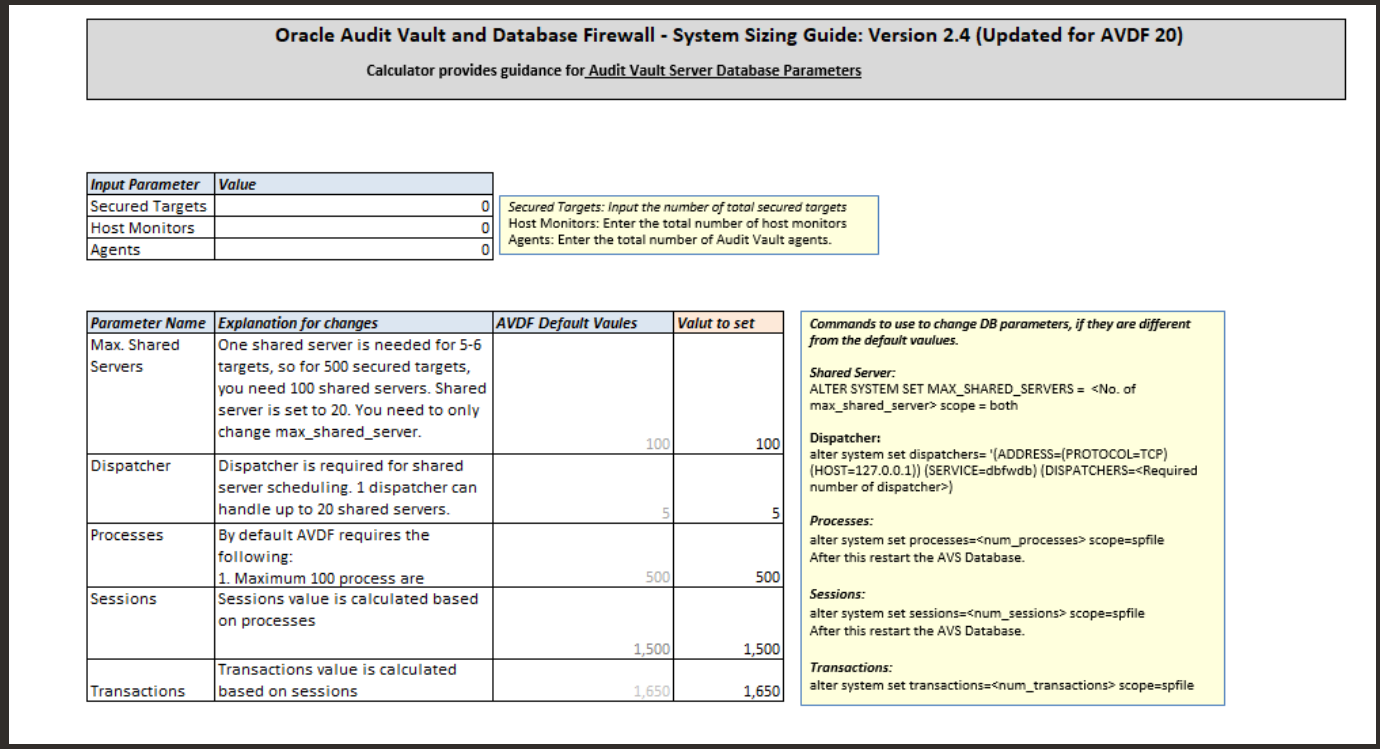
- Refer to section 5.2.7 Pre-upgrade RPM Boot Partition Space Check Warning

#5 Compatible Java Version on Agent hosts ?

- While AVDF12.2 is still configured
- Check and ensure Java version is 1.8 or above on all agent hosts
- If any agent hosts are using Java versions < 1.8, reconfigure them
  - Stop the audit trails
  - Stop the agent
  - Update Java on the agent host
  - Re-start the agent
  - Re-start the audit trails
  - Ensure the audit trails are up and running

#6 Configure AVS Database Parameters for Scalability

- Refer to Sizing spreadsheet in MOS note 2092683.1 for sizing the following AVS Database parameters in AVDF12.2
- Bounce the 12.2 AVS appliance post the configuration
- Ensure AVS 12.2 is up and running
- MUST prior to upgrading to AVDF20 for large scale enterprise deployments



Oracle Audit Vault and Database Firewall - System Sizing Guide: Version 2.4 (Updated for AVDF 20)

Calculator provides guidance for Audit Vault Server Database Parameters

Input Parameter	*Value*
Secured Targets	0
Host Monitors	0
Agents	0

Secured Targets: Input the number of total secured targets
Host Monitors: Enter the total number of host monitors
Agents: Enter the total number of Audit Vault agents.

Parameter Name	*Explanation for changes*	*AVDF Default Vaules*	*Valut to set*
Max. Shared Servers	One shared server is needed for 5-6 targets, so for 500 secured targets, you need 100 shared servers. Shared server is set to 20. You need to only change max_shared_server.	100	100
Dispatcher	Dispatcher is required for shared server scheduling. 1 dispatcher can handle up to 20 shared servers.	5	5
Processes	By default AVDF requires the following: 1. Maximum 100 process are	500	500
Sessions	Sessions value is calculated based on processes	1,500	1,500
Transactions	Transactions value is calculated based on sessions	1,650	1,650

Commands to use to change DB parameters, if they are different from the default vaulues.

Shared Server:
ALTER SYSTEM SET MAX_SHARED_SERVERS = <No. of max_shared_server> scope = both

Dispatcher:
alter system set dispatchers= '(ADDRESS=(PROTOCOL=TCP)(HOST=127.0.0.1)) (SERVICE=dbfwdb) (DISPATCHERS=<Required number of dispatcher>)

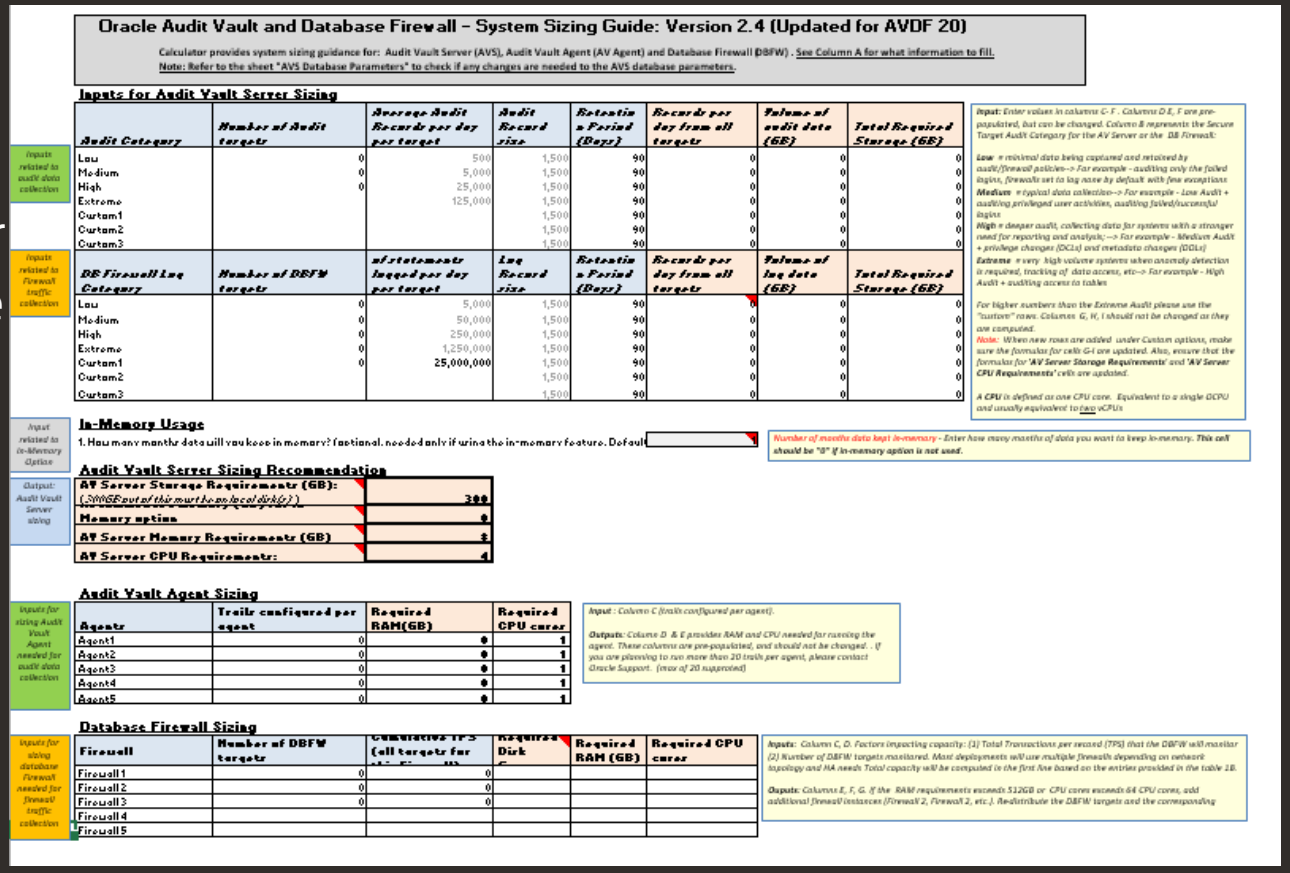
Processes:
alter system set processes=<num_processes> scope=spfile
After this restart the AVS Database.

Sessions:
alter system set sessions=<num_sessions> scope=spfile
After this restart the AVS Database.

Transactions:
alter system set transactions=<num_transactions> scope=spfile

#7 Re-evaluate Sizing of AVS and DBFW Appliance

- Refer to sizing spreadsheet in MOS note 2092683.1 for re-evaluating the AVS and DBFW server configuration prior to AVDF20 upgrade
  - Start AVDF20 on the recommended sizing configuration
  - Reach out to Product Management for any help with review /validation of the sizing spreadsheet



Oracle Audit Vault and Database Firewall – System Sizing Guide: Version 2.4 (Updated for AVDF 20)

Calculator provides system sizing guidance for: Audit Vault Server (AVS), Audit Vault Agent (AV Agent) and Database Firewall (DBFW) . See Column A for what information to fill.
Note: Refer to the sheet "AVS Database Parameters" to check if any changes are needed to the AVS database parameters.

Inputs for Audit Vault Server Sizing

Audit Category	Number of Audit targets	Average Audit Records per day per target	Audit Record size	Retention Period (Days)	Records per day from all targets	Volume of audit data (GB)	Total Required Storage (GB)
Low	0	500	1,500	90	0	0	0
Medium	0	5,000	1,500	90	0	0	0
High	0	25,000	1,500	90	0	0	0
Extreme		125,000	1,500	90	0	0	0
Custom1			1,500	90	0	0	0
Custom2			1,500	90	0	0	0
Custom3			1,500	90	0	0	0

DB Firewall Log Category	Number of DBFW targets	# of statements logged per day per target	Log Record size	Retention Period (Days)	Records per day from all targets	Volume of log data (GB)	Total Required Storage (GB)
Low	0	5,000	1,500	90	0	0	0
Medium	0	50,000	1,500	90	0	0	0
High	0	250,000	1,500	90	0	0	0
Extreme	0	1,250,000	1,500	90	0	0	0
Custom1	0	25,000,000	1,500	90	0	0	0
Custom2			1,500	90	0	0	0
Custom3			1,500	90	0	0	0

In-Memory Usage

1. How many months data will you keep in memory? (optional, needed only if using the in-memory feature. Default

Audit Vault Server Sizing Recommendation

AV Server Storage Requirements (GB):	300
Memory option	0
AV Server Memory Requirements (GB)	8
AV Server CPU Requirements:	4

Audit Vault Agent Sizing

Agents	Trails configured per agent	Required RAM(GB)	Required CPU cores
Agent1	0	0	1
Agent2	0	0	1
Agent3	0	0	1
Agent4	0	0	1
Agent5	0	0	1

Database Firewall Sizing

Firewall	Number of DBFW targets	Cumulative TPS (all targets for	Required Disk	Required RAM (GB)	Required CPU cores
Firewall1	0	0			
Firewall2	0	0			
Firewall3	0	0			
Firewall4					
Firewall5					

Upgrade Checklist

Step 1: Take Backup

- Take backup prior to performing any upgrade
  - Regardless of the upgrade paths (and multiple hops if you are upgrading from releases prior to 12.2 BP9), perform a single backup operation prior to performing the first upgrade.
  - Always recommended to do full back of the AVDF appliance
  - Ensure the backup is operational by restoring and validating
  - If AV Server is installed on a virtual machine (for example VM on Oracle VM or VMWare), it is recommended to take a VM snapshot before starting the upgrade process
- Refer to section 14.7 Backing Up and Restoring the Audit Vault Server

Step 2: Ensure the Pre-Upgrade RPM is executed successfully

- Install and execute the pre-upgrade RPM.
- Ensure pre-upgrade RPM checks are successful
- Refer to the section 5.2.1 Install Oracle AVDF Pre-Upgrade RPM

Step 3: Upgrade the Audit Vault Server

- Stop all the audit trails
- Transfer the upgrade iso and start the upgrade process following the section 5.3.4 Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances
- If the Audit Vault Server is configured in High Availability pair,
  - Upgrade the standby AVS first, followed by primary AVS upgrade
  - Follow the steps in the section 5.3.1.2 Upgrading A Pair Of Audit Vault Servers Configured For High Availability

Step 4: Upgrade the Database Firewall Server

- Stop all the monitoring points
- Transfer the upgrade iso and start the upgrade process following the section 5.3.4 Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances
- If the Database Firewall Server is configured in High Availability pair,
  - Upgrade the standby DBFW first, followed by primary DBFW upgrade
  - Follow the steps in the section 5.3.3.2 Upgrading A Pair Of Database Firewalls Configured For High Availability

Step 5: Automatic upgrade of Audit Vault Agents and Host Monitor

- Agents and Host Monitors are automatically upgraded when you upgrade the Audit Vault Server
  - Send update signal will be sent to all agents which are up and running to auto-update
  - During the Audit Vault Agent auto-update process, its status will be UNREACHABLE for a while. It may take as much as 45 minutes to return to RUNNING state.

Post Upgrade Checklist

Step 1: Apply the patch to remove Deprecated Ciphers

- Ensure all Audit vault Agents are upgraded to 20 and Host Monitor Agents are in Installed state
- Apply the patch Deprecated-Cipher-Removal.zip to remove deprecated ciphers post upgrade
- Refer to the section 1.1 About the Software Installation Procedure

Step 2: Confirming the success of Audit Vault Upgrade

- The Audit Vault Server console can be launched without any issues.
- Successful log in to Audit Vault Server console as administrator and auditor without any issues.
- The home page of the Audit Vault Server console displays the correct version
- SSH connection to the Audit Vault Server is successful without any errors.
- Check the following items as administrator in Settings->System main page
  - Check the Uptime on the main page.
  - Check the status of Database Firewall log collection is up.
  - Check the status of Background Job is up.
  - Check the High Availability Status.

Step 3: Confirming the success of Database Firewall Upgrade

- Log in to the Audit Vault Server console as administrator.
  - Click Database Firewalls tab.
  - The main page contains a list of Database Firewall instances. The status must be Up.
  - The Version should indicate release 20.
  - Click on a specific Database Firewall instance under the Name field.
  - Click Health Indicators under the Diagnostics section. All the health indicators must have a green mark.
  - Ensure all the monitoring points are up in the Database Firewall Monitoring tab
  - Ignore the blank NIC interface field on the monitoring point configuration as the monitoring point is functional if it is Up. The UI issue will stand addressed in near RU release

Step 4: Confirming the success of Audit Vault agent /Host monitor

- Log in to the Audit Vault Server console as administrator.
- Click Agents tab.
- The status of the Agents must be RUNNING.
- Check the version in the Agent Details column. It should indicate release 20.
- Check the Host Monitor version. It should indicate release 20.

Step 5: Miscellaneous Post-Upgrade Tasks

- Enable automated archiving

- Refer to the following section in AVDF Install Guide for other post upgrade tasks
  - 5.4 Post Upgrade Tasks

- Refer to the list of known issues/workaround:
  - 1.5 Known Issues

Step 6: What functionality is carried over to AVDF 20 following the Upgrade ?

- All the configurations done on 12.2 AVDF appliance that are saved in AVSYS database, including
  - Policies provisioned (Audit policies, Alert policies, Firewall policies)
    - Note the nomenclature changes in AVDF20 for user-defined firewall policy rules in section 6.2.1 Understanding Database Firewall Policies
    - Note that Unified Audit policies in the Oracle database target can be retrieved and provisioned from AVDF console. Refer section 5.4 Provisioning Unified Audit Policies
  - Data retention policies
  - Registered targets, and corresponding audit trails and monitoring points
- All customizations done on 12.2 AVDF appliance that are saved in AVSYS database, including
  - Any custom reports created
  - Any custom collectors configured with audit collection plug-ins

ORACLE